RAPPORT D'ACTIVITÉS 2011
ACTIVITEITENVERSLAG 2011

Quis custodiet ipsos custodes?

Quis custodiet ipsos custodes? est une série de publications qui a pour objectif de stimuler une discussion approfondie quant au fonctionnement, aux compétences et au contrôle des services de renseignements et de sécurité et du travail de renseignements. Dans cette série on trouvera e.a. repris des études scientifiques, les rapports d'activités du Comité permanent R et des rapports de colloques.

Rédaction

Comité permanent de contrôle des services de renseignements et de sécurité, rue de Louvain 48 bte 4, 1000 Bruxelles (02 286 29 88).

Déjà paru dans cette série

1) D. Van Daele, et B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Comité permanent R, *Rapport d'activités 2006*, 2007, 143 p.
3) Comité permanent R, *Rapport d'activités 2007*, 2008, 85 p.
4) *All Source Threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, Belgian Standing Committee I (ed.), 2010, 220 p.
5) Comité permanent R, *Rapport d'activités 2008*, 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Comité permanent R, *Rapport d'activités 2009*, 2010, 127 p.
8) Comité permanent R, *Rapport d'activités 2010*, 2011, 119 p.
9) Comité permanent R, *Rapport d'activités 2011*, 2012, 134 p.

RAPPORT D'ACTIVITÉS 2011

Comité permanent de contrôle des services de renseignements et de sécurité

Comité permanent de contrôle des services de renseignements
et de sécurité

intersentia
Antwerpen – Cambridge

Le présent *Rapport d'activités 2011* a été approuvé par le Comité permanent de contrôle des services de renseignements et de sécurité lors de la réunion du 8 mai 2012.

(*soussignés*)
Guy Rapaille, président
Gérald Vande Walle, conseiller
Peter De Smet, conseiller
Wouter De Ridder, greffier

Rapport d'activités 2011
Comité permanent de contrôle des services de renseignements et de sécurité

ISBN 978-94-000-0313-2
D/2012/7849/49
NUR 823

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

A.M.	Arrêté ministériel
Ann. Parl.	Annales parlementaires
AR C&HS	Arrêté royal du 24 mars 2000 portant exécution de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
AR OCAM	Arrêté royal du 28 novembre 2006 portant exécution de la Loi du 10 juillet 2006 relative à l'analyse de la menace
BSC	*Balanced Score Card*
CANPAN	Commission d'avis pour la non-prolifération des armes nucléaires
CERT	*Computer Emergency Response Team*
CIC	Code d'instruction criminelle
CMRS	Comité ministériel du renseignement et de la sécurité
Comité permanent P	Comité permanent de contrôle des services de police
Comité permanent R	Comité permanent de contrôle des services de renseignement et de sécurité
Commission BIM	Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil des données par les services de renseignement et de sécurité
CRIV	Compte Rendu Intégral – Integraal Verslag
Doc. Parl.	Documents parlementaires
ENNIR	*European Network of National Intelligence Reviewers*
HUMINT	*Human intelligence*
IMINT	*Image intelligence*
L.Contrôle	Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace
L.C&HS	Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
L.OCAM	Loi du 10 juillet 2006 relative à l'analyse de la menace
Loi MRD	Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité
L.Org.recours	Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité

L.R&S	Loi organique du 30 novembre 1998 des services de renseignement et de sécurité
M.B.	Moniteur belge
MRD	Méthodes de recueil des données
OCAM	Organe de coordination pour l'analyse de la menace
OSINT	*Open source intelligence*
PSE	Potentiel scientifique et économique
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
RFI	*Request for Information*
SGRS	Service général du renseignement et de la sécurité des Forces Armées
SIGINT	*Signals intelligence*
SPF	Service public fédéral
TIC	Technologies de l'information et de la communication
VSSE	Sûreté de l'État

PRÉFACE

La rédaction d'un rapport annuel constitue l'occasion idéale pour se pencher rétrospectivement sur son propre fonctionnement. Qu'avons-nous réalisé ? Sur quels aspects avons-nous mis l'accent ? Avons-nous atteint les objectifs que nous nous étions fixés ? Ce retour sur l'année 2011 a mis en évidence de nombreux faits marquants, dont quatre retiennent particulièrement notre attention dans cette préface.

Citons tout d'abord l'audit mené au sein du Service général du renseignement et de la sécurité. Après une radiographie approfondie de la Sûreté de l'État en 2009, le Comité permanent R s'est intéressé, l'an passé, au service de renseignement militaire. Réaliser un tel audit requiert un travail considérable. Il a dès lors littéralement mobilisé le Comité. Tant la Commission de suivi du Sénat, le ministre de la Défense que le SGRS ont reconnu la plus-value des résultats de l'audit en termes d'amélioration de l'efficacité et de l'efficience (voir II.1 et IX.2.1).

Rome ne s'est pas faite en un jour. Il en va de même pour l'*European Network of National Intelligence Reviewers* (ENNIR), une initiative du Comité et de sa Commission sénatoriale de suivi. Cette plateforme d'échange d'informations basée sur un site Internet et destinée aux organes européens de contrôle des services de renseignement et de sécurité a pris une forme encore plus concrète : le site Internet est en ligne (www.ennir.be) et plusieurs pays ont déjà promis d'y collaborer (voir V.5). L'année 2012 sera consacrée au développement de ce réseau, qui doit permettre l'échange d'informations intéressantes et de *best practices*.

Dans un tout autre registre, notons également le déménagement du Comité permanent R vers le nouveau bâtiment du Forum. Tout le travail effectué en amont a permis de mener l'opération à bien (voir VIII.5). Il va de soi que le personnel et les moyens investis dans ce déménagement n'ont pas pu être directement utilisés dans le contrôle des services de renseignement. Le nouvel environnement de travail et la proximité immédiate du principal partenaire du Comité – c'est-à-dire le Parlement – auront assurément un effet positif sur notre fonctionnement.

L'année 2011 fut surtout la première année où la Loi sur les méthodes de recueil des données était pleinement en vigueur (voir III). La Sûreté de l'État et le Service général du renseignement et de la sécurité ont pu faire usage de leurs compétences spécifiques et exceptionnelles pour la première fois. La nomination des membres de la Commission BIM a également rendu opérationnel le contrôle

administratif (parallèlement au contrôle juridictionnel du Comité permanent R). Une préface n'a naturellement pas pour vocation d'évaluer une législation d'une telle complexité. Nous estimons toutefois que l'année écoulée a démontré que la Loi MRD fonctionne réellement et efficacement : les services de renseignement appliquent les méthodes, sans pour autant verser dans l'excès, et le double contrôle externe démontre toute son utilité en matière de garantie des droits et libertés des personnes. Ce contrôle strict était d'ailleurs l'une des principales raisons pour lesquelles la Cour constitutionnelle a laissé intacte – à une disposition près – la Loi MRD dans son arrêt du 22 septembre 2011. La réglementation actuelle n'est pas pour autant parfaite. Il est certainement toujours possible de l'améliorer et de l'affiner : le Comité ne manquera pas de formuler les recommandations qu'il jugera nécessaires. En outre, le Comité continuera de s'investir dans sa nouvelle mission juridictionnelle dans cette matière extrêmement importante.

Guy Rapaille,
Président du Comité permanent de contrôle
des services de renseignements et de sécurité

1er juin 2012

CHAPITRE I.
LE SUIVI DES RECOMMANDATIONS DU COMITÉ PERMANENT R

L'une des tâches principales du Comité permanent R consiste à formuler, pour les pouvoirs législatif et exécutif, des recommandations qui portent notamment sur la légitimité, la coordination et l'efficacité de l'intervention des deux services de renseignement belges, de l'OCAM et, dans une moindre mesure, de ses services d'appui. Les recommandations que le Comité a formulées en 2011 figurent au dernier chapitre du présent rapport d'activités. Ce chapitre introductif énumère les principales initiatives que les différents acteurs ont prises dans la lignée des recommandations du Comité permanent R. Ensuite, une attention particulière est accordée aux recommandations que le Comité estime essentielles, mais qui n'ont pas encore été mises en œuvre.

I.1. INITIATIVES ET RÉALISATIONS DANS LA LIGNÉE DES DIFFÉRENTES RECOMMANDATIONS

Le Comité permanent R a pu constater que plusieurs recommandations majeures ont été concrétisées en 2011.

I.1.1. MISE EN ŒUVRE DES RECOMMANDATIONS FORMULÉES DANS LE CADRE DE L'AUDIT DE LA VSSE

En 2008-2009, le Comité permanent R a réalisé un audit au sein de la Sûreté de l'État. Le rapport final contenait 31 recommandations, réparties en quatre thèmes (leadership, gestion de l'information, processus de travail et satisfaction qualité).[1] En novembre 2010, la Commission de suivi du Sénat a demandé au Comité permanent R d'indiquer les recommandations qu'il considérait comme

[1] COMITÉ PERMANENT R, *Rapport d'activités 2009*, 5-23 et 81-83.

primordiales. Le Comité a alors procédé à une sélection sur la base de quatre principes de bonne gestion. Un état des lieux a été demandé au service concerné.

Le premier principe consistait à « *définir des objectifs après consultation des donneurs d'ordre et parties prenantes, et définir les moyens* ». En ce qui concerne les recommandations formulées dans ce cadre, le Comité a pu constater que la VSSE avait finalisé à temps son Plan stratégique 2011, les plans opérationnels requis, le plan du personnel et le budget. En outre, plusieurs initiatives ont été lancées afin d'impliquer plus étroitement les donneurs d'ordre et parties prenantes dans le fonctionnement de la VSSE. En raison de restrictions budgétaires, le plan du personnel n'a toutefois pas pu être entièrement réalisé. Plusieurs projets en ont souffert, comme par exemple l'initiative qui a pour but d'interroger les « clients » des services d'analyse ou encore l'initiative relative au déroulement du cycle d'évaluation dans les services internes.

Un deuxième principe consistait à « *traduire les objectifs en processus de travail et identifier les risques* ». La VSSE a énuméré plusieurs processus de travail et en a commencé la description. Elle a également décrit les risques liés aux processus critiques de gestion et déterminé les mesures à prendre pour les maîtriser. Le Comité a néanmoins remarqué qu'en raison d'un manque d'encadrement, la description des processus de travail a été plus lente que prévu. Les *Key Performance Indicators*, qui mesurent le déroulement des processus de travail, n'étaient pas encore élaborés.

L' « *apport de moyens en vue d'atteindre les objectifs et la bonne gestion de ces moyens* » est le troisième principe sur lequel le Comité s'est basé pour sélectionner les recommandations. Dans ce cadre, le Comité a pu constater que les descriptions de fonction requises et les compétences qui y sont liées ont été établies. En outre, la VSSE a investi dans la formation, surtout dans le cadre de l'évolution de la carrière des collaborateurs. La manière dont la formation a été abordée restait cependant assez formaliste et ne dépassait pas le cadre strictement réglementaire. Plusieurs initiatives qui ont été développées mettaient l'accent sur le cadre de valeurs de la VSSE, dont l'importance de la collaboration interne. Un projet était en chantier en matière de gestion des connaissances et des outils spécifiques ont été mis à disposition. Par manque de moyens, aucune cellule spécifique, censée prendre en charge cette gestion des connaissances, n'a pu être mise en place.

Enfin, le Comité a souhaité se faire une idée de l'avancement du « *suivi de la situation externe et interne afin d'adapter l'organisation (mécanisme de feedback)* », et ce grâce à plusieurs instruments élaborés par la VSSE elle-même. Celle-ci manque toutefois de moyens (TIC) pour en poursuivre le développement. La VSSE avait également l'intention de suivre la réalisation de la vision et la stratégie de sa direction en utilisant un tableau de bord prospectif (*Balanced Score Card* – BSC). Cet instrument doit évoluer pour devenir un véritable outil de gestion permettant de suivre les différents processus. Peu de progrès ont toutefois été enregistrés dans le projet BSC.

En conclusion, le Comité a pu constater que la Sûreté de l'État a vraiment tenu compte des recommandations et a tenté de les mettre en pratique. Bien que des améliorations aient été constatées pour toutes les recommandations, les progrès ont été généralement lents, et ce surtout en raison d'un manque de moyens. Enfin, il s'est avéré que certaines recommandations ont fait l'objet d'une approche relativement formaliste, et ce à cause, entre autres, du cadre réglementaire dans lequel la VSSE est tenue de fonctionner. Le Comité permanent R a estimé que la Sûreté de l'État devrait déterminer les risques liés à l'exécution retardée, ainsi que les mesures correctives requises.

I.1.2. ADAPTATION DE LA POSITION D'INFORMATION AUX BESOINS DES AUTORITÉS COMPÉTENTES EN MATIÈRE DE DEMANDES DE RECONNAISSANCE DE COMMUNAUTÉS RELIGIEUSES

Dans son rapport d'activités relatif à l'année 2009, le Comité recommandait que la VSSE veille à l'actualisation systématique des données qu'elle recueillait sur les communautés religieuses. Le ministre de la Justice a en effet besoin de ces informations car il doit ensuite conseiller les autorités régionales dans le cadre de demandes de reconnaissance de communautés religieuses.[2]

A la mi-2011, la VSSE a rédigé une note de service concernant le traitement de telles demandes de reconnaissance. Dans ce contexte, il a été annoncé que les agents qui travaillent dans le domaine du radicalisme islamiste avaient pris des mesures allant dans le sens de la remarque formulée par le Comité.

I.1.3. DIRECTIVES CLAIRES CONCERNANT *HUMINT*

Le Comité permanent R a régulièrement formulé des recommandations concernant le travail avec les informateurs. Ainsi, le Comité s'était entre autres étonné de l'éparpillement des directives *HUMINT* dans différents documents, directives ou cursus. Vu l'importance du travail avec les informateurs, la VSSE avait déjà annoncé en 2009 qu'elle se chargerait d'élaborer une réglementation interne globale.[3]

En 2011, ce fut chose faite avec le document intitulé «*Instructies over het werken met menselijke bronnen*»[4] et une note de service sur «*l'évaluation des informations émanant de sources humaines*». Le Comité souligne l'importance du contenu des deux documents, qui englobent tous les aspects du travail avec

2 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 87.
3 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 35-36 et 84-85.
4 «Instructions concernant le travail avec les sources humaines» (traduction libre).

des informateurs. Ces directives émanent de l'Administrateur général de la VSSE. Le Comité insiste toutefois sur le fait que l'obligation d'édicter des directives concernant le travail avec des sources humaines incombe au Comité ministériel du renseignement et de la sécurité depuis janvier 2011 (art. 18 L.R&S).

I.1.4. SYSTÈME *REQUEST FOR INFORMATION* AU SEIN DU SGRS

Le Comité a dû constater que cinq ans après la découverte d'une lacune majeure dans le système de gestion des données du SGRS, des considérations d'ordre budgétaire et des réticences internes n'avaient pas permis de la combler. Cette situation était sans aucun doute de nature à compromettre la bonne exécution des missions du SGRS. Le Comité permanent R a dès lors recommandé que le service y remédie.[5]

À l'occasion de l'audit (voir II.1), le Comité a pu constater que le SGRS a introduit le système baptisé *Request for information* en septembre 2011. Ce système doit résoudre les problèmes constatés.

I.1.5. PLAN D'ACTION DU SGRS À LA SUITE DE L'AUDIT

En 2010, le Comité a lancé un audit sur le service de renseignement militaire. Cet audit s'est clôturé à la mi-2011 (voir II.1) et a donné lieu à de nombreuses recommandations (voir IX.2.1). En 2011 déjà, le SGRS a élaboré un plan d'action afin de mettre effectivement en œuvre ces recommandations. C'est ainsi qu'une *task force* a été mise en place. Elle se réunit à un rythme hebdomadaire autour de six thèmes : processus, personnel, formation, investissements, sécurité et divers. La première phase de la mise en œuvre de ce plan d'action est en cours. Il s'agit d'analyser, d'inventorier et de réaliser un screening des zones à problèmes.

I.1.6. L'AUDITION D'ANCIENS MEMBRES DES SERVICES DE RENSEIGNEMENT

Jusqu'en 2010, le Comité permanent R pouvait uniquement convoquer, en vue de les auditionner, les membres de la VSSE et du SGRS en fonction, et donc pas d'anciens membres de ces services de renseignement. Cette possibilité a été inscrite à l'article 48 L.Contrôle par la Loi du 9 février 2011 (*MB* 29 mars 2011) sur la recommandation du Comité.[6]

---

5 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 41-42 et 103.
6 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 88.

I.1.7. STRATÉGIE RELATIVE À LA SÉCURITÉ DE L'INFORMATION

Dans son «*enquête sur la manière dont les services de renseignement belges envisagent la nécessité de protéger les systèmes informatiques contre des interceptions et cyberattaques d'origine étrangère*» (voir II.2), le Comité a constaté un grand morcellement de la politique en matière de sécurité des systèmes informatiques. Il s'est dès lors rallié aux conclusions du *Livre blanc pour une politique nationale de la sécurité de l'information*. Le Comité permanent R a également recommandé l'élaboration d'une stratégie fédérale en la matière et la création rapide d'une agence ayant pour mission de coordonner les activités relatives à la sécurité de l'information (voir IX.2.3). Le passage suivant a été intégré dans l'Accord gouvernemental du 1er décembre 2011: «*Afin de donner suite aux recommandations du Comité R, le Gouvernement élaborera une stratégie fédérale de sécurité des réseaux et systèmes d'information, dans le respect de la protection de la vie privée*».

I.1.8. DESCRIPTION DES PROCESSUS *SIGINT*

Dans le cadre de sa mission de contrôle spécifique en matière d'interception par le SGRS de communications émises à l'étranger (voir Chapitre IV), le Comité avait insisté sur l'importance de décrire les processus de manière élaborée.[7] Les descriptions des processus ont été finalisées entre-temps. Elles rendront notamment les vérifications légales plus efficaces.

I.2. RETOUR SUR DES RECOMMANDATIONS ANTÉRIEURES

L'article 35, alinéa 3, L.Contrôle confère au Comité permanent R la mission de faire rapport à la Chambre des Représentants et au Sénat «*lorsqu'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*». Le Comité permanent R recourt à cette possibilité uniquement s'il estime que les recommandations essentielles à la préservation des droits fondamentaux, à un fonctionnement optimal des services de renseignement et de l'OCAM ou à un contrôle efficace, sont restées sans réponse, et ce sans raison apparente.

Le Comité demande une nouvelle fois d'accorder une attention particulière à la manière dont le SGRS ou la VSSE transmettent des données (à caractère

7 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 74 et 103.

personnel) à des services homologues étrangers. En effet, le Comité a pu constater, dans le cadre de son contrôle MRD (voir Chapitre III), que les services de renseignement belges sont régulièrement interrogés par des services étrangers. Le (contrôle de ce) flux d'informations n'est toutefois pas suffisamment réglementé.[8]

[8] Voir précédemment, COMITÉ PERMANENT R, *Rapport d'activités 2006*, 128 ; *Rapport d'activités 2007*, 71 ; *Rapport d'activités 2008*, 6 et 105-106 ; *Rapport d'activités 2009*, 4 et 106-107 et *Rapport d'activités 2010*, 3-4. Voir également, dans le même sens, les recommandations émises dans le cadre du rapport suivant : United Nations General Assembly, Human Rights Council, *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including their oversight*, Report of the special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin SCHEININ, 17 May 2010, A/HRC/14/46, particulièrement *« 31 – 35 Good practices on intelligence sharing and cooperation »*, 26-29.

CHAPITRE II.
LES ENQUÊTES DE CONTRÔLE

En 2011, le Comité permanent R a reçu 25 nouvelles plaintes ou dénonciations de particuliers. Après avoir procédé à la vérification de plusieurs données objectives, le Comité a classé sans suite 19 plaintes ou dénonciations, soit parce qu'elles étaient manifestement non fondées (art. 34 L.Contrôle), soit parce qu'il n'était pas compétent. Dans ces derniers cas, les plaignants ont été renvoyés, si c'était possible, vers l'instance compétente. Les deux plaintes qui étaient encore pendantes à la fin de l'année 2010 n'ont pas non plus donné lieu à l'ouverture d'une enquête. Une enquête de contrôle a été ouverte pour trois nouvelles plaintes ou dénonciations. Pour les trois plaintes restantes de 2011, des vérifications sont toujours en cours pour déterminer si une enquête se justifie.

Outre les trois enquêtes faisant suite à des plaintes, le Comité permanent R a ouvert, en 2011, une enquête de contrôle à l'initiative du président du Sénat.

En 2011, dix enquêtes ont été clôturées. Les sous-chapitres suivants traitent en premier lieu des enquêtes de contrôle clôturées (de II.1 à II.10). Ils énumèrent et décrivent ensuite de manière succincte les enquêtes toujours en cours (II.11).

II.1. UN AUDIT AU SEIN DU SERVICE DE RENSEIGNEMENT MILITAIRE

II.1.1. INTRODUCTION

Le service de renseignement militaire belge s'est vu confier quatre missions par le législateur :

- une mission de renseignement relative à toute activité qui menace ou pourrait menacer entre autres l'intégrité du territoire national, les plans de défense militaires, le potentiel scientifique et économique, l'accomplissement des missions des Forces armées ou la sécurité des ressortissants belges à l'étranger ;
- le maintien de la sécurité militaire du personnel et des installations militaires ;
- une mission de protection des secrets qui s'attachent entre autres aux installations et renseignements militaires ;
- et, enfin, l'exécution d'enquêtes de sécurité (art. 11 L.R&S).

Ces missions ne peuvent naturellement être menées à bien que si le SGRS emploie les moyens dont il dispose de manière effective et efficace. Avec le soutien de la Commission de suivi du Sénat, le Comité permanent R a décidé d'effectuer un audit pour déterminer si tel était le cas.[9]

Le Comité ne s'est pas contenté de réaliser un *performance audit*[10] dans le but de se faire une idée de la situation du service concerné. Il tenait également à initier une dynamique qui donnerait lieu à de réels changements et améliorations là où c'était nécessaire. Le Comité a formulé plusieurs recommandations circonstanciées visant à mettre en place cette dynamique.[11] Afin de situer ces recommandations, le Comité présente brièvement dans ce chapitre la structure du service audité, ainsi que le déroulement et les résultats de l'audit.

II.1.2. LES THÈMES PRINCIPAUX

Étant donné que le Comité s'était fixé un délai relativement court (six mois), il se devait de sélectionner les domaines qu'il allait examiner. Cette sélection s'est appuyée sur des critères tels que la valeur ajoutée[12], la matérialité[13] et les degrés de risque et d'incertitude.[14]

Les deux premiers domaines d'enquête sélectionnés concernaient « les moyens humains » et « la gestion de l'information ». L'affectation du personnel et l'utilisation des informations disponibles jouent en effet un rôle essentiel au sein d'un service de renseignement. Il n'est pas seulement question d'investissements[15], mais aussi de stratégie puisque que le travail de renseignement dépend entièrement des moyens humains et de la possession des informations correctes. Le Comité s'est également intéressé au « système de gestion de l'organisation » (contrôle interne de l'organisation auditée). Comme le contrôle interne se fonde sur la gestion des risques au sein d'une organisation, le Comité s'est également penché sur cette matière dans le troisième volet de son audit.

---

9 « *Audit en vue de la définition et de la vérification des conditions nécessaires à l'affectation des moyens du Service général du Renseignement et de la Sécurité (SGRS), avec notamment une attention portée à la gestion et à la direction du personnel, aux flux d'informations et à la gestion des risques* ».

10 Voir également à cet égard l'audit mené au sein de la Sûreté de l'État : COMITÉ PERMANENT R, *Rapport d'activités 2009*, 5-23.

11 Voir Chapitre IX. Recommandations (particulièrement le point IX.2.1). En outre, le Comité a regroupé les considérants formulés dans l'audit sous la forme d'une feuille de route (« *roadmap* ») visant une meilleure utilisation des moyens au sein du SGRS.

12 « Moins un domaine est connu, plus grande sera la valeur ajoutée d'un audit dans ce domaine. ».

13 « L'importance du domaine en termes d'investissements, d'intérêt stratégique, d'impact public… ».

14 « En principe, les domaines dont on ne sait pas grand-chose (par exemple, parce qu'ils n'ont jamais fait l'objet d'un audit) ou dans lesquels des incidents se sont produits par le passé, constituent des domaines de risque ou d'incertitude. ».

15 Les coûts en personnel représentent la majeure partie du budget du SGRS.

II.1.3. PHASAGE ET MÉTHODOLOGIE

Le Comité permanent R a énormément investi en termes d'effectifs et de moyens dans cette enquête de contrôle.

L'audit proprement dit a naturellement été précédé par la réalisation d'un plan d'audit et par l'élaboration d'une méthodologie fondée, conformément aux normes internationales en vigueur.

L'audit a été divisé en phases. La première phase avait pour but de se faire une idée de la situation en étudiant la documentation demandée au SGRS et en menant des entretiens exploratoires (décembre 2010).

Durant la deuxième phase, des données concernant des questions qui concernaient toutes les couches de l'organisation (par exemple, la communication interne, la formation, la collaboration) ont été recueillies. Ces données ont ensuite été converties en chiffres bruts. Les auditeurs ont également examiné d'éventuelles pistes d'amélioration, entre autres en faisant appel à l'expérience et aux suggestions des membres du service. Le personnel a eu l'occasion de donner son avis en répondant à un questionnaire écrit (janvier – février 2011).[16] Lors d'un entretien personnel et confidentiel, les personnes interrogées ont également pu communiquer des informations complémentaires. Toutes les (sub)divisions du SGRS ont reçu la visite des auditeurs. Lors de ces visites, les responsables et les collaborateurs ont pu expliquer en quoi consistaient leurs tâches et quelles étaient leurs conditions de travail.

Au cours de la troisième phase, les informations collectées ont de nouveau été soumises au SGRS, et les questions identifiées ont été vérifiées et approfondies lors des entretiens menés avec les responsables et les spécialistes. Les auditeurs ont également tenté de formuler des suggestions d'amélioration. À cette fin, des groupes cibles ont été constitués pour travailler de manière transversale, en d'autres termes par-delà les divisions (mars – mai 2011).

La dernière phase a porté sur la rédaction du rapport (juin 2011). L'audit a donné lieu à un rapport volumineux (198 pages), qui a dû être classifié « SECRET ».

II.1.4. STRUCTURE DU SERVICE DE RENSEIGNEMENT MILITAIRE

Le SGRS est dirigé par le Commandement (SGRS/C), qui dispose d'un état-major composé de quelques personnes et d'un secrétariat. Le SGRS (qui emploie tant des civils que des militaires) compte quatre divisions, qui opèrent en majeure partie depuis Bruxelles.

[16] Le taux de réponse brut de cette enquête s'élevait à 71,5 %, contre 67,3 % pour le taux de réponse net (sans les questions restées sans réponse). Ces résultats sont certainement représentatifs.

La Division A(*ppui*) regroupe tous les services chargés de l'appui général du SGRS, à savoir la gestion du personnel et du budget, les technologies de l'information et de la communication (TIC), les aspects logistiques qui sont gérés au sein du SGRS…

La Division C(*ounter*)I(*ntelligence*) suit les phénomènes qui sont susceptibles de menacer la sécurité militaire et qui se situent principalement sur le territoire belge. Cette division dispose de plusieurs détachements provinciaux qui transmettent les données recueillies aux analystes de cette section.

La Division I(*ntelligence*) constitue la plus grande division du SGRS et remplit également une mission de recueil et d'analyse. Elle s'intéresse aux phénomènes qui se produisent à l'étranger et qui se situent dans le rayon d'action du SGRS. Les services d'analyse de cette division sont en grande partie organisés par région géographique. Elle compte également des bureaux pour les trois matières *Naval, Air* et *Land Intelligence*, ainsi que pour les questions transnationales. Le département I/Ops est actif à l'étranger en appui des troupes belges. Il recueille des renseignements sur place, tant au profit des militaires sur le terrain que du SGRS dans son ensemble.

La Division S(*ecurity*) doit s'acquitter de deux grandes missions. D'une part, elle effectue des enquêtes de sécurité sur des personnes ou sociétés qui demandent une habilitation ou attestation de sécurité dans le but de pouvoir effectuer certaines tâches ou missions au sein de ou pour la défense (S/Habilitations). Cette division peut également faire appel aux détachements provinciaux. D'autre part, la division veille également à la sécurité militaire (domaines, personnes, systèmes TIC) dans le sens où elle formule des directives qui doivent être suivies par les différentes entités de la Défense nationale et où elle peut procéder à des inspections dans certains cas (S/Security, MIS[17] et S/Infosec).

II.1.5. LIGNES DIRECTRICES DE L'AUDIT

Les paragraphes qui suivent expliquent brièvement les résultats de l'audit par domaine sélectionné.

II.1.5.1. Affectation, gestion et motivation du personnel

Le SGRS est encore confronté à de nombreux défis en matière de gestion[18] et de motivation du personnel.

Les points forts du service sont sans aucun doute le caractère passionnant de la fonction et la possibilité pour le personnel de développer ses propres initiatives

17 *Military and Industrial Security.*

18 Les thèmes relatifs aux ressources humaines, tels que le recrutement, la gestion des départs naturels, la carrière, la rémunération…

dans les domaines où cela s'avère nécessaire. La motivation et l'affectation du personnel s'appuient sur ces éléments extrêmement importants.

Le personnel peut toutefois être utilisé avec davantage d'efficience et d'efficacité. La manière dont les objectifs sont formulés en interne et traduits pour les personnes sur le terrain peut être améliorée. L'audit a par ailleurs révélé que les collaborateurs en sont eux-mêmes demandeurs.

L'audit a également démontré que la fonction d'organisation et de gestion du personnel (fonction P&O) devait être renforcée afin de pouvoir investir dans les descriptions de fonction, la gestion prévisionnelle du personnel, le coaching… La capacité de développement organisationnel, dont toute organisation a besoin pour examiner, améliorer et modifier (capacité d'apprentissage) en permanence son propre fonctionnement, devait également être renforcée.

Les collaborateurs étaient plutôt moyennement satisfaits des perspectives de carrière et de la rémunération. Il s'agit toutefois d'aspects qui ne relèvent pas (uniquement) de la responsabilité du SGRS. Pour de telles matières, le service de renseignement dépend en effet de la collaboration d'autres entités, telles que la Direction générale *Human Resources* de la Défense. Là aussi, les moyens sont plutôt limités. Une concertation et une collaboration actives entre tous les partenaires tant au sein qu'en dehors du SGRS restent nécessaires.

Un autre point délicat concerne l'égalité de traitement des différents groupes du personnel au sein du SGRS notamment en termes de perspectives de carrière et de système d'allocations… La situation du personnel civil a particulièrement attiré l'attention. Sa place au sein des structures militaires et ses perspectives de carrière au sein du SGRS n'étaient pas claires. Plusieurs facteurs ont indiqué que l'équilibre entre civils et militaires était fort perturbé. Bien que les inégalités (statutaires) dépassent le cadre du SGRS, elles se sont avérées très problématiques dès lors que le nombre total de civils au sein de l'effectif du SGRS semble proportionnellement relativement élevé. En outre, le personnel civil occupe une place centrale dans le cycle de renseignement, et plus particulièrement dans la phase d'analyse. Le Comité permanent R estime toutefois que cette problématique doit être traitée avec prudence, car toute mesure prise au profit d'un groupe donné peut être considérée comme injuste par d'autres collaborateurs.

L'audit a cependant montré que les inégalités ne concernaient pas qu'un seul groupe, mais plusieurs, qu'il s'agisse de civils ou de militaires. Comme le Comité estime que le service doit permettre à tous les collaborateurs de réaliser leurs ambitions, il a indiqué que la « logique de groupe » en vigueur doit faire place à une logique « fonctionnelle ». Il convient de ne pas penser en termes de « catégories de personnel » (militaires par opposition à civils, contractuels par opposition à statutaires, niveau X par opposition à niveau Y…), mais plutôt en termes de « fonctions » (par exemple, la fonction de ligne[19], d'analyse ou de

[19] Il s'agit d'une fonction hiérarchique.

collecte). Au sein de ces fonctions, il est possible de veiller à traiter chacun de la même manière, quel que soit son statut ou grade.

Le Comité a estimé que la fonction d'analyse, qui emploie du personnel aux statuts variés, méritait une attention prioritaire, ce qui ne signifie pas que d'autres « inégalités » (entre autres dans les services de collecte) méritent moins d'attention.

Le fait que le personnel militaire du SGRS provient d'autres entités des Forces armées, et n'est parfois affecté que peu de temps au SGRS, constitue une autre source de préoccupation. La rotation relativement importante posait problème pour l'accueil, la formation et la gestion des connaissances. Le Comité permanent R a estimé que la solution pourrait résider dans la création d'une branche « renseignement » dans le cadre de laquelle peuvent se dérouler l'évolution des carrières et le développement des connaissances. Le recrutement de collaborateurs, la rédaction de profils de fonction cohérents, l'élaboration d'une gestion des compétences, l'organisation des carrières et formations pourraient être organisés depuis et au sein de cette branche. Le personnel civil pourrait également bénéficier d'une position plus claire et mieux faire évoluer sa carrière.

II.1.5.2. Gestion de l'information

En ce qui concerne la gestion de l'information, le Comité permanent R a pu constater que le personnel du SGRS tentait de maîtriser le volume sans cesse croissant d'informations et de documentation, avec les « moyens du bord » très limités. Un système RFI (*Request for Information*)[20] a été mis en œuvre à l'automne 2011 afin de répondre aux constatations d'une enquête de contrôle antérieure.[21]

En dépit des efforts déployés, le Comité a dû constater qu'un système TIC intégré, dans lequel le personnel peut aisément et rapidement saisir et retrouver des données, ne pourrait pas être mis sur pied à court terme. Les investissements requis sont reportés indéfiniment. Plusieurs changements ont toutefois pu être apportés, bien qu'ils soient ralentis par le report des investissements prévus (au moment de l'audit déjà et jusqu'en 2016). Le Comité a dû constater que les activités de renseignement ne bénéficient pas (plus) d'un soutien au niveau des TIC. En raison du volume important, certaines informations étaient difficilement accessibles ou exploitables. Le SGRS risquait aussi de passer à côté de ces

---

20 Le système *Request for Information* se fonde sur un document standardisé qui décrit les renseignements demandés.

21 Enquête de contrôle relative à la gestion de l'information au sein du service de renseignement militaire. À l'origine, cette enquête de contrôle avait été ouverte parce qu'un défaut de communication avait été constaté dans un cas concret entre les Divisions *Intelligence et Counter Intelligence*. Voir à cet égard COMITÉ PERMANENT R, *Rapport d'activités 2010*, 41-42.

informations. Dans ce sens, les conditions d'une bonne gestion de l'information n'étaient pas (plus) totalement remplies.

Le Comité permanent R a souligné les risques évidents qui en découlent. Il est effectivement impossible de garantir que les informations (qui *a posteriori* s'avèrent cruciales dans un dossier) soient interceptées, retrouvées et/ou traitées (à temps) par le service. Ces risques doivent être réduits en investissant dans les technologies de l'information et de la communication.

Cependant, comme c'est le cas pour la gestion du personnel, le SGRS dépend d'autres entités de la Défense pour ses besoins matériels et budgétaires. Ce qui a amené le Comité à conclure que la collaboration entre le SGRS et ces entités de toutes les parties concernées requiert une nouvelle forme d'ouverture, où le caractère souvent « secret » des activités du SGRS ne peut pas entraver la communication.

II.1.5.3. Systèmes de contrôle interne et gestion des risques

Le dernier domaine examiné dans le cadre de l'enquête concernait la gestion de l'organisation et la gestion des risques qui y est liée. Le Comité permanent R a souligné qu'en raison de la rotation et des départs au sein du personnel, le SGRS était exposé à un certain nombre de risques[22] en termes de discontinuité et de perte de connaissances. Ces risques devaient être davantage identifiés et mieux gérés. À cette fin, une fonction P&O forte, des outils TIC efficaces et une gestion sérieuse des connaissances s'avèrent nécessaires pour progresser. Récemment, le SGRS a lancé un outil de gestion des risques. Toutefois, la maîtrise des risques passe nécessairement par une définition correcte des objectifs du SGRS et la mise au point des processus.

II.1.5.4. Autres constatations

Durant l'audit, le Comité a dressé plusieurs constats qui sortaient du cadre de l'enquête.

La protection physique de l'infrastructure et les moyens de surveillance déployés au sein du SGRS n'atteignaient pas partout le niveau que l'on est en droit d'attendre d'un service de renseignement militaire.

En ce qui concerne les besoins en personnel[23], le Comité a constaté que certains bureaux d'analyse et de collecte devaient se contenter d'un effectif

---

22 La notion de « risques » désigne l'incertitude qui pèse sur les objectifs de l'organisation. Les risques correspondent à tous les évènements et circonstances susceptibles d'influencer la réalisation de ces objectifs.

23 L'audit n'a pas permis de se prononcer davantage à ce sujet. Les besoins en personnel ne peuvent être déterminés qu'une fois que les objectifs et les *Service Levels* du SGRS ont été définis dans les détails.

minimum, ce qui présentait également des risques pour la continuité des services fournis.

Enfin, le Comité a également dû constater qu'il convenait de renforcer la collaboration entre le SGRS et d'autres composantes de la Défense comme les directions *Human* et *Material Resources* ainsi que l'Audit Interne de la Défense.

II.1.6. ÉVALUATION GÉNÉRALE

À la question de savoir si les conditions d'une bonne gestion du personnel sont remplies, le Comité a pu répondre par l'affirmative, bien que des améliorations et changements soient naturellement possibles et nécessaires.

En ce qui concerne l'accès et l'exploitation des informations disponibles (c.-à-d. le travail de renseignement), la réponse s'est toutefois révélée plutôt négative. Le Comité permanent R a pu constater que le service de renseignement militaire ne disposait pas des moyens requis (certainement en matière de TIC) et courait dès lors le risque de passer à côté de certaines données ou de ne pas les exploiter.

Enfin, la gestion de l'organisation et des risques est un domaine auquel le SGRS ne s'intéresse que depuis peu et pour lequel beaucoup reste à faire.

Si le SGRS est encore en mesure de fournir un bon travail, c'est en grande partie grâce à l'assiduité et au professionnalisme de son personnel. Les problèmes et risques réels auxquels l'organisation est confrontée sont quelque peu masqués par le dévouement de nombreux collaborateurs.

Il est prévisible que la situation précaire dans laquelle le SGRS se trouvait au moment de l'audit ne sera pas tenable à terme. Le Comité a conclu qu'il convient soit de rectifier le niveau d'ambition, soit d'adapter les moyens (et l'organisation). Sinon, les risques découlant de la situation doivent être acceptés. Et parmi ces risques, figure celui de ne plus être à même de satisfaire les attentes (élevées) des donneurs d'ordre du SGRS.

II.2. LA PROTECTION DES SYSTÈMES DE COMMUNICATION CONTRE D'ÉVENTUELLES INTERCEPTIONS ET CYBERATTAQUES ÉTRANGÈRES

Dans une société de l'information, il est crucial de protéger les systèmes de communication gérés par des technologies informatiques. En effet, plusieurs grandes puissances considèrent les attaques massives sur ces systèmes comme l'une des principales menaces pour la sécurité, les intérêts militaires et l'économie d'un pays, ainsi que pour les libertés et droits fondamentaux des

citoyens. La Commission de suivi du Sénat a dès lors exprimé le souhait que le Comité permanent R l'informe de la manière dont les services de renseignement suivent cette matière.[24]

Les sous-sections suivantes présentent successivement un aperçu des institutions fédérales qui sont actuellement chargées de la protection des systèmes TIC et le rôle de la Sûreté de l'État et du SGRS. Cette section se termine par quelques conclusions.

II.2.1. INSTITUTIONS FÉDÉRALES CHARGÉES DE CETTE MATIÈRE

Contrairement à ses voisins[25], la Belgique ne compte pas d'organe dédié spécifiquement à la protection des systèmes d'information. Plusieurs services publics fédéraux sont impliqués dans cette problématique, mais les moyens dont ils disposent ne sont pas toujours suffisants. Quels sont ces services ?

Tout d'abord, la politique en matière de lutte contre les menaces à l'encontre de systèmes d'information en général – et la politique en matière de renseignement en particulier – relève du Comité ministériel du renseignement et de la sécurité (CMRS). Toutefois, le CMRS n'a, à ce jour, formulé aucune directive concrète en la matière.

Le SPF Technologie de l'Information et de la Communication (FEDICT) a également pour mission d'élaborer et de mettre en œuvre une politique visant la protection des systèmes d'information des administrations fédérales. FEDICT est entre autres chargé de mettre en place une structure de services gouvernementaux en ligne (*e-government*) et de favoriser l'informatisation de la société. Il s'est également vu confier la tâche de réaliser un inventaire de l'infrastructure informatique critique.

L'Autorité nationale de sécurité (ANS) a été désignée en tant qu'autorité d'homologation pour les systèmes et réseaux des services publics fédéraux appelés à traiter, transporter ou conserver des informations classifiées nationales ou internationales (UE, OTAN). L'ANS a pour mission de veiller à la sécurité des systèmes d'information en trois étapes : l'évaluation, la certification et l'homologation proprement dite. Faute de moyens suffisants, l'ANS n'est pas en mesure d'exécuter pleinement cette tâche.

---

24 La Commission a également souhaité recevoir une mise à jour du rapport Échelon présenté en 2000 par le Comité permanent R (COMITÉ PERMANENT R, *Rapport d'activités 2000*, 27 et suiv.).

25 Voir, par exemple, l'*Agence Nationale de la Sécurité des Systèmes d'Information* (France), *le Bundesamt für Sicherheit in der Informationstechnik* (Allemagne) ou l'*Office of Cyber Security* (Royaume-Uni).

BELNET[26] a vu le jour en 2000. Ce service est entre autres chargé du développement, de l'introduction et de la gestion du réseau de communication entre les services publics fédéraux et Internet. Certaines connexions de ce réseau dit FEDMAN (*Federal Metropolitan Area Network*) ont été sécurisées. Une partie – appellée BINII[27] – est réservée à l'échange d'informations classifiées. Cette fonction est gérée par le SGRS. BELNET s'est également vu confier la tâche de créer une *Computer Emergency Response Team* (CERT)[28] au niveau fédéral.[29] Ce centre d'avertissement et de réaction peut être sollicité par des instances publiques et des entreprises qui sont la cible d'une attaque électronique. Le service public CERT.be a démarré ses activités en septembre 2009.[30]

Auparavant, la Plateforme de concertation fédérale sur la sécurité de l'information, mieux connue sous le nom de BELNIS (*Belgian Network Information Security*), avait déjà été créée. Outre la VSSE et le SGRS, cette plateforme réunit des représentants d'autorités fédérales telles que l'ANS, le Centre de crise du gouvernement, la *Federal Computer Crime Unit*, le Collège des procureurs généraux, la Commission de la protection de la vie privée… La plateforme BELNIS a entre autres formulé des propositions en matière de protection des infrastructures TIC critiques ainsi qu'en matière d'homologation des systèmes qui traitent des données classifiées. Au cours de l'année 2007, BELNIS a rédigé le livre blanc intitulé *« Pour une politique nationale de la sécurité de l'information »*. Il y a été constaté que cet enjeu n'était que très partiellement couvert en Belgique. Ce livre blanc a formulé plusieurs propositions de nature à

26 BELNET est un service public à gestion séparée au sein du SPF Politique scientifique.

27 Voir également COMITÉ PERMANENT R, *Rapport d'activités 2007*, 48.

28 Normalement, un CERT doit s'acquitter des tâches suivantes :
- la centralisation des signalements d'incidents (attaques) sur les réseaux et systèmes d'information, celle des demandes d'assistance suite à ces incidents de sécurité (réception des demandes, analyse des symptômes et éventuelle corrélation des incidents) ;
- le traitement des alertes et la réaction aux attaques informatiques : analyse technique, échange d'informations avec d'autres CERTs, contribution à des études techniques spécifiques ;
- l'établissement et la maintenance d'une base de données des vulnérabilités ;
- la prévention par la diffusion d'informations sur les précautions à prendre pour minimiser les risques d'incident ou, au pire, leurs conséquences ;
- la coordination éventuelle avec les autres entités (hors du domaine d'action) : centres de compétence, réseaux, opérateurs et fournisseurs d'accès à Internet, CERTs nationaux et internationaux.

29 Dans ce cadre, BELNET a collaboré avec l'Institut belge des services postaux et des télécommunications (IBPT).

30 Un CERT a également été créé au sein de la Défense nationale, avec pour mission d'analyser les activités suspectes et de traiter les incidents de sécurité qui surviennent sur les ordinateurs de ses réseaux. Cette équipe avait été initialement baptisée *Computer Security Incident Response Capability* (CSIRC) ; sa mission se limitait au traitement des incidents en matière de sécurité de l'information.

remédier aux lacunes constatées.[31] Pour le Comité permanent R, les recommandations ci-dessous étaient essentielles[32] :

- l'adoption d'une loi-cadre précisant les objectifs généraux du pays en matière de sécurité de l'information ;
- la désignation des institutions chargées de la réalisation de ces objectifs ;
- la mise en place d'une autorité nationale de certification et d'homologation des systèmes sensibles agissant en concertation avec l'ANS et le SGRS ;
- l'amélioration et la coordination de la représentation belge dans les groupes de travail internationaux[33] ;
- la réalisation d'un inventaire des infrastructures TIC critiques, publiques et privées, en Belgique.

II.2.2. LA SÛRETÉ DE L'ÉTAT

II.2.2.1. Compétences et moyens

Dans l'ensemble des services publics décrits ci-dessus, la VSSE ne joue qu'un rôle limité. Le législateur n'a pas confié au service la mission légale de « protéger » les réseaux TIC. En outre, la VSSE ne dispose d'aucune capacité légale ni technique de procéder à des contre-mesures électroniques.

Avec les moyens dont elle dispose et compte tenu des initiatives développées par des différents services et diverses instances concernés, la VSSE s'en tient à sa « mission de renseignement ». Cette mission consiste à recueillir des informations sur des attaques, sur des menaces d'attaques et sur des interceptions de communications provenant d'Etats et d'acteurs non étatiques.

Les seules sources d'informations pertinentes sont les investigations informatiques (« *computer forensics* ») menées sur les attaques (réussies ou non) qui ont été détectées. Celles-ci supposent une capacité légale et technique de pouvoir, par exemple, identifier des adresses électroniques ainsi que leurs titulaires. Jusqu'à la mise en œuvre de la Loi MRD, la VSSE ne disposait pas de cette capacité. Depuis lors, le service peut, à titre de méthode spécifique, prendre des « *mesures d'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques ou du moyen de communication électronique utilisé* », et des « *mesures de repérage des données d'appel de moyens de*

31 Le Comité permanent R a dû constater que le Livre blanc ne faisait nulle part mention du rôle que la VSSE peut jouer en la matière.

32 Dans l'intervalle, plusieurs recommandations ont été concrétisées : la création d'un CERT national (à savoir CERT.be) ; la création d'un système pour réaliser l'inventaire de l'infrastructure TIC critique ; la désignation de consultants en sécurité de l'information dans les administrations fédérales…

33 Ainsi, l'IBPT, le SGRS et plusieurs experts individuels (souvent bénévoles) assurent une représentation de la Belgique dans toute une série de groupes de travail internationaux, mais sans réelle coordination avec les autres autorités concernées.

communications électroniques et de localisation de l'origine ou de la destination de communications électroniques ».[34]

II.2.2.2. La section informatique de la VSSE

Au sein de la VSSE, une section informatique a pour tâche d'apporter un soutien opérationnel TIC aux services extérieurs et de gérer le système informatique de la VSSE. La mission de cette section consiste aussi à suivre les menaces visant les systèmes TIC, à établir de la documentation sur les tendances constatées, à mener des actions de sensibilisation, à émettre des avis de sécurité et à mener des enquêtes en réaction à des faits constatés.[35]

Le Plan stratégique de la VSSE prévoyait la désignation d'un directeur TIC ainsi que l'extension du cadre de cette section. Le service n'a toutefois pas reçu l'accord du Service d'encadrement Personnel et Organisation du SPF Justice ni de l'Inspecteur des Finances. Le Comité permanent R a estimé que cette situation était très problématique et a recommandé que les ressources humaines qualifiées soient mises à la disposition de la VSSE.

II.2.2.3. Matériel INFOSEC[36]

Les informations émanant des services étrangers peuvent uniquement être traitées dans le respect des normes de sécurité en vigueur au niveau international. La VSSE n'utilise dès lors que du matériel certifié et homologué. Compte tenu de l'insuffisance des moyens (techniques) mis à la disposition de l'ANS (cf. ci-dessus), la VSSE est toujours obligée de recourir à des systèmes et à des procédures qui ont été certifiés par des autorités étrangères. Le Comité permanent R estime que cette situation est problématique.

II.2.2.4. Évaluation de la menace

Étant donné le nombre de cibles potentielles (les institutions européennes, les quartiers généraux de l'OTAN et du SHAPE, les institutions publiques belges, les instituts de recherche et les entreprises *high-tech*), la VSSE estime que la menace de cyberattaques doit être prise au sérieux. Les cyberattaques susceptibles de

---

34 Article 18/2 § 1er, 4° et 5° L.R&S.

35 Les membres de cette section participent également aux travaux du « *Working Group on Electronic Attack* » (WGEA) du Club de Berne. Ce groupe de travail se réunit pour échanger des informations sur les tendances et les faits constatés en matière d'attaques électroniques contre des systèmes TIC et pour pouvoir coordonner, le cas échéant, des actions communes.

36 INFOSEC vise l'application de mesures de sécurité destinées à protéger les informations traitées, stockées ou transmises par des systèmes d'information, de communication ou d'autres systèmes électroniques contre des atteintes à la confidentialité, à l'intégrité ou à la disponibilité de ces informations (que celles-ci soient accidentelles ou intentionnelles) ainsi qu'à empêcher les atteintes à l'intégrité et à la disponibilité des systèmes eux-mêmes.

menacer les intérêts et la sécurité de la Belgique émanent de puissances étrangères, d'individus et de groupes autonomes, de pirates informatiques classiques et du crime organisé. La VSSE demande dès lors aux autorités belges de prendre d'urgence des mesures de protection et de détection[37], par exemple, des actions de sensibilisation, des mesures de prévention et un plan d'urgence en cas d'attaque électronique à grande échelle.

II.2.2.5. Actions de sensibilisation et interventions ciblées

La VSSE attache beaucoup d'importance à la sensibilisation en matière de menaces générales ou concrètes. Elle a ainsi averti les autorités belges de la vulnérabilité de la confidentialité et de l'intégrité de la communication par *BlackBerry*. Dans le même sens, le service a informé les autorités (comme le ministre de la Justice, le Collège du renseignement et de la sécurité, le Comité de direction du SPF Justice, le SPF Affaires étrangères) des menaces de cyberattaques. La VSSE a également participé à l'organisation d'une campagne de sensibilisation destinée aux parlementaires européens. Un briefing a par ailleurs été organisé pour des parlementaires belges et des représentants d'autres autorités.

Aujourd'hui, les activités INFOSEC de la VSSE se limitent à des interventions ponctuelles sur des incidents portés à sa connaissance par les victimes elles-mêmes et où celles-ci coopèrent spontanément avec le service. Par exemple, le service informatique de la VSSE a participé à une enquête menée par des officiers de sécurité des Affaires étrangères. Cette enquête poursuivait un double objectif : trouver une preuve numérique d'une attaque et examiner si et dans quelle mesure les attaques électroniques avaient porté atteinte à l'intégrité de l'infrastructure informatique visée.

II.2.3. LE SERVICE GÉNÉRAL DU RENSEIGNEMENT ET DE LA SÉCURITÉ

II.2.3.1. Menaces

Le SGRS suit le nombre sans cesse croissant d'attaques contre les réseaux informatiques des autorités fédérales (telles que la Défense nationale[38]) et recueille des informations auprès de sources ouvertes concernant des

37 En novembre 2007, la VSSE n'a pas hésité à qualifier l'attitude du gouvernement de l'époque en la matière de « quasi-cécité ».

38 L'une de ces attaques portait sur le virus « Conficker » et ses variantes. Le SGRS n'a pu constater aucune infection dans les systèmes informatiques classifiés. Pourtant, à la fin 2008, des cas d'infection ont été constatés dans le réseau administratif non classifié de la Défense nationale.

cyberattaques découvertes à l'étranger. Ces intrusions semblent toujours plus complexes et difficiles à détecter, si bien que la source et les motifs précis de ces attaques sont souvent difficiles à identifier.

En ce qui concerne le renforcement de la législation américaine sur les interceptions de communications (cf. *Échelon*), le Comité a pu constater que les actions des services de renseignement américains ne figurent pas dans le Plan directeur du Renseignement. Le SGRS compte en effet sur la loyauté des services partenaires au sein de l'OTAN, puisque l'application du *Patriot Act* est dirigée contre les ennemis des États-Unis.[39] Le SGRS reconnaît toutefois que le risque d'interception s'est accru et prescrit dès lors que les informations classifiées soient codées lors de la transmission.

II.2.3.2. La section INFOSEC

Au sein de la Division S(*ecurity*) du SGRS, la section INFOSEC déploie son action dans les mesures de recherche et de protection électroniques. En d'autres termes, elle est active sur le plan de la prévention et la détection, et récemment de la réaction (voir II.2.3.4). Ces dernières années, elle a enquêté sur plusieurs incidents. Le SGRS a analysé les modes opératoires, a évalué les dommages subis et en a informé les autorités militaires.

Cette section a toutefois éprouvé de sérieuses difficultés à recruter et à conserver du personnel qualifié. Nombre de collaborateurs sont partis pour le secteur privé, où les salaires sont nettement plus attractifs. Le plan de recrutement pour 2009 prévoyait le recrutement d'informaticiens supplémentaires pour le SGRS. Ils sont entrés en service en 2010. L'enquête de contrôle a indiqué que ces recrutements pourraient ne pas suffire à pallier le manque chronique de personnel.

II.2.3.3. Sensibilisation, soutien et gestion

Sur les indications du SGRS, le Ministère de la Défense a pris plusieurs mesures pour faire face aux attaques dirigées contre les systèmes d'information. Par exemple, le personnel est systématiquement informé des menaces et des règles de sécurité à appliquer, un règlement de sécurité interne a été élaboré, des audits et contrôles de sécurité sont menés dans les unités, et de nouveaux moyens techniques sont mis en œuvre (amélioration du software, configuration de l'*Intrusion Prevention and Detection System*…).

---

[39] En 2000, le SGRS avait déclaré au Comité permanent R que l'espionnage militaire éventuel émanant de pays alliés de la Belgique ne constituait pas pour lui une priorité (voir COMITÉ PERMANENT R, *Rapport d'activités 2000*, 55). La VSSE a déclaré à cet égard que si la mise en œuvre du *Patriot Act* devait entraîner une activité portant atteinte à l'un des intérêts qu'elle est légalement chargée de protéger, elle ne manquerait pas de communiquer ses renseignements aux instances compétentes.

Le SGRS appuie également d'autres services fédéraux. Ainsi, le service participe à la plateforme BELNIS, il collabore avec la VSSE dans l'analyse de logiciels d'espionnage, il soutient le CERT.be, et il sensibilise et conseille les SPF lors de la mise en œuvre de réseaux sécurisés.

Enfin, le SGRS administre un service Intranet sécurisé porté par le réseau FEDMAN (voir II.2.1). Ce réseau a été créé, d'une part, pour échanger des renseignements classifiés entre l'OCAM, les services de renseignement et la police fédérale et, d'autre part, pour diffuser des informations classifiées depuis l'OCAM vers les SPF concernés. Le réseau peut également être utilisé pour échanger des informations classifiées entre toutes les administrations fédérales connectées.

II.2.3.4. Une nouvelle mission pour le SGRS

Jusqu'il y a peu, le SGRS ne pouvait pas prendre de contre-mesure électronique en cas d'attaque électronique. Aucune disposition légale ne le permettait. La Loi MRD a changé la donne pendant le déroulement l'enquête de contrôle : « *dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense nationale gère,* [le SGRS a pour mission] *de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés* ».[40]

Le Comité permanent R s'est réjoui que ce nouveau moyen d'action ait été octroyé au SGRS. Il s'est toutefois demandé pourquoi une telle faculté de neutralisation n'avait pas aussi été prévue en cas d'attaques menées contre le système informatique d'autres services publics ou contre des systèmes TIC qui figurent parmi l'infrastructure critique nationale.

II.2.4. CONCLUSIONS

Tant la VSSE que le SGRS ont conscience de la gravité des menaces que représentent les attaques électroniques dirigées contre les systèmes d'information vitaux (civils et militaires) du pays. Les deux services de renseignement ont dès lors pris des initiatives en vue de sensibiliser leurs « clients » à la problématique et soulignent constamment la nécessité de prendre des mesures de protection.

Dans la mesure des moyens limités mis à leur disposition, les services enquêtent aussi sur des attaques spécifiques détectées contre les systèmes information. Cette approche essentiellement défensive se fonde sur la détection et l'évaluation. Récemment, le SGRS a également pu prendre des mesures réactives.

---

40 Article 11 L.R&S.

Force est cependant de constater que l'absence d'une politique fédérale globale en matière de sécurité de l'information rend notre pays vulnérable aux agressions sur ses systèmes d'information et réseaux vitaux.[41]

Il convient également de mentionner l'absence de service centralisé pour la protection des systèmes TIC. Aucune des institutions qui exercent aujourd'hui une compétence dans ce domaine n'a pas de vue d'ensemble sur la problématique. Compte tenu de ce grand morcellement, le Comité permanent R a souscrit aux conclusions du *Livre blanc pour une politique nationale de la sécurité de l'information*. Le Comité permanent R a également recommandé l'élaboration d'une stratégie fédérale en la matière et la création rapide d'une agence chargée de coordonner les activités relatives à la sécurité de l'information.[42] L'expérience et le savoir-faire dont disposent les services de renseignement belges peuvent être mis en œuvre au sein ou au profit de cette agence.

Il a pu être constaté que les membres du SGRS et de la VSSE (sans la moindre coordination avec d'autres autorités) assurent la représentation de la Belgique dans certains groupes de travail internationaux. La clarification du rôle assigné aux services de renseignement dans la protection des systèmes d'information s'impose. Le Comité permanent R recommande que le CMRS s'y attèle.

Enfin, il convient de veiller à ce que les services de renseignement belges puissent disposer des moyens (techniques et humains) requis pour pouvoir accomplir leur mission dans ce domaine. Plus précisément, ils doivent recruter et conserver du personnel qualifié.

II.3. LA POSITION D'INFORMATION ET LES ACTIONS DES SERVICES DE RENSEIGNEMENT CONCERNANT LORS DOUKAEV

Le 10 septembre 2010, une explosion s'est produite dans un hôtel de Copenhague, la capitale danoise. Un certain Lors Doukaev a été légèrement blessé lors de cette explosion. Les explosifs qu'il portait sur lui en vue de commettre un attentat contre le journal danois Jyllands Posten ont explosé prématurément.[43]

Comme Doukaev possédait la nationalité belge, le Comité permanent R a ouvert une enquête sur la position d'information et les actions éventuelles des services de renseignement belges avant l'attentat manqué.

---

41 En 1995 déjà, le Comité permanent R attirait l'attention sur l'importance de la sécurité des systèmes d'information et la nécessité d'élaborer une politique de sécurité globale en la matière (voir COMITÉ PERMANENT R, *Rapport d'activités 1995*, 114-118).

42 Voir également « Chapitre I.1.7. Stratégie en matière de sécurité de l'information » et « Chapitre V.3. Proposition de résolution en matière de protection des systèmes d'information et de communication ».

43 A la mi-2011, Doukaev a été condamné pour ces faits à douze ans de prison par un tribunal danois.

II.3.1. LES FAITS

II.3.1.1. Qui est Lors Doukaev ?

Doukaev est né en Tchétchénie en 1986. À l'âge de dix ans, il a été victime d'une explosion de grenade, à la suite de laquelle il a dû subir une amputation partielle de la jambe droite. En 2000, il a fui avec sa mère et sa sœur vers la Belgique, où ils ont obtenu le statut de réfugié politique. Plus tard, en mars 2006, Doukaev a obtenu la nationalité belge. Conformément à la procédure, la VSSE a examiné son dossier afin d'identifier d'éventuelles contre-indications. À l'époque, l'intéressé n'était pas connu du service.

II.3.1.2. La position d'information et les actions du SGRS

En 2007, Doukaev a par hasard attiré l'attention d'un agent des services extérieurs du SGRS. Il a remarqué dans la rue un homme barbu et amputé d'une jambe en compagnie d'une femme voilée et a souhaité vérifier si l'intéressé ne faisait pas partie d'un mouvement radical. Les vérifications effectuées au sein de son service, auprès de la police fédérale et de l'Office des étrangers[44] n'ont toutefois rien révélé de suspect. Dès lors, l'agent du renseignement n'a pas établi de rapport pour son service[45], mais a conservé les informations dans sa documentation personnelle.

II.3.1.3. La position d'information et les actions de la VSSE

Fin janvier 2010, un « message de routine » d'un service partenaire étranger a indiqué à la VSSE que des participants à une réunion d'un mouvement radical islamiste avaient été identifiés lors d'un contrôle routier en octobre 2009. Lors Doukaev était l'un d'entre eux. Jusqu'à ce moment-là, il n'avait jamais attiré l'attention de la VSSE.

Au sein de la VSSE, le message du service partenaire a simplement été transmis aux divisions opérationnelles concernées et au service d'analyse compétent. Ce message a fait l'objet d'un « traitement de routine » pour trois raisons : entre les constatations (octobre 2009) et la transmission du message (janvier 2010), plusieurs mois se sont écoulés ; le service partenaire n'avait posé aucune question spécifique et Doukaev ne figurait pas dans la base de données de la VSSE.

L'une des divisions opérationnelles a alors consulté les éléments dont disposait l'Office des étrangers et a transmis le message du service partenaire,

44 La VSSE n'a donc pas été consultée.

45 Aucune information n'a naturellement été communiquée à d'autres services, tels que la VSSE ou l'OCAM.

ainsi que les résultats de son enquête, au poste de province compétent. Le message et les résultats de l'enquête ont été envoyés « pour information », sans comporter de questions spécifiques.

Le même jour, le chef de poste a confié l'affaire « pour enquête » à l'agent du renseignement chargé de suivre le milieu tchétchène. Il est donc important de noter que le statut initial du message a été modifié. L'agent de la VSSE a pris contact avec l'inspecteur de police du quartier où Doukaev résidait et a appris que l'intéressé était seulement connu pour d'anciens faits de coups et blessures et qu'il était parti plusieurs mois auparavant, sans plus de précisions. Il a alors contacté ses informateurs, sans résultat, mais pas le SGRS ni la police fédérale.

L'agent de la VSSE n'a pas jugé utile de rédiger un rapport et d'informer d'autres services, car il estimait ne pas disposer d'éléments suffisants. La VSSE a jugé par la suite que ce comportement n'était pas du tout professionnel et a pris des mesures pour éviter que la situation ne se reproduise (voir ci-après). Le Comité a également conclu que le dossier méritait davantage d'attention, étant donné le message du service partenaire, la « disparition » de Doukaev et ses origines. D'autre part, le Comité a souligné que les services centraux de la VSSE n'avaient transmis le message initial que « pour information ».

II.3.1.4. Informations policières

En mai 2010, la police d'un pays voisin a demandé à la police judiciaire fédérale de Liège des informations concernant un dénommé « Lors ». La police liégeoise a répondu qu'il s'agissait de Lors Doukaev, qu'il était connu pour des faits de coups et blessures et qu'il faisait l'objet d'une ordonnance de capture à la suite d'une condamnation du tribunal correctionnel de février 2010. Pour conclure, la police indiquait que Lors Doukaev n'était pas connu « *'terro' à l'époque et que nous n'avons jamais entendu parler de lui au sein de la communauté musulmane de Liège* ».

En outre, la police fédérale disposait d'informations provenant d'une source. En résumé, une organisation islamiste fondamentaliste aurait recruté Lors Doukaev. Il se serait laissé pousser la barbe et serait parti à la recherche d'armes et d'explosifs. Le Comité permanent R n'a toutefois pas pu déterminer si ces informations étaient antérieures ou postérieures à l'attentat manqué.

II.3.2. CONCLUSIONS

Le Comité a insisté sur la difficulté pour les services de sécurité d'identifier un « loup solitaire », surtout si le processus de radicalisation est rapide comme cela semble être le cas pour Doukaev. Il ne sera toutefois possible de déterminer si l'intéressé répond ou non à ce profil qu'après confrontation avec les informations dont disposait la police fédérale.

Indépendamment de ce fait, le Comité a constaté que les deux services de renseignement disposaient d'informations ponctuelles à des moments différents concernant Doukaev.

En ce qui concerne le SGRS, la pertinence des informations de l'agent et leur intérêt pour une quelconque banque de données ont posé question. Il semble exagéré, voire contraire à la législation sur la protection de la vie privée, de saisir des informations dans un fichier uniquement sur la base d'éléments tels que la tenue vestimentaire et les particularités physiques.

Concernant la VSSE, le Comité a constaté que les informations d'un service ami n'ont pas été exploitées. L'enquête du poste de province a été menée *a minima* et n'a pas été suivie d'un rapport adéquat. La VSSE a toutefois tiré des leçons de cette faille et a pris des mesures structurelles destinées à y remédier.

Le Comité a également dû constater qu'aucune information n'avait été échangée entre les services de renseignement, ni entre les services de renseignement et les services de police. À cet égard, le Comité a spécifiquement attiré l'attention sur les informations policières qui étaient disponibles. Il a dès lors demandé au Comité permanent P d'ouvrir une enquête sur les renseignements dont les services de police disposaient avant l'arrestation de Doukaev à Copenhague. Le cas échéant, le rapport du Comité permanent R sera complété et modifié en fonction des constatations de cette enquête de contrôle.

Le Comité a souligné que si les informations partielles avaient été partagées, il était clair que les services de renseignement et de police auraient dû prêter une attention particulière à l'intéressé. Il ne faut cependant pas en déduire que la tentative d'attentat aurait pu être évitée avec certitude.

De manière générale, le Comité a insisté sur l'importance de l'échange direct d'informations concrètes entre les services de renseignement et les services de police. Il a mis l'accent sur le fait que cet échange d'informations ne peut pas se limiter à l'échange d'analyses (générales ou spécifiques), par exemple au niveau de l'OCAM. En l'absence de communication directe des données, les services risquent effectivement de laisser passer des occasions de repérer des personnes susceptibles de mettre la société et les citoyens en danger.

II.4. LES FLUX D'INFORMATIONS ENTRE L'OCAM ET SES SERVICES D'APPUI

L'OCAM a pour mission principale d'effectuer, de sa propre initiative ou à la demande de certaines autorités, des évaluations ponctuelles ou stratégiques sur des menaces en matière de terrorisme et d'extrémisme.[46] Cette tâche incombe

[46] Cette mission est décrite dans la Loi du 10 juillet 2006 relative à l'analyse de la menace (L.OCAM) et dans l'A.R. du 28 novembre 2006 portant exécution de la Loi du 10 juillet 2006 relative à l'analyse de la menace (AR.OCAM).

aux analystes (recrutés en externe) et aux experts (détachés desdits « services d'appui »). Ces services d'appui constituent la principale source d'informations de l'OCAM. Il s'agit de la VSSE, du SGRS, de la police intégrée (police fédérale et corps de la police locale), de l'Administration des douanes et accises du SPF Finances, de l'Office des étrangers du SPF Intérieur, du SPF Mobilité et Transport, et du SPF Affaires étrangères.[47] En principe, chacun de ces services doit disposer d'un point de contact central par lequel doit transiter l'échange d'informations, de renseignements et d'analyses en provenance et à destination de l'OCAM.

Par cette enquête de contrôle conjointe, les Comités permanents P et R souhaitaient procéder à un *status quaestionis* des flux d'informations entre l'OCAM et les services d'appui, et ce au moyen d'une enquête détaillée. Les Comités ont en outre étudié l'échange d'informations à la lumière d'un *test case* concret. Ce *test case* portait sur l'analyse de la menace lors d'une éventuelle tentative d'évasion pendant le procès de terrorisme de Malika El Aroud et consorts.[48] Les sous-chapitres suivants relatent brièvement les constatations générales des deux phases de cette enquête.

II.4.1. L'APPROCHE QUANTITATIVE DES FLUX D'INFORMATIONS

Les Comités souhaitaient disposer d'une vision globale du volume de renseignements, de messages et d'analyses mutuellement échangés. Mission quasi impossible, puisqu'il s'est avéré que chaque acteur utilise un mode de calcul propre et que certains points de contact centraux n'étaient pas au courant de tous les renseignements et documents échangés. Et ce, entre autres parce que l'OCAM communiquait souvent directement avec certaines personnes clés au sein des services d'appui. Les Comités ont estimé que cette méthode de travail

47 La loi autorise l'augmentation du nombre de services d'appui. L'OCAM estime que ce n'est pas nécessaire pour l'instant, ce qui ne signifie pas que les contacts avec d'autres services ne sont pas maintenus. Par exemple, l'OCAM entretient des contacts avec le Centre de crise du gouvernement (en matière d'évaluations de menaces lors de visites), la Direction générale Sécurité et Prévention du SPF Intérieur (pour le soutien des initiatives sociales avec l'accent sur la radicalisation), le parquet fédéral, la Cellule de traitement des informations financières (en matière de transactions suspectes), le SPF Justice (pour la coopération internationale), le Service de la politique criminelle, et le Commissariat général aux réfugiés et aux apatrides. L'OCAM considère ces services comme des « partenaires ». Ils n'entrent pas dans le cadre de cette enquête de contrôle.

48 Par la suite, il s'est avéré que ce *test case* n'était pas représentatif pour les constatations de la partie générale de l'enquête, et ce pour différentes raisons : il s'agissait d'une instruction pénale en cours soumise à une procédure d'embargo ; les informations ont été fournies en réponse à une question très ciblée ; l'évaluation de la menace s'est principalement appuyée sur des éléments d'un autre dossier pénal ; la courte période qui s'est écoulée entre la demande d'évaluation et le début du procès ; le nombre limité de services d'appui ayant joué un rôle dans cette analyse de la menace.

n'est pas problématique en soi, à condition de garantir la traçabilité de ces échanges et leur accès pour point de contact central.

Autre constatation surprenante dans ce volet de l'enquête : les chiffres que l'OCAM a communiqués aux Comités étaient différents de ceux publiés ailleurs par la suite.

Malgré ces constatations, il est apparu clairement que le flux d'informations en provenance et à destination de la VSSE, de la police et du SPF Affaires étrangères était substantiel[49] et suivait une tendance à la hausse. Il n'en va pas de même pour l'Administration des douanes et accises, l'Office des étrangers et le SPF Mobilité, puisque les informations que ces services ont transmises à l'OCAM se limitaient à quelques (dizaines) de messages par an.

II.4.2. LES POINTS DE CONTACT CENTRAUX

Chaque service d'appui doit prévoir en son sein un point de contact central par lequel transite l'échange d'informations avec l'OCAM (art. 11 AR.OCAM).

L'OCAM a qualifié de très positifs les points de contact de la VSSE, du SGRS et du SPF Affaires étrangères (à savoir le coordinateur terrorisme).

L'Administration des douanes et accises[50], l'Office des étrangers[51] et le SPF Mobilité[52] sont toutefois dépourvus d'un point de contact clairement établi et reconnu en tant que tel. Bien que cette lacune ait été partiellement comblée par les experts détachés, les Comités estiment qu'il convient d'y remédier à court terme.

L'OCAM a également exprimé des réserves quant au « point de contact Police ». En effet, aucun point de contact central n'a jamais été désigné pour la police intégrée en tant que telle. Or il existe bel et bien un point de contact pour la police fédérale : le Point de contact national (PCN), mais qui fait apparemment office de simple boîte aux lettres, d'une part, pour la DGA (DAO)[53] (qui traite les informations administratives) et, d'autre part, pour la DJP/TERRO[54] (qui se

---

49 Voir néanmoins les constatations issues de l'enquête de contrôle relative à « Une visite de travail prévue à l'étranger par l'OCAM » (Chapitre II.5).

50 Lors du premier entretien, le point de contact désigné pour l'Administration des douanes et accises a indiqué qu'il n'était pas au courant de sa nomination.

51 L'Office des étrangers avait désigné le Bureau des Recherches au sein de la direction Inspection en tant que point de contact central. L'OCAM était toutefois convaincu que le point de contact était l'Administrateur général du service.

52 Le point de contact du SPF Mobilité n'apparaissait pas du tout dans la structure de l'organisation. La structure même de ce SPF, qui s'articule autour de trois piliers indépendants (transport terrestre, maritime et aérien), complique aussi le travail de ce point de contact. Sa contribution est donc très limitée. L'OCAM le reconnaît également et s'adresse en général directement à certaines personnes au sein de l'organisation.

53 La direction des opérations et de la gestion de l'information de la direction générale Police administrative de la police fédérale.

54 La direction de la lutte contre la criminalité contre les personnes – Terrorisme.

charge des informations judiciaires).[55] En outre, il convient de souligner l'implication limitée de la police locale. Étant donné l'organisation des flux d'informations au sein de la police intégrée, toutes les informations pertinentes devraient, en théorie, arriver à la DJP/TERRO et, par ce biais, à l'OCAM. Néanmoins, la direction de l'OCAM doutait que ce soit effectivement le cas et souhaitait une plus grande implication de la police locale en la matière.[56]

II.4.3. LES NOTIONS DE « RENSEIGNEMENTS » ET DE « PERTINENCE »

En vertu de l'article 6 L.OCAM, les services d'appui sont tenus de communiquer à l'OCAM tous les « renseignements » dont ils disposent dans le cadre de leurs missions légales et qui s'avèrent « pertinents » pour le fonctionnement de cet organe. Les Comités ont fait deux constatations relatives à cette obligation.

D'une part, contrairement à la police, les deux services de renseignement interprètent cette règle dans le sens où ils ne transmettent, en principe, aucune information brute, mais uniquement des informations traitées (voir également II.4.10 et II.4.11).

D'autre part, il s'est avéré que tous les services d'appui ne savent pas toujours exactement quand une information est « pertinente » ou non. Cette constatation s'applique, par exemple, au SPF Affaires étrangères, qui a tenté d'y remédier par une concertation régulière avec l'OCAM. La police intégrée semble elle aussi avoir rencontré quelques problèmes par le passé, surtout dans le volet « extrémisme ». Pour résoudre ces problèmes, elle a créé un groupe de travail avec des membres de l'OCAM, de la police judiciaire et administrative fédérale et de la Commission permanente de la police locale.

II.4.4. ACCUSÉS DE RÉCEPTION ET SUIVI DES DÉLAIS DE RÉPONSE

L'article 11 §§ 2 et 3 AR.OCAM prescrit que toute demande d'informations doit faire l'objet d'une confirmation automatique ou d'un accusé de réception qui fait

---

55 L'OCAM a plaidé pour que la DGA devienne le canal principal. Les Comités doutent de la faisabilité de cette piste, compte tenu de la confidentialité de certaines informations judiciaires, dont on peut difficilement admettre que les autorités judiciaires consentent qu'elles soient traitées simplement par le biais des canaux d'information de la police administrative.

56 Étant donné la structure de la police intégrée, la police fédérale n'a aucune autorité sur la police locale. L'OCAM a dès lors défendu le fait qu'il doit entretenir des liens directs avec les principaux corps de la police locale. Les Comités peuvent souscrire à cette méthode de travail, à condition que le point de contact de la police intégrée conserve une vision globale du flux d'informations en provenance et à destination de la police.

courir les délais de réponse réglementaires. Ce règlement ne semble toutefois pas être appliqué dans la pratique : ni l'OCAM ni les services d'appui n'utilisent un système de suivi élaboré. Ils partent du principe que ceux qui ne répondent pas à une demande ne disposent pas d'informations pertinentes.[57]

Par ailleurs, il n'a pas toujours été aisé de déterminer si les messages émanant de l'OCAM étaient envoyés « pour info » ou « pour action ».

II.4.5. LES DEUX PROCÉDURES D'EMBARGO

Afin de combattre la diffusion incontrôlée de certaines informations sensibles, la L.OCAM a instauré deux « procédures d'embargo » : l'une concernant les renseignements de nature judiciaire émanant des services de police (art. 11 L.OCAM) et l'autre à l'égard des renseignements fournis par la VSSE, le SGRS, l'Administration des douanes et accises et le SPF Affaires étrangères (art. 12 L.OCAM). Ces deux procédures doivent permettre que de tels renseignements ne soient pas repris tels quels dans des analyses ou que toutes les autorités ne reçoivent pas les analyses qui font mention de ces informations.

Dans les deux cas, le service fournisseur communique en principe les renseignements uniquement au directeur de l'OCAM. Dans la pratique, la direction de l'OCAM interprète toutefois ce règlement de la manière suivante : ces informations sensibles sont portées à la connaissance tant du directeur que du personnel chargé de la matière concernée.[58]

Ces dernières années, la procédure d'embargo décrite à l'article 12 L.OCAM n'a plus été utilisée. En revanche, il y a eu plusieurs dossiers d'embargo relevant de l'article 11 L.OCAM. Leur application n'a posé aucun problème.

Outre les articles 11 et 12 L.OCAM, la Loi sur la Fonction de police décrit également une procédure d'embargo dans ses articles 44/1 et suivants. Les Comités ont toutefois remarqué que le terme « embargo » est souvent utilisé sans qu'il soit clairement indiqué à quelle procédure il est fait référence. Il conviendrait de s'employer à dissiper toute confusion possible.

II.4.6. LA RÈGLE DU TIERS SERVICE OU LA RÈGLE DU PAYS TIERS

L'OCAM a déclaré que la « règle du tiers service » évolue, dans la pratique (internationale), vers une « règle du pays tiers », où des informations émanant de l'étranger sont transmises avec la mention « *for Belgian eyes only* ». Selon l'OCAM, cela laisse supposer que la méfiance originelle à l'égard de l'Organe de coordination se dissipe progressivement.

---

57 Cette méthode de travail a également été suivie dans le cadre du *test case*.

58 Voir également à cet égard COMITÉ PERMANENT R, *Rapport d'activités 2008*, 108-109.

De même, la VSSE et le SGRS n'ont rencontré aucun problème concernant l'application de la règle du tiers service dans la pratique. Comme l'OCAM devient de plus en plus connu à l'étranger, la plupart des pays semblent désormais transmettre leurs informations «*for Belgian eyes only*» et ne limitent donc plus l'exploitation des données à un service en particulier.

II.4.7. UNE PLATEFORME D'INFORMATION ET DE COMMUNICATION SÉCURISÉE

La plupart des services d'appui ont souligné le caractère particulièrement onéreux et peu performant du système d'information et de communication existant. En outre, il s'est avéré que de nombreuses connexions requises n'avaient toujours pas été établies. Cette situation concernait certains services d'appui (comme le SPF Mobilité), ainsi que d'autres destinataires des analyses de l'OCAM, comme les membres du Comité ministériel du renseignement et de la sécurité, et les différents «partenaires». Enfin, tous les services d'appui n'assuraient pas une surveillance permanente du système, et certains documents étaient envoyés par d'autres canaux (par exemple, par fax ou par porteur).

II.4.8. TRAITEMENT DES INFORMATIONS CLASSIFIÉES

Bien que dotés d'un officier de sécurité, tous les services d'appui ne pouvaient pas garantir le respect de l'ensemble des dispositions de la législation relative à la classification. Un incident de sécurité concernant des informations classifiées n'est dès lors pas exclu dans ces services.

L'utilisation des informations classifiées n'a posé problème que dans des cas exceptionnels: le cas échéant, les informations sont (partiellement) déclassifiées et peuvent être diffusées au sein du service d'appui. Si les informations ne peuvent pas être déclassifiées, il en va bien entendu tout autrement. Dans ce cadre, la police a relevé qu'il est parfois difficile d'utiliser de telles données de manière optimale, puisque la police ne dispose d'aucun système TIC (tel que la Banque de données nationale générale) qui satisfait aux normes réglementaires en la matière, et qu'elle est alors contrainte de se contenter d'une diffusion sur papier.

II.4.9. QUELQUES OBSERVATIONS SPÉCIFIQUES DE L'OCAM ET SUR L'OCAM

De manière générale, la direction de l'OCAM a déclaré que son fonctionnement a atteint sa vitesse de croisière. L'échange d'informations n'a plus rencontré de

problèmes notables. L'OCAM était convaincu d'avoir reçu toutes les informations pertinentes[59] et que ce flux d'informations continue de croître. L'Organe de coordination a dès lors constaté une amélioration de la relation de travail avec les services d'appui. Alors que les premières années, certains services considéraient l'OCAM plutôt comme un concurrent, ils seraient aujourd'hui conscients de sa plus-value, et ce grâce à ses analyses qui donnent une vision plus globale de certaines menaces.

Au moment où s'est déroulée l'enquête, le cadre de l'OCAM était presque entièrement pourvu[60] : dix des douze analystes et neuf des onze experts étaient opérationnels. En ce qui concerne les experts, tous les services d'appui ont accepté le principe selon lequel ils doivent détacher un collaborateur. Pourtant, ils ne considèrent pas ce détachement comme une véritable priorité, puisque la délégation d'un nouvel expert peut prendre un certain temps. Pendant longtemps, la VSSE et le SPF Affaires étrangères n'ont, par exemple, mandaté aucun expert. L'OCAM semblait toutefois très satisfait du niveau des personnes mises à disposition, malgré les difficultés que rencontrent certains services à désigner une personne rompue à tous les aspects de son administration. C'est par exemple le cas du SPF Mobilité, qui se subdivise en trois entités totalement différentes[61], et de l'Administration des douanes et accises, qui compte quatorze divisions fonctionnant de manière autonome. Quant à la police, il semble également difficile de représenter la « police intégrée », puisqu'elle englobe à la fois la police fédérale et chaque zone de police locale.

Enfin, les Comités permanents P et R ont estimé que les objectifs que l'OCAM s'est fixés s'avèrent très généraux et peu mesurables et il n'était pas clair si ces objectifs correspondaient aux attentes des différentes autorités concernées.

II.4.10. QUELQUES OBSERVATIONS SPÉCIFIQUES DE LA VSSE ET SUR LA VSSE

De manière générale, la VSSE a décrit sa relation avec l'OCAM comme positive.

Le flux d'informations en provenance et à destination de la VSSE[62] s'est accru en chiffres absolus et son contenu s'est considérablement amélioré. La VSSE qualifie toutefois la qualité des renseignements de très variable. Et le service de souhaiter que le niveau de l'analyse de la menace soit affiné et que les sources

---

59 En ce qui concerne le *test case*, l'OCAM a également estimé avoir reçu à l'époque toutes les informations pertinentes.

60 Malgré cet effectif, l'OCAM n'est pas en mesure d'organiser une permanence. En dehors des heures de service, seule la possibilité de rappeler du personnel est prévue.

61 Transport terrestre, maritime et aérien.

62 La VSSE ne transmet à l'OCAM que des analyses et des renseignements. Ce n'est qu'en cas de danger imminent qu'elle lui communique aussi les informations brutes.

soient mieux indiquées. Par exemple, il n'est pas toujours aisé de déterminer la provenance de certaines informations. La VSSE peut dès lors voir dans une analyse de l'OCAM une confirmation de ses constatations, alors que le travail de l'OCAM se fonde exclusivement sur les informations émanant de la VSSE elle-même. Il arrive également que les informations sur lesquelles l'OCAM se base proviennent simplement de sources ouvertes, sans que ce soit explicitement indiqué.

Autre point sensible : les contacts que l'OCAM entretient avec des services étrangers homologues en vertu de l'article 8, 3° L.OCAM. Lorsque ces services font partie d'un service de renseignement opérationnel[63], la VSSE juge ces contacts comme problématiques. En effet, elle considère les services homologues comme ses correspondants naturels et craint que les contacts de l'OCAM ne se limitent pas dans ces cas au département chargé des analyses de menace.

II.4.11. QUELQUES OBSERVATIONS SPÉCIFIQUES DU SGRS ET SUR LE SGRS

L'OCAM et le SGRS décrivent leurs rapports mutuels comme positifs. Aucun problème grave ne serait survenu.

À l'instar de la VSSE, le SGRS part du principe que l'OCAM a surtout besoin de données contextualisées et transmet donc principalement des produits finis (analyses). Il ne fournit des informations brutes qu'à titre exceptionnel (en cas de danger imminent). Cette méthode de travail a été mise sur pied en accord avec l'OCAM et est en vigueur depuis 2007.

Le SGRS a déjà recouru à plusieurs reprises à la possibilité de demander à l'OCAM d'analyser une menace donnée, et ce parce que le SGRS était confronté à une capacité d'analyse insuffisante en raison du départ de plusieurs de ses analystes pour l'OCAM.

Pour le SGRS, le rôle que l'OCAM joue en matière d'analyses des menaces qui pèsent sur les intérêts belges à l'étranger demeure un point sensible. C'est surtout la Division I du SGRS qui n'est pas convaincue de la compétence de l'OCAM pour effectuer des analyses sur les menaces à l'étranger. En outre, cette division se pose beaucoup de questions sur la qualité des analyses qui ont déjà été réalisées en la matière.

Le SGRS plaide pour des analyses plus globales et prospectives. Les évaluations se focaliseraient aujourd'hui trop sur la question de l'ordre public.

Contrairement à la VSSE, le SGRS estimait que l'OCAM mentionnait suffisamment ses sources dans ses analyses.

---

63 Pour des exemples, voir : COMITÉ PERMANENT R (éd.), *Fusion Centres Throughout Europe. All-Source Threat Assessments in the Fight Against Terrorism*, Intersentia, Antwerp, 2009, 220 p.

II.4.12. CONCLUSION GÉNÉRALE

Les deux Comités ont pu constater que les flux d'informations suivaient une courbe ascendante, tant d'un point de vue quantitatif que qualitatif. Plusieurs services d'appui devaient toutefois encore déployer des efforts considérables pour combler leur retard et fonctionner au même niveau.

D'une manière générale, les services d'appui se montrent positifs sur le fonctionnement de l'OCAM[64] et considèrent le travail de l'Organe de coordination comme une plus-value. Les Comités ont toutefois estimé que des améliorations sont encore possibles, et ce en répondant aux besoins spécifiques de certains services d'appui.

II.5. UNE VISITE DE TRAVAIL PRÉVUE À L'ÉTRANGER PAR L'OCAM

Début 2009, l'Organe de coordination pour l'analyse de la menace (OCAM) planifiait une brève mission en République démocratique du Congo (RDC). Cette mission fut toutefois annulée au tout dernier moment.

Par cette mission, l'OCAM souhaitait entre autres se faire une meilleure idée des conditions de sécurité en RDC et de la présence éventuelle de groupements radicaux, extrémistes ou terroristes. Des rencontres avec de nombreuses personnalités et instances publiques et privées avaient été prévues.

Selon l'OCAM, ce voyage était en partie motivé par le fait que le SPF Affaires étrangères omettait depuis longtemps de lui communiquer des renseignements concernant l'Afrique centrale, et ce en dépit de son obligation et initiatives concrètes de la part de l'OCAM. L'OCAM a en fait profité d'une occasion inopinée pour partir en RDC et développer ainsi sur le terrain ses connaissances de la région : il restait des places à bord d'un vol militaire qui partait dans la semaine. Les préparatifs de la mission ont donc été très courts.

La direction a désigné en son sein un analyste et un expert pour effectuer cette mission, et a contacté le SPF Affaires étrangères ainsi que le ministère et le cabinet de la Défense.[65]

Bien que les intéressés aient collaboré dans un premier temps, le cabinet du ministre des Affaires étrangères a soudain fait savoir que la mission ne pouvait pas avoir lieu à cette période en raison de son caractère trop délicat. Le directeur de l'OCAM a toutefois estimé que la véritable raison était ailleurs : un service d'appui n'aurait pas été satisfait de l'initiative par laquelle l'OCAM souhaitait opérer en toute indépendance.

---

64 Toutes les personnes interrogées ont qualifié l'évolution des flux d'informations de très positive à plutôt modérément positive. Cependant, des incidents isolés ont aussi été mentionnés.

65 L'OCAM aurait également informé le dirigeant du SGRS de cette mission.

Bien que cette mission à l'étranger ait été annulée, les Comités permanents P et R ont ouvert une enquête de contrôle conjointe. Ils souhaitaient vérifier si, de manière générale, l'accomplissement de telles missions s'inscrit dans le cadre ou découle des tâches confiées à l'OCAM par le législateur. Quant à la mission annulée, il s'agissait de déterminer si l'OCAM s'était suffisamment préparé et avait pris les mesures de précaution requises. Finalement, un troisième aspect, abordé au point II.5.1 ci-après, a également été mis en évidence en marge de cette enquête.

II.5.1. LE MANQUE D'INFORMATIONS CONCERNANT L'AFRIQUE CENTRALE

D'après l'OCAM, cette visite de travail a été organisée parce que depuis 2008, le SPF Affaires étrangères ne lui communiquait aucun renseignement sur cette région. Dès la mi-2009, ce service d'appui a fourni un volume sensiblement plus important de renseignements, sauf en ce qui concerne la situation en Afrique centrale, et ce en dépit de demandes ciblées. Par cette mission, l'OCAM souhaitait dès lors parfaire sa connaissance de la région afin de pouvoir réaliser des analyses précises. Selon le directeur, le fait que cette mission n'ait pas pu avoir lieu a, à l'époque, empêché l'OCAM de consolider sa position d'information à propos de la RDC.

Les Comités ont néanmoins dû constater que la mission avait simplement été déclenchée par une occasion fortuite (à savoir la mission militaire imminente en RDC). Aussi le caractère prétendument indispensable de la mission prévue s'est-il avéré peu convaincant.

Indépendamment de ce fait, les Comités ont toutefois estimé que l'attitude du SPF Affaires étrangères était inadmissible. Suite à cette enquête de contrôle, le ministre des Affaires étrangères est d'ailleurs intervenu pour remédier à cette situation. Il a été décidé, en concertation avec l'OCAM, d'organiser régulièrement des réunions d'information sur l'Afrique centrale. En outre, le ministre a procédé au détachement obligatoire d'un expert du SPF Affaires étrangères à l'OCAM.

Les Comités ont également déploré que le malaise entre l'OCAM et ses services d'appui n'ait été porté à leur connaissance que par accident et de manière indirecte. Cependant, l'OCAM a affirmé que son fonctionnement relatif à l'Afrique centrale a été hypothéqué pendant plus d'un an par un manque d'informations sur cette région de la part du SPF Affaires étrangères. Bien que cette problématique ait pu mettre en lumière un dysfonctionnement structurel, les Comités (qui ont précisément pour mission de formuler des recommandations visant à accroître l'efficacité) n'en ont pas été informés spontanément.

II.5.2. LA PRÉPARATION DU VOYAGE D'ÉTUDES

Les Comités permanents P et R ont également remarqué que la planification de la mission paraissait plutôt maigre. Les préparatifs ont consisté en une correspondance restreinte et un état des lieux général des desiderata. Il n'est nulle part question d'un programme au contenu détaillé ni d'un briefing de sécurité. De plus, les ministres de la Justice et de l'Intérieur n'ont pas été préalablement informés.

Les Comités ont estimé que le caractère délicat des visites officielles en Afrique centrale requiert un maximum de diplomatie et de prudence, certainement pour un organe tel que l'OCAM.

La préparation de cette mission aurait donc pu être plus minutieuse, tant du point de vue du contenu que sur le plan de la communication et de l'organisation. Outre un planning détaillé, l'OCAM aurait aussi dû prendre des mesures de précaution adaptées et spécifiques. De plus, une concertation avec les services de renseignement était indiquée. Enfin, les ministres de tutelle politiquement responsables, auraient dû être préalablement informés.

II.5.3. LES DIFFÉRENTS ASPECTS DE LA MISSION ET LE CADRE LÉGAL ET RÉGLEMENTAIRE

L'OCAM est chargé de réaliser des évaluations ponctuelles et stratégiques concernant les menaces extrémistes et terroristes susceptibles de porter atteinte à la sécurité de l'État, mais également « *aux intérêts belges et à la sécurité des ressortissants belges à l'étranger* » (art. 3 et 8, 1° et 2° L.OCAM). En outre, l'OCAM a pour mission « *d'assurer les relations internationales spécifiques avec des services étrangers ou internationaux homologues, conformément aux directives du Comité ministériel* » (article 8, 3° L.OCAM).

La Loi du 10 juillet 2006 relative à l'analyse de la menace n'a pas conféré d'autres missions à l'OCAM. Un voyage d'études ne peut dès lors en aucun cas être considéré comme une mission, mais seulement comme une plus-value éventuelle pour l'accomplissement des tâches énumérées à l'article 8 L.OCAM.

Ladite visite de travail s'inscrit-elle dans ce cadre légal et réglementaire ? La mission poursuivait une triple finalité, dont chaque aspect est traité séparément ci-après.

II.5.3.1. Un voyage d'études

Une partie de la mission pouvait certainement être considérée comme un voyage d'études. Dans la mesure où ces voyages ont pour but de permettre aux experts et aux analystes de consolider leurs relations professionnelles et leur expertise lors de forums organisés en Belgique ou à l'étranger, la volonté du directeur de

l'OCAM d'encourager autant que possible ces déplacements mérite d'être saluée. La qualité des analyses ne peut en effet que s'en trouver améliorée.

II.5.3.2. Contacts spécifiques avec des services homologues

La visite de travail planifiée incluait également une rencontre avec le délégué congolais du *Centre africain d'Étude et de Recherche sur le Terrorisme* (CAERT). Vu la mission du CAERT, l'OCAM considère ce centre comme un service homologue étranger dans le sens de l'article 8, 3° L.OCAM.

Bien que la mission décrite dans cet article doive encore faire l'objet d'une directive du Comité ministériel du renseignement et de la sécurité, l'OCAM a eu raison de ne pas attendre pour assumer cette tâche. Cette directive devrait toutefois être édictée dans les meilleurs délais afin de définir plus précisément les notions de « contacts spécifiques » et « services homologues ». À cet égard, les Comités ont attiré l'attention sur le fait que par cette mission, le législateur n'a pas souhaité que l'OCAM recueille lui-même des informations sur le terrain, à la place et aux côtés des services d'appui (voir aussi II.5.3.3) : « *S'il advenait que par ces contacts, l'OCAM acquiert connaissance d'informations ou de données, il est prévu qu'il les communique aux services ou aux autorités belges compétents pour traiter ces informations ou ces données en vertu de leurs missions légales.* »[66]

II.5.3.3. Le recueil de renseignements sur le terrain

Les Comités ont dû constater que la mission avait surtout pour objectif de mieux comprendre quelle était exactement la situation en RDC et d'obtenir davantage de renseignements en la matière. Les deux Comités ont toutefois insisté sur le fait que l'OCAM n'est ni compétent ni chargé de combler lui-même sur le terrain d'éventuelles lacunes dans les renseignements qui lui sont fournis.[67] Le législateur l'a clairement voulu. Les travaux parlementaires dans le cadre de la Loi du 10 juillet 2006 ne laissent planer aucun doute à cet égard : « *l'OCAM n'est pas un nouveau service de renseignement ou de police, il ne récolte pas d'informations en première ligne, mais évalue la menace sur la base des renseignements produits et fournis par les services participants* ».[68] Aussi l'OCAM occupe-t-il une position particulière dans le paysage de la sécurité en Belgique. Ses évaluations sont au fond le produit façonné des renseignements et informations qui lui sont fournis par les services d'appui. Ces produits doivent être considérés comme des « renseignements ». Or l'OCAM n'en est pas pour autant un service de renseignement. L'Organe de coordination doit dès lors

66 *Doc. parl.* Chambre 2005-06, n° 51 2032/001, 20.

67 L'OCAM ne dispose d'ailleurs pas non plus du savoir-faire ou des moyens requis pour se déplacer sur le terrain.

68 *Doc. parl.* Chambre 2005-06, n° 51 2032/001, 4. Voir dans le même sens : *Doc. parl.* Sénat, 2005-06, 3-1611/3, 3 et 12.

particulièrement veiller à ce que sa mission et son statut soient correctement perçus, afin d'éviter toute tension avec les services de renseignement ou tout incident diplomatique. Si l'OCAM estime que certains services d'appui manquent à leurs devoirs, il doit, par exemple, s'adresser aux Comités permanents P et R.

II.6. LA SÛRETÉ DE L'ÉTAT, LA LUTTE CONTRE LA PROLIFÉRATION ET LA PROTECTION DU PSE

II.6.1. ENQUÊTE DE SUIVI AU MOYEN D'UN CAS CONCRET

Le Comité permanent R a déjà enquêté à plusieurs reprises sur la problématique de la lutte contre la prolifération[69] et sur la protection du potentiel scientifique et économique (PSE)[70] par les services de renseignement. La VSSE[71] a un rôle important à jouer dans ces deux matières. Les renseignements que le service communique aux différents services publics et la manière dont ceux-ci utilisent ces données par la suite peuvent parfois avoir de lourdes conséquences (néfastes) pour les entreprises concernées. En outre, les intérêts qui prévalent en matière de lutte contre la prolifération ne coïncident pas toujours avec ceux qui priment pour la protection du PSE.

Les enquêtes de contrôle antérieures ont révélé que la VSSE abordait parfois cette matière avec une certaine nonchalance. Les autorités compétentes et le ministre de tutelle n'ont pas (toujours) été correctement informés. Aussi le Comité a-t-il entre autres souhaité une collaboration plus étroite entre les services de renseignement et les autres autorités concernées.

Par la présente enquête, le Comité permanent R voulait vérifier, au moyen d'un cas concret, comment la VSSE avait opéré ces dernières années (2006-2011) pour le suivi d'une entreprise belge spécialisée dans la fabrication de matériel de haute technologie. Le Comité a également vérifié si la VSSE avait tenu compte des recommandations précédentes dans le cadre de la lutte contre la prolifération et la protection du PSE. Cette enquête de contrôle n'a en tout cas pas permis de conclure que les lacunes constatées par le passé ont été comblées de manière significative.

---

69 Voir, par exemple, COMITÉ PERMANENT R, *Rapport d'activités 2005*, 16-35 et *Rapport d'activités 2008*, 40-54.

70 Voir, par exemple, COMITÉ PERMANENT R, *Rapport d'activités 2005*, 73 et *Rapport d'activités 2008*, 58-63.

71 Récemment, la Loi MRD a également élargi la mission de renseignement du SGRS au «*potentiel scientifique et économique en rapport avec les acteurs, tant personnes physiques que personnes morales, qui sont actifs dans les secteurs économies et industriels liés à la défense*» (art. 11 L.R&S).

II.6.2. CONSTATATIONS DE L'ENQUÊTE

II.6.2.1. Approche de la thématique par la VSSE

II.6.2.1.1. Intervention réactive *versus* proactive en matière de prolifération

La VSSE estime que son rôle en matière de prolifération est limité[72] en raison de la régionalisation de la compétence relative à l'octroi d'autorisations pour l'exportation d'armes. Pour la VSSE, c'est aux services chargés d'octroyer les licences qu'il appartient d'effectuer les premières vérifications et de déterminer quelles demandes d'autorisation lui sont soumises. En outre, la VSSE estime ne pas être compétente pour délivrer des avis aux autorités, mais seulement des renseignements. Le Comité ne partage pas cette opinion.

Le Comité a toutefois pu constater que récemment (à savoir dans son *Plan d'action 2011*), la VSSE a accordé un « suivi prioritaire actif » entre autres au commerce (intermédiaire) en matières premières, outils et technologies susceptibles de contribuer à la prolifération d'armes de destruction massive. La VSSE a prévu un « suivi actif » pour l'étude de certains « pays à risque », pour la sensibilisation ciblée du monde scientifique, industriel et académique, de même que pour l'élaboration d'un profil de cibles potentielles.

Le Comité a toutefois insisté sur le fait que la VSSE[73] ne dispose toujours pas des moyens matériels et humains nécessaires pour répondre à l'accroissement et à l'urgence du travail à réaliser dans la lutte contre la prolifération.

Par ailleurs, la VSSE a estimé qu'un accord avec l'Administration des douanes et accises est absolument nécessaire pour pouvoir mener une analyse stratégique globale de la prolifération en Belgique. Un tel accord doit définir des procédures claires et pratiques pour l'échange d'informations entre les deux administrations.[74]

II.6.2.1.2. Intérêts économiques *versus* intérêts en matière de sécurité

La VSSE est pleinement consciente que la lutte *contre* la prolifération et donc *pour* la sécurité a aussi son revers : des intérêts économiques sont également en jeu, dans le sens où il ne faut pas perdre de vue la compétitivité d'une

---

72 Certes, la VSSE n'a pas le pouvoir de contrôler ni d'empêcher *matériellement* les exportations sensibles, comme le lui demandent parfois certains services étrangers. Cette compétence est du ressort exclusif de l'Administration des douanes et accises.

73 En ce qui concerne le SGRS, le Comité permanent R a déjà déploré dans son *Rapport d'activités 2008* (p. 49) que ce service n'ait désigné qu'un seul analyste pour la section « *prolifération des armes de destruction massive et de leurs vecteurs* ». Cette situation n'a en aucun cas évolué de manière favorable.

74 La réunion qui s'est tenue en février 2010 dans le but de relancer le « Groupe de travail Prolifération » (réunissant des représentants des deux instances) a manqué son objectif. Les services de douane ne seraient plus tentés de conclure un protocole avec la VSSE depuis qu'ils ont conclu un accord avec les Régions.

entreprise.[75] Dans ce cadre, la VSSE a souligné les risques engendrés par la régionalisation de l'octroi de licences d'exportation : les différentes autorités compétentes appliquent des critères divergents lors de l'évaluation des demandes. À cet égard, les administrations régionales ont parfois tendance à privilégier les intérêts commerciaux, tandis que la CANPAN met l'accent sur la sécurité.

Le point de vue de la VSSE en la matière est clair : dans de tels dossiers, l'intérêt sécuritaire doit toujours être prioritaire, même si l'intérêt économique d'une entreprise est plus concret et plus immédiat. Le Comité partage cet avis.

Le Comité a néanmoins remarqué qu'une proposition circulait depuis longtemps déjà pour concilier ces deux intérêts antagoniques : une procédure de « *pré-avis* » pourrait être introduite lancée au sein de la CANPAN. Elle permettrait de limiter les préjudices commerciaux qu'une entreprise pourrait subir en raison d'avis négatifs qui ne sont émis qu'après une longue période (et parfois même après la fabrication du matériel). Cette piste a été examinée, mais les discussions ne sont pas (encore) terminées.

II.6.2.1.3. Lutte contre la prolifération *versus* la protection du PSE contre l'ingérence

Le Comité a pu constater que la VSSE s'intéressait à d'éventuelles tentatives d'« ingérence dans des processus décisionnels » par des puissances étrangères dans le cadre de la lutte contre la prolifération. Une telle ingérence peut représenter une menace pour le PSE.

Il est essentiel de disposer d'une bonne position d'information pour être en mesure d'évaluer correctement cette menace. La VSSE semble toutefois (encore) trop dépendante des informations (classifiées) transmises par des services étrangers, même en ce qui concerne des transactions suspectes menées en Belgique.

Un autre élément important à cet égard est « le couplage » nécessaire entre ces deux matières. Le Comité a précédemment proposé de réunir les analystes et les agents opérationnels actifs dans ces deux domaines afin d'établir une méthodologie commune pour pouvoir adopter un point de vue univoque au nom de la VSSE à l'égard des instances politiques compétentes. Cette proposition est restée sans suite par manque de moyens suffisants.

II.6.2.1.4. Collaboration au sein de la CANPAN

Il n'existe aucune directive interne relative au mandat du représentant de la VSSE à la CANPAN. Aussi le contenu des informations transmises à cette commission

[75] Par exemple, la VSSE a constaté que les mesures de contrôle renforcées et les sanctions internationales à l'égard d'un pays « proliférant » ont engendré une diminution du nombre d'exportations (sensibles) de l'entreprise à laquelle le Comité s'est intéressé pour son enquête de contrôle.

et leur mode de communication (par écrit ou par voie orale) sont-ils laissés à la libre appréciation de l'intéressé.

En outre, aucun protocole de coopération ne définit les modalités de communication et de protection des informations classifiées qui sont transmises à cette commission.

II.6.2.2. Le suivi de la société concernée

Le Comité a pu constater que la VSSE avait suivi attentivement plusieurs transactions de la société avec un ou plusieurs « pays proliférants » jusqu'à la mi-2008.

L'entreprise n'a de nouveau suscité l'intérêt qu'après une interruption de près de deux ans, et ce parce que des services de renseignement étrangers ont informé la VSSE de nouveaux projets de transactions avec des « pays sensibles ». Pendant toute la phase de collaboration bilatérale intense qui s'en est suivie, la VSSE a été pressée d'utiliser tous les moyens dont elle disposait pour s'opposer à l'exportation d'un matériel donné. Le suivi de ces transactions n'a été effectué qu'en fonction d'informations spontanément livrées par des services de renseignement étrangers. La VSSE a informé les ministres et les services fédéraux[76] et régionaux concernés de manière complète et régulière. Cependant, la « règle du tiers service » a parfois compliqué ce processus.

Le Comité a dû constater que le suivi de l'entreprise concernée était essentiellement « réactif » et ponctuel et ceci probablement à cause d'un manque de moyens.

Il faudra attendre la fin de l'année 2010 pour que la VSSE s'intéresse de manière plus globale à l'entreprise elle-même, à sa production et à sa clientèle, entamant ainsi une première recherche « proactive » de renseignements.

II.7. PLAINTE D'UN MEMBRE DE LA VSSE ET DE SON ÉPOUSE

A la mi-2010, le Comité a reçu une plainte d'un membre de la VSSE et de son épouse. Cette plainte portait sur quatre aspects.

---

[76] « *En vue d'améliorer l'efficacité de notre travail (…), nous avons renforcé les échanges d'informations avec les Administrations belges compétentes dans le domaine de la contre-prolifération, et avons informé de façon systématique le ministre de la Justice quant aux faits pertinents dont nous avions connaissance* », a déclaré l'AG de la VSSE. Le représentant de la VSSE à la CANPAN a également évoqué à plusieurs reprises des transactions de l'entreprise avec certains pays « sensibles ». Des informations concernant des commandes suspectes ont été communiquées à la commission.

Le plaignant avait reçu précédemment un « avertissement écrit » pour avoir dévoilé à un tiers sa qualité de membre de la VSSE. Il n'a pas accepté que cette note ait été conservée dans son dossier personnel.

Un autre aspect concernait le fait que le service Enquêtes de sécurité de la VSSE était au courant des déclarations que le plaignant aurait faites lors d'un entretien confidentiel avec un psychologue de la VSSE.

Au cours de cette même enquête de sécurité, des faits anciens, dont son épouse a été victime, auraient également été mis en doute d'une manière calomnieuse et diffamatoire.

Enfin, le plaignant a affirmé qu'un climat d'antisémitisme régnait au sein du département où il travaillait. Selon lui, l'affichage d'une coupure de presse et d'un dépliant dans un local de service de la VSSE était symptomatique de ce climat.

Le Comité a examiné chaque aspect de la plainte[77], tout en veillant à ne pas outrepasser son mandat légal. Certains éléments de la plainte ne relevaient effectivement pas de ses compétences. Ainsi, les plaignants ont qualifié les propos des enquêteurs de la VSSE de « calomnieux et diffamatoires ». Or il s'agit d'une qualification pénale sur laquelle seul un tribunal peut statuer. Cependant, le Comité permanent R est toujours compétent pour constater la matérialité des faits et les apprécier à la lumière de ses propres compétences. Il va de même pour l'avertissement écrit figurant dans son dossier personnel : bien que n'étant pas un organe de recours en matière disciplinaire, le Comité est en droit d'examiner si la VSSE ne porte pas atteinte aux droits que la Constitution et la loi confèrent aux membres de son personnel et si une pratique déterminée peut avoir un impact sur l'efficacité du service. De ces deux points de vue, le Comité peut également analyser le déroulement des enquêtes de sécurité, sans se substituer pour autant à l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité.

II.7.1. L'« AVERTISSEMENT ÉCRIT » DANS LE DOSSIER PERSONNEL

Malgré que le plaignant niait avoir divulgué sa qualité de membre de la VSSE à un tiers sans motif professionnel, et en dépit de l'arrêt de la procédure disciplinaire, la VSSE a décidé de lui donner un « avertissement écrit ». Cet avertissement a été consigné dans le dossier personnel du plaignant.

Le Comité a estimé qu'une telle méthode n'était pas admissible dans l'état actuel de la réglementation. En effet, cette possibilité n'est pas prévue dans le statut du personnel du 13 décembre 2006. Du reste, la conservation de notes

[77] En vertu de l'article 3, alinéa 3 de la Loi du 11 décembre 1998 relative à la classification, l'enquête a été temporairement suspendue à la suite du recours que le membre du personnel concerné a introduit contre le retrait de son habilitation de sécurité.

contenant des éléments défavorables sans la moindre limite de temps est susceptible de porter un préjudice grave à la carrière de certaines personnes.

II.7.2. LE SECRET PROFESSIONNEL ET L'ENQUÊTE DE SÉCURITÉ

En présence de son supérieur, le plaignant a fait certaines déclarations devant un psychologue de la VSSE.[78] Par la suite, ces données – qui portaient sur un problème de fonctionnement grave au sein de son service – ont été utilisées dans une enquête de sécurité relative au plaignant. Le supérieur en avait effectivement informé sa hiérarchie. Le Comité a insisté sur le fait que si le psychologue est bel et bien lié par le secret professionnel[79], il n'en va pas de même pour le supérieur concerné. Il pouvait dès lors communiquer ces déclarations à sa hiérarchie et faire ainsi passer l'intérêt général de son service avant l'intérêt spécifique de son collaborateur.

II.7.3. L'ENTRETIEN FAISANT SUITE À L'ENQUÊTE DE SÉCURITÉ

Afin de vérifier la fiabilité du plaignant, les enquêteurs de sécurité ont abordé plus en détail les anciens faits d'agression commis sur la personne de son épouse. Lorsque le plaignant a eu l'impression que les enquêteurs minimalisaient ces faits, il a refusé de continuer à collaborer à l'entretien.

Le Comité permanent R a souligné que l'enquête de sécurité avait pour principal objectif de contrôler la véracité des déclarations du plaignant. Aussi les enquêteurs devaient-ils vérifier si et pourquoi son épouse avait déposé plainte à l'époque. En revanche, ils n'auraient pas dû réagir à la qualification pénale que la victime a estimé devoir donner aux faits.

---

78 Ce psychologue faisait partie de l'équipe d'encadrement psychologique et social de la VSSE. Tenant compte de l'impact des responsabilités et des contraintes psychologiques et sociales assumées par les agents de la VSSE, l'A.R. du 13 décembre 2006 a institué une telle équipe.

79 L'article 143 de l'A.R. du 13 décembre 2006 s'énonce comme suit: «*L'équipe d'encadrement intervient soit à la demande du membre du personnel lui-même, soit à la demande du chef hiérarchique ou d'un collègue et, dans ce cas, en accord avec le membre du personnel concerné. Les membres de l'équipe d'encadrement psychologique sont tenus au secret professionnel. Ils travaillent en dehors de tout dossier du personnel et en garantissent l'anonymat. Ils ne communiquent en aucun cas à la hiérarchie le contenu des entretiens sauf autorisation écrite du membre du personnel concerné.*».

II.7.4. LES DOCUMENTS INCRIMINÉS

Une coupure de presse et un dépliant exprimant un point de vue dans le conflit israélo-palestinien ont été affichés dans un local de service. Cet acte a été posé à l'insu du chef de service.

Le Comité a estimé que les documents n'étaient pas révélateurs d'un prétendu climat antisémite. En revanche, le Comité était d'avis qu'ils n'avaient pas leur place dans un local de la VSSE car contraire au devoir de discrétion et de neutralité que les agents de ce service sont tenus de respecter.

Les agents des services extérieurs de la VSSE jouissent en principe de la liberté d'expression, mais ils doivent s'abstenir en toutes circonstances de manifester publiquement leurs opinions politiques et de se livrer publiquement à des activités politiques.[80] Ces principes sont régulièrement rappelés aux agents concernés. Ils ont été repris dans un projet de vade-mecum administratif/code de déontologie qui était toujours en cours de préparation au moment de la clôture de cette enquête de contrôle.

II.8. LA REPRÉSENTATION BELGE À DES RÉUNIONS INTERNATIONALES EN MATIÈRE DE TERRORISME

Les Comités permanents P et R ont constaté que les services de police et de renseignement belges et l'OCAM participaient régulièrement à des réunions consacrées à la lutte contre le terrorisme. La question s'est dès lors posée de savoir s'il existait une quelconque coordination entre ces services et si, en d'autres termes, les exigences d'efficacité et d'efficience étaient respectées. Il va de soi que l'OCAM, la police fédérale, la VSSE et le SGRS, en tant que principaux acteurs de la lutte contre le terrorisme et l'extrémisme, étaient concernés par cette enquête. Mais les Comités ont également interrogé les autres services d'appui de l'OCAM : les corps de la police locale, l'Administration des douanes et accises du SPF Finances, l'Office des étrangers du SPF Intérieur, le SPF Mobilité et Transport, et le SPF Affaires étrangères.[81] Le parquet fédéral et le Centre de crise du gouvernement sont eux aussi régulièrement représentés aux réunions internationales. Ces instances n'ont toutefois pas fait l'objet de la présente enquête, puisque les Comités ne sont pas compétents pour les contrôler.

Cette enquête a porté sur le thème des réunions ou groupes de travail (stratégiques ou opérationnels) internationaux dans le cadre de la lutte contre le terrorisme et l'extrémisme, ainsi que sur les personnes qui y ont participé pour la

80 Article 12 AR 13 décembre 2006.

81 Certains services et ministres n'ont répondu qu'après plusieurs lettres de rappel. Les Comités n'ont reçu aucune réponse des ministres des Finances et de l'Intérieur.

Belgique. Les Comités ont également examiné si les acteurs belges se concertaient préalablement sur l'ordre du jour et sur les positions qui seraient ou devaient être prises au nom de la Belgique. Ils ont en outre étudié la manière dont les résultats, les comptes-rendus, les accords ou les positions relatifs à la réunion étaient diffusés entre les services participants et/ou non participants. Enfin, les acteurs concernés ont été invités à donner leur vision de la composition de la délégation à certains forums.

L'enquête a confirmé que les services de police et de renseignement belges et l'OCAM, ainsi que le SPF Affaires étrangères, participent à de nombreuses réunions internationales en matière de lutte contre le terrorisme et/ou l'extrémisme. Les informations recueillies offraient aussi une vision quelque peu kaléidoscopique de qui était présent et à quelle(s) réunion(s). Il arrive que différents services soient simultanément représentés à un même forum ou à une même réunion.[82] Il n'est pas toujours clair de déterminer si le ou les services présents représentent la Belgique ou se représentent eux-mêmes. Enfin, il est apparu qu'aucun service ne disposait d'une vision complète des forums internationaux existants.

Bien que toutes les instances se soient préalablement concertées d'une manière ou d'une autre en préparation des réunions internationales (y compris avec des services qui ne participaient pas aux réunions), les Comités ont pu constater qu'aucune méthode de travail ne décrivait clairement comment préparer les réunions et comment déterminer la position que la Belgique devait adopter le cas échéant.[83] Les Comités ont constaté que le mode de fonctionnement était informel et non structuré, si bien qu'il était impossible de déterminer avec certitude si tous les services concernés avaient préalablement

---

82 Certains forums sont naturellement réservés à un seul acteur. Ainsi, la VSSE affirme qu'il existe deux types de réunions : les réunions des services de renseignement, qui obéissent aux règles de base du monde du renseignement (à savoir le « *need to know* » et la « règle du tiers service »), et les réunions mixtes à la fois destinées aux services de renseignement et aux autres services compétents en matière de terrorisme et d'extrémisme. Ces dernières ont lieu principalement dans le cadre de l'Union européenne.

83 La police fédérale a déclaré à cet égard qu'il n'existe que peu ou pas de mécanismes structurels spécifiques pour discuter de la participation aux réunions et des positions qui doivent être prises. En règle générale, un accord ponctuel est recherché si nécessaire. Dans de nombreux cas, une certaine harmonisation est trouvée au sein de forums nationaux, tels que le Collège du renseignement et de la sécurité.
La VSSE a déclaré que les participants belges, ainsi que les services qui ne participent pas, se rencontrent avant ces réunions et échangent leurs points de vue. Ainsi, le programme relatif à la lutte contre le terrorisme et l'extrémisme a été élaboré dans la perspective de la présidence belge du Conseil Justice et Affaires intérieures de l'Union européenne (JAI), en concertation avec toutes les instances concernées.
Pour les réunions qui se tiennent au niveau des Nations Unies et de l'Union européenne, le SPF Affaires étrangères organise des réunions préalables, où la position de la Belgique est constamment discutée. Le SPF Justice, le SPF Intérieur, la police fédérale, la VSSE, le SGRS et l'OCAM participent à ces réunions.

exposé leur point de vue et si une « position commune » au niveau belge avait été adoptée lors des réunions.

La diffusion des résultats des réunions s'effectue elle aussi sur un mode informel et non structuré, sans que l'on puisse avoir la certitude que tous les services concernés recevaient le *feedback* requis.

II.9. PLAINTE RELATIVE À LA COMMUNICATION D'INFORMATIONS PAR LE SGRS À LA POLICE FÉDÉRALE

Après avoir échoué lors de sa formation de base, un candidat volontaire de carrière auprès des Forces armées profère des menaces concrètes à l'encontre de l'armée belge devant ses collègues. Sa hiérarchie en informe le SGRS. Le service de renseignement militaire mène alors une enquête et en arrive à la conclusion qu'il existe effectivement une menace potentielle. Ces informations sont ensuite communiquées à la police.

Lorsque, plus tard, l'intéressé se porte candidat pour une fonction au sein de la police fédérale, il échoue au test de personnalité. Selon lui, cet échec est la conséquence de la transmission de ces informations par le SGRS à la police. Il affirme à cet égard être victime de discrimination en raison de son origine ethnique.

Le Comité permanent R est toutefois arrivé à la conclusion que le SGRS a agi conformément à sa mission légale (article 11 L.R&S) et que la police, eu égard à ses compétences, était habilitée à avoir connaissance de ces informations (articles 19 L.R&S et 44/1 de la Loi sur la Fonction de police). Il est clairement apparu que les renseignements n'ont pas été transmis dans le but de communiquer à la police un élément d'appréciation concernant la personnalité du plaignant dans le cadre d'une procédure de sélection. Le SGRS n'a dès lors pas porté atteinte aux droits de l'intéressé et le Comité permanent R n'a constaté aucun traitement discriminatoire.

II.10. LA POSSIBILITÉ DE PÉNÉTRER DANS DES LIEUX PRIVÉS LORS DE MISSIONS DE PROTECTION

Les officiers de protection de la VSSE ont pénétré dans le jardin privé d'un immeuble à appartements afin d'explorer une voie d'évacuation. Ce jardin jouxtait un lieu où ils étaient chargés de protéger un haut dignitaire. Le contrôle s'est effectué en présence de collaborateurs du service privé de sécurité du lieu concerné, mais sans que les propriétaires des appartements en soient informés.

Deux occupants ont déposé plainte. Ils se demandaient si les officiers de protection avaient le droit de s'introduire à tout moment dans leur propriété privée.[84]

La Loi du 30 novembre 1998 organique des services de renseignement et de sécurité stipule que les agents de la VSSE ne peuvent pénétrer dans des lieux privés «*à l'insu du propriétaire et sans son consentement*»[85] que sous certaines conditions. Cette compétence spécifique ou exceptionnelle ne concerne toutefois que l'exercice de leurs missions de renseignement. Cette compétence ne peut pas être utilisée dans le cadre de missions de protection. Les officiers de protection de la VSSE disposent certes de certaines compétences de police administrative comparables à celles des services de police: ils sont armés et peuvent faire usage de la violence lorsque la vie ou l'intégrité physique de la personne protégée est menacée. Cependant, à moins qu'il ne s'agisse d'un domaine abandonné[86], ils ne peuvent pas pénétrer dans des lieux privés sans autorisation.

À la suite de l'incident, le service privé de sécurité et le représentant des occupants de l'immeuble à appartements sont parvenus à un accord, selon lequel ce dernier serait préalablement informé de toute inspection par la VSSE.

II.11. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ POSÉS EN 2011 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2011

Cette section énumère et situe brièvement toutes les enquêtes que le Comité permanent R a démarrées en 2011, ainsi que les enquêtes sur lesquelles il a continué de travailler au cours de cette même année, mais qui n'ont pas encore pu être clôturées.

II.11.1. ENQUÊTE RELATIVE AUX ACTIVITÉS DU SGRS EN AFGHANISTAN

Les troupes belges font partie de l'ISAF, la force internationale de maintien de la paix en Afghanistan. La majeure partie du contingent belge est basée dans la capitale afghane Kaboul et se compose d'une compagnie de protection sur l'aéroport international. À Kunduz, la Belgique appuie les équipes provinciales

84 Le jardin de l'immeuble à appartements était grevé d'une servitude de passage en cas d'extrême urgence et d'évacuation du bâtiment voisin. Toutefois, cette servitude ne s'étendait pas à d'éventuels contrôles préalables de l'issue de secours.

85 Voir art. 18/2, 18/4 et 18/5 L.R&S.

86 Article 24 L.R&S.

de reconstruction et fournit également des *Operational Mentoring and Liaison Teams*. Enfin, à Kandahar, la Belgique apporte sa contribution en engageant des avions F-16.[87]

Il est ressorti d'un briefing du SGRS concernant la situation sur place que de nombreuses méthodes de renseignement (HUMINT, OSINT, IMINT, SIGINT…) étaient mises en œuvre par ce service et qu'il collaborait étroitement avec des services de renseignement d'autres pays. Afin de se faire une idée globale (et éventuellement d'élaborer un cadre de référence), le Comité a décidé d'ouvrir une enquête de contrôle *« concernant le rôle du SGRS dans le suivi de la situation en Afghanistan »*. Cette enquête s'est intéressée à des thèmes tels que le personnel déployé, les méthodes de renseignement utilisées, la collaboration avec des services de renseignement étrangers et la transmission de renseignements.

Le Comité permanent R a l'intention de clôturer cette enquête de contrôle à l'automne 2012.

II.11.2. SUIVI D'UN TERRORISTE CONDAMNÉ PENDANT ET APRÈS SA DÉTENTION EN BELGIQUE

Selon un article du journal britannique *The Independent*[88], un agent d'un service secret britannique aurait exercé des pressions sur un terroriste condamné en Belgique et détenu à la prison de Forest afin qu'il travaille pour eux. Cette information a été abondamment relayée par la presse belge. L'intéressé aurait été transféré illégalement en Grande-Bretagne et « séquestré » dans une base secrète, où il aurait été interrogé et contraint de collaborer.

Selon son avocat, cette opération n'a pas pu avoir lieu sans être approuvée, entre autres par les services de renseignement belges, ni à leur insu.

Le Comité permanent R a dès lors décidé d'ouvrir une enquête de contrôle *« sur le suivi éventuel d'un particulier (M.J.) par la VSSE et le SGRS pendant et après sa détention en Belgique »*. Les résultats de cette enquête de contrôle ont été transmis au printemps 2012 à la Commission de suivi du Sénat et aux ministres compétents.

II.11.3. ANALYSES PONCTUELLES DE L'OCAM DANS LE CADRE DE VISITES DE PERSONNALITÉS ÉTRANGÈRES

En octobre 2010, le Comité permanent R a ouvert une enquête conjointe avec le Comité permanent P, *« sur l'évaluation de la menace effectuée par l'OCAM*

87 A la fin 2011, le gouvernement belge a décidé de commencer le retrait des soldats belges à partir de 2012. Les derniers militaires seraient partis en 2014.

88 *The Independent*, 23 juillet 2010.

relative aux personnalités étrangères lors des visites en Belgique». Les chiffres mentionnés par l'OCAM dans son rapport annuel laissaient en effet supposer que de telles analyses ponctuelles représentent un investissement colossal en temps et en moyens pour l'organe de coordination.

Le rapport final était prévu en 2011. Toutefois, en raison de la réponse tardive de l'OCAM, les devoirs d'enquête n'ont pas pu être finalisés. Les résultats de l'enquête de contrôle sont attendus en 2012.

II.11.4. AVIS ÉMIS PAR LA VSSE DANS LE CADRE DE DEMANDES DE NATURALISATION

L'«affaire Belliraj»[89] a entre autres soulevé la question de savoir de quelle manière la Sûreté de l'État serait intervenue dans la naturalisation de l'intéressé. Les membres de la Commission sénatoriale de suivi sont eux aussi revenus en détail sur cet élément lors de la discussion sur l'enquête de contrôle en novembre 2010.

Dans le prolongement de cette discussion, le président du Sénat de l'époque a demandé au Comité permanent R d'ouvrir une enquête de contrôle sur «*la manière et les circonstances dans lesquelles la VSSE examine et traite les demandes de renseignements introduites dans le cadre des procédures d'acquisition de la nationalité belge*». Les résultats de cette enquête, qui comporte un volet juridique, descriptif et quantitatif, ont été transmis à la Commission de suivi au printemps 2012.

II.11.5. SUIVI PAR CERTAINS SERVICES DE RENSEIGNEMENT ÉTRANGERS DE LEUR DIASPORA EN BELGIQUE

La Belgique semble exercer un grand pouvoir d'attraction sur les services de renseignement étrangers. La présence des institutions européennes et de l'OTAN sur le territoire explique en partie cet attrait. Les services de renseignement étrangers sont également très intéressés par la recherche de pointe menée dans des programmes spatiaux, l'industrie de l'armement et la politique énergétique en Belgique. Certains services de renseignement étrangers suivent aussi de près les activités de leurs communautés de migrants (leur diaspora) en Belgique.

À la demande du président du Sénat de l'époque, le Comité permanent R a ouvert, en juillet 2011, une enquête de contrôle «*sur la manière dont les services de renseignement belges suivent les éventuelles activités déployées sur le territoire*

[89] COMITÉ PERMANENT R, *Rapport d'activités 2009*, 30-40.

belge par les services de renseignement de pays d'immigration importants situés hors de l'Union européenne».

Dans le courant de l'année 2011, le Comité a posé différentes questions à la VSSE et au SGRS. Les résultats de l'enquête de contrôle sont attendus dans le courant de l'année 2012.

II.11.6. LE DROIT À L'ASSISTANCE SYNDICALE DANS LE CADRE D'ENQUÊTES DE SÉCURITÉ

En octobre 2011, le Comité permanent R a été interrogé sur le droit éventuel d'un délégué syndical d'assister un militaire lors d'un entretien mené dans le cadre d'une enquête de sécurité. Le Comité permanent R a ouvert une enquête de contrôle à la suite de cette demande.

Le militaire concerné a toutefois interjeté appel en décembre 2011 auprès de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. Le Comité permanent R a dès lors suspendu l'enquête de contrôle en exécution de l'article 3 L.Organe de recours. L'Organe de recours a rendu sa décision début 2012 et l'enquête a pu reprendre son cours.

CHAPITRE III.
CONTRÔLE DES MÉTHODES PARTICULIÈRES DE RENSEIGNEMENT

L'article 35 § 1er, 1° L.Contrôle stipule que le Comité doit consacrer, dans son rapport d'activités annuel, *« une attention spécifique aux méthodes spécifiques et exceptionnelles de recueil de données, telles qu'elles sont visées dans l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité [et] à l'application du chapitre IV/2 de la même loi »*.[90] Ce chapitre traite dès lors de l'utilisation des méthodes particulières de renseignement par les deux services de renseignement et de la manière dont le Comité permanent R exerce son rôle juridictionnel à cet égard. Ce rapport est un condensé des deux rapports semestriels que le Comité a rédigés pour la Commission de suivi du Sénat.[91]

III.1. QUELQUES POINTS D'ATTENTION SPÉCIFIQUES

III.1.1. CONCERTATIONS INFORMELLES AVEC LES ACTEURS CONCERNÉS

Le Comité permanent R a organisé à intervalles réguliers une concertation sur l'application de la Loi MRD, et ce avec la VSSE, le SGRS et la Commission BIM.

Avec la Commission BIM, les aspects suivants ont notamment été discutés :

- la circulation des informations et des documents de la Commission BIM vers le Comité permanent R ;
- la permanence de la Commission BIM pendant les périodes de congés, vu l'absence de suppléants ;
- le retard dans l'envoi au Comité des autorisations pour l'utilisation des méthodes spécifiques dans les cas où la Commission BIM a demandé un complément d'informations aux services de renseignement ;

---

90 Pour une analyse des méthodes particulières de renseignement et du contrôle exercé sur celles-ci, voir : COMITÉ PERMANENT R, *Rapport d'activités 2010*, 49-61 en W. VAN LAETHEM, D. VAN DAELE et B. VANGEEBERGEN (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, 299 p.

91 Art. 35 § 2 et 66*bis* § 2, alinéa 3, L.Contrôle. Les deux rapports ont été transmis respectivement à la mi-septembre 2011 et début février 2012 à la Commission de suivi.

– la problématique de la mise en œuvre de méthodes spécifiques pour l'identification d'utilisateurs de moyens de communication, à la lumière de l'exigence de subsidiarité (voir aussi III.2.2.1 et III.3.2.6) ;
– la manière dont les membres de la commission sont informés par notification dans le cas où une méthode est autorisée après avis conforme du président de la Commission BIM saisie en extrême urgence.

Les points repris ci-après ont été abordés avec les services de renseignement :
– les conditions auxquelles le service d'Enquêtes du Comité permanent R peut obtenir des services de renseignement un complément d'informations de manière informelle avant l'éventuelle saisine par le Comité ;
– les conséquences éventuelles pour le travail des services de renseignement ou la réaction de ceux-ci lorsque le Comité constate que la VSSE ou le SGRS mettent en œuvre chacun de leur côté une ou des méthode(s) particulière(s) à l'égard d'une même cible.

III.1.2. LES « RÉSULTATS OBTENUS » PAR LA MISE EN ŒUVRE DE MÉTHODES PARTICULIÈRES

L'article 35 § 2 L.Contrôle stipule que « *le cas échéant, les résultats obtenus* » doivent être repris dans le rapport semestriel que le Comité est tenu de transmettre à la Commission de suivi. Vu la complexité et la sensibilité d'un tel rapport dans un contexte du renseignement, le Comité développe actuellement une méthodologie afin d'évaluer l'appréciation donnée par les services de renseignement des résultats qu'ils ont obtenus. Cet instrument doit permettre de faire utilement rapport (c'est-à-dire en fonction des recommandations relatives à l'efficacité et à la légalité du fonctionnement des services) sur la mise en œuvre des méthodes particulières.

III.1.3. ARRÊT DE LA COUR CONSTITUTIONNELLE

La Cour constitutionnelle s'est prononcée le 22 septembre 2011 sur les deux requêtes en annulation de diverses dispositions de la Loi MRD.[92] Un seul article de loi a *in fine* été annulé : l'article 2 § 3 L.R&S, qui crée une obligation de notification passive, doit être adapté sur deux points. D'une part, les personnes morales doivent également être informées lorsqu'elles font l'objet d'une méthode

[92] Par *l'Orde van Vlaamse balies* (*M.B.* 16 août 2010) et par la *Liga voor Mensenrechten* (*M.B.* 27 octobre 2010). Un extrait de l'arrêt a été publié au Moniteur belge du 12 décembre 2011.

particulière. D'autre part, le service de renseignement concerné doit informer de sa propre initiative une personne (morale) dès que la Commission BIM l'estime possible.

III.2. DONNÉES CHIFFRÉES RELATIVES AUX MÉTHODES SPÉCIFIQUES ET EXCEPTIONNELLES

En 2011, 831 autorisations[93] ont été accordées pour les deux services de renseignement pour l'utilisation des méthodes particulières de renseignement : 764 pour la VSSE (dont 731 spécifiques en 33 exceptionnelles) et 67 pour le SGRS (dont 60 spécifiques en 7 exceptionnelles). Lors de l'interprétation de ces chiffres, il convient de ne pas perdre de vue les deux éléments suivants :

- en principe, un seul type de méthode particulière est autorisée par « autorisation » (une observation *ou* une inspection, pas les deux). Il existe une exception à cette règle : dans une seule et même autorisation, un service de renseignement peut être autorisé à recevoir des données d'appel ou de localisation et ensuite de procéder à l'identification des informations ainsi obtenues (voir III.2.2.1) ;
- plusieurs cibles peuvent être visées par méthode autorisée (telles que des personnes, organisations, lieux, objets, moyens de communication…). Une méthode peut dès lors avoir davantage de répercussions qu'une autre sur la charge de travail des services de renseignement et sur la vie privée du citoyen.

Les chiffres ci-dessous sont repris séparément pour les deux services. Certes, les deux services se sont vu conférer les mêmes compétences, mais leurs missions sont tellement différentes qu'on ne peut tirer que peu d'enseignements d'une comparaison chiffrée entre eux.

Trois grandes rubriques sont établies pour chaque service : des données chiffrées sur les méthodes spécifiques, sur les méthodes exceptionnelles et sur les menaces visées par les différentes méthodes ainsi que les intérêts à protéger.

93 Dans la loi, les termes « autorisation » et « décision » sont souvent utilisés indifféremment. Par souci de lisibilité, le premier terme sera réservé, dans ce rapport, à toutes les méthodes particulières autorisées par le dirigeant du service ou par le ministre, tandis que le terme « décision » sera réservé au contrôle juridictionnel exercé par le Comité permanent R.

III.2.1. AUTORISATIONS RELATIVES AU SGRS

III.2.1.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	7
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	0
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	0
Prise de connaissance des données d'identification de moyens de communication électroniques ; réquisition du concours d'un opérateur ; ou l'accès direct à des fichiers de données	23
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	17
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	13
TOTAL	60[94]

III.2.1.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	0
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	0
Création ou recours à une personne morale fictive	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	0
Collecte de données concernant des comptes bancaires et des transactions bancaires	5
Intrusion dans un système informatique	0
Ecoute, prise de connaissance et enregistrement de communications	2
TOTAL	7

[94] Dans trois cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, médecin ou journaliste professionnel.

III.2.1.3. Les intérêts et les menaces justifiant le recours à des méthodes particulières

Le SGRS est autorisé à utiliser les méthodes spécifiques et exceptionnelles dans le cadre de trois missions, qui elles-mêmes comprennent des intérêts spécifiques à protéger :

- la mission de renseignement orientée vers les menaces visant, entre autres, l'intégrité du territoire national, les plans de défense militaires et le potentiel scientifique et économique en rapport avec la défense (art. 11, 1° L.R&S) ;
- la mission en matière de sécurité militaire qui vise par exemple le maintien de la sécurité militaire du personnel relevant de la Défense, des installations militaires et des installations militaires et des systèmes informatiques et de communications militaires (art. 11, 2° L.R&S) ;
- la protection des secrets militaires (art. 11, 3° L.R&S).

INTÉRÊT PROTEGÉ	NOMBRE
Mission de renseignement	38
Sécurité militaire	8
Protection de secrets	19

Contrairement à la VSSE, les menaces auxquelles le SGRS peut ou doit être attentif ne sont pas définies dans la loi. Cependant, ce service mentionne systématiquement quelle menace est visée dans ses autorisations. Une telle transparence mérite d'être soulignée. En ce qui concerne la mise en œuvre de méthodes particulières, la lutte contre l'espionnage constitue la toute première priorité du service de renseignement militaire.

NATURE DE LA MENACE	NOMBRE
Espionnage	54
Terrorisme	10
Extrémisme	3

III.2.2. AUTORISATIONS RELATIVES À LA VSSE

III.2.2.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	89
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	0
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	4
Prise de connaissance des données d'identification de moyens de communication électroniques ; réquisition du concours d'un opérateur ; ou l'accès direct à des fichiers de données	355
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	237
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	46
TOTAL	731[95]

Ce tableau fait clairement apparaître que la plupart des méthodes mises en œuvre par la VSSE concernent l'identification (peu intrusive) de l'abonné ou de l'utilisateur d'un numéro de téléphone ou de GSM. Cela concerne 355 autorisations permettant une identification, dans le cadre de laquelle plusieurs numéros sont le plus souvent repris dans une seule autorisation. En l'espèce, les 355 autorisations se rapportaient à 1892 numéros. Cependant, le nombre d'identifications effectivement réalisées est encore plus élevé. En accord avec la Commission BIM le Comité permanent R a en effet approuvé une méthode de travail qui permet au dirigeant d'un service de renseignement d'autoriser, dans une seule et même autorisation, le repérage *et* l'identification de données d'appel. Le dirigeant du service n'est dès lors plus obligé d'accorder successivement deux autorisations quasi identiques dans un même dossier. Les deux méthodes sont en effet très liées : les données d'appel ne sont utiles que si elles peuvent être attribuées à une personne ou une organisation déterminée. Il est vrai que cette méthode de travail implique que le Comité n'a pas une vue automatique sur le nombre d'identifications effectuées.

Le Comité exige cependant que le service de renseignement identifie uniquement les numéros via un opérateur, si ces numéros ne peuvent pas être

[95] Dans neuf cas, l'autorisation concernait une catégorie professionnelle protégée, c'est-à-dire un avocat, médecin ou journaliste professionnel.

identifiés par le biais d'une méthode ordinaire et si l'identification est nécessaire dans le cadre de la mission de renseignement. Les principes de proportionnalité et de subsidiarité sont ainsi respectés. Les services ont adapté leurs autorisations dans ce sens, autorisations par lesquelles ils veulent prendre successivement connaissance de données d'appel et d'identification. Le Comité a vérifié ponctuellement la manière dont les services respectent cet accord.

III.2.2.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	2
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	3
Création ou recours à une personne morale fictive	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	4
Collecte de données concernant des comptes bancaires et des transactions bancaires	10
Intrusion dans un système informatique	3
Ecoute, prise de connaissance et enregistrement de communications	11
TOTAL	33

Il ressort de ce tableau que la VSSE, en comparaison avec le SGRS, exploite davantage la possibilité qui lui est offerte d'utiliser les méthodes particulières de renseignement.

III.2.2.3. Les menaces et les intérêts justifiant le recours aux méthodes particulières

La VSSE n'est autorisée à intervenir que pour la sauvegarde des intérêts suivants :
- la sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel ;
- la sûreté extérieure de l'Etat et les relations internationales ;
- les éléments essentiels du potentiel scientifique et économique.

INTÉRÊTS PROTÉGÉS	NOMBRE[96]
La sûreté intérieure de l'Etat et la pérennité de l'ordre démocratique et constitutionnel	694
La sûreté extérieure de l'Etat et les relations internationales	571
La sauvegarde des éléments essentiels du potentiel scientifique et économique	24

Le tableau suivant reprend les menaces (potentielles) visées par la VSSE dans le contexte de la mise en œuvre des méthodes spécifiques et exceptionnelles. Une méthode peut naturellement viser plusieurs menaces. La VSSE peut utiliser les méthodes spécifiques dans le cadre de toutes les menaces qui relèvent de sa compétence (art. 8 L.R&S). Des méthodes exceptionnelles ne peuvent pas être utilisées dans le cadre de l'extrémisme ni de l'ingérence. Elles sont toutefois autorisées dans le cadre du processus de radicalisation menant au terrorisme (art. 3, 15° L.R&S).

NATURE DE LA MENACE	NOMBRE[97]
Espionnage	193
Terrorisme (et processus de radicalisation)	371
Extrémisme	319
Prolifération	17
Organisations sectaires nuisibles	4
Ingérence	3
Organisations criminelles	3

En matière d'utilisation de méthodes particulières, le terrorisme et l'extrémisme demeurent clairement les toutes premières priorités de la VSSE. L'on remarque en outre que – comme pour le SGRS – la mise en œuvre de méthodes spécifiques et exceptionnelles concerne dans une très large mesure l'espionnage comme menace.

96 Plusieurs menaces peuvent figurer dans une même autorisation.
97 Plusieurs menaces peuvent figurer dans une même autorisation.

III.3. LES ACTIVITÉS DU COMITÉ PERMANENT R EN SA QUALITÉ D'ORGANE JURIDICTIONNEL

III.3.1. LES CHIFFRES

Le Comité permanent R peut être saisi de cinq manières pour se prononcer sur la légalité des méthodes particulières de renseignement (art. 43/4 L.R&S) :
- d'initiative ;
- à la demande de la Commission de la protection de la vie privée ;
- par le dépôt d'une plainte d'un citoyen ;
- de plein droit chaque fois que la Commission BIM a suspendu une méthode spécifique ou exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données ;
- de plein droit quand le ministre compétent a donné son autorisation sur base de l'article 18/10, § 3 L.R&S.

De plus, le Comité peut aussi être saisi en sa qualité d'« auteur d'avis préjudiciels » (articles 131*bis*, 189*quater* et 279*bis* CIC). Le Comité rend, sur demande, un avis sur la légalité de renseignements recueillis au moyen de méthodes spécifiques ou exceptionnelles, et qui sont utilisés dans le cadre d'une affaire pénale. Les demandes d'avis sont introduites par les juridictions d'instruction ou par les juridictions de fond. Dans ce cadre, le Comité n'intervient pas *stricto sensu* comme un organe juridictionnel.

TYPE DE SAISINE	NOMBRE
D'initiative	28
Commission Vie Privée	0
Plainte	0
Suspension par la Commission BIM	9[98]
Autorisation du ministre	0
Auteur d'avis préjudiciel	0
TOTAL	37

Sur un total de 831 autorisations pour l'utilisation de méthodes particulières, le Comité s'est saisi à 37 reprises.[99] Une fois saisi, le Comité peut prendre plusieurs

[98] Dans deux dossiers, la Commission BIM a suspendu l'autorisation après que le Comité permanent R a été saisi. Ces suspensions n'ont pas été comptabilisées ici.

[99] La « saisine » concerne toujours l'autorisation donnée par le dirigeant du service de renseignement.

types de décisions (intermédiaires). Dans les deux premiers cas, une décision est toutefois prise avant la saisine proprement dite.

- constater la nullité de la plainte pour cause de vice de forme ou absence d'un intérêt personnel et légitime (art. 43/4, alinéa 1er, L.R&S) ;
- décider de ne pas donner suite à une plainte qui est manifestement non fondée (art. 43/4, alinéa 1er, L.R&S) ;
- suspendre la méthode contestée dans l'attente d'une décision définitive (art. 43/4, dernier alinéa, L.R&S) ;
- demander des informations complémentaires à la Commission BIM (art. 43/5 § 1er, alinéa 1er et alinéa 3, L.R&S) ;
- demander des informations complémentaires au service de renseignement concerné (art. 43/5 § 1er, alinéa 3, L.R&S) ;
- ordonner une mission d'enquête pour le service d'Enquêtes R (art. 43/5 § 2 L.R&S). Dans cette rubrique, on ne fait pas référence aux multiples informations complémentaires recueillies par le Service d'Enquêtes R avant la saisine proprement dite et donc d'une manière plutôt informelle ;
- procéder à l'audition des membres de la Commission BIM (art. 43/5 § 4, alinéa 1er, L.R&S) ;
- procéder à l'audition du dirigeant du service de renseignement ou des membres du service de renseignement concerné (art. 43/5 § 4, alinéa 1er, L.R&S) ;
- statuer sur les secrets relatifs à une information ou instruction judiciaire en cours dont les membres des services de renseignement sont dépositaires, après concertation avec le magistrat compétent (art. 43/5 § 4, alinéa 2, L.R&S) ;
- pour le président du Comité permanent R, statuer sur la demande du dirigeant du service ou le membre du service de renseignement qui estime devoir garder le secret dont il est dépositaire parce que sa divulgation est de nature à porter préjudice à la protection des sources, à la protection de la vie privée de tiers ou à l'accomplissement des missions du service de renseignement (art. 43/5 § 4, alinéa 3, L.R&S) ;
- mettre fin à la méthode concernée si celle-ci est toujours en cours ou si elle a été suspendue par la Commission BIM, et interdire l'exploitation des données recueillies grâce à cette méthode et leur destruction (art. 43/6 § 1er, alinéa 1er, L.R&S) ;
- mettre fin partiellement à une méthode autorisée. Il est question ici, par exemple, d'une situation où une méthode est limitée dans le temps, pas d'une situation où une seule autorisation d'un dirigeant du service autorise plusieurs méthodes et où le Comité ne met fin qu'à une seule d'entre elles ;
- lever totalement ou partiellement la suspension et l'interdiction qui ont été décidées par la Commission BIM (art. 43/6 § 1er, alinéa 1er, L.R&S), ce qui implique que la méthode autorisée par le dirigeant du service a bien été considérée par le Comité comme (partiellement) légale, proportionnelle et subsidiaire ;

- constater l'incompétence du Comité permanent R ;
- déclarer le caractère infondé de l'affaire pendante et permettre la poursuite de la méthode ;
- délivrer un avis préjudiciel (articles 131*bis*, 189*quater* en 279*bis* CIC).

NATURE DE LA DÉCISION	NOMBRE	NOMBRE DE DÉCISIONS FINALES
Plainte frappée de nullité	0	
Plainte manifestement non fondée	1	
Suspension de la méthode	3	
Informations complémentaires de la Commission BIM	4	
Informations complémentaires du service de renseignement	9	
Mission d'enquête du service d'Enquêtes R	17	
Audition membres de la Commission BIM	0	
Audition membres des services de renseignement	1	
Décision relative au secret de l'instruction	0	
Informations sensibles lors de l'audition	0	
Cessation de la méthode	12	39
Cessation partielle de la méthode	7	
Levée (partielle) de l'interdiction de la Commission BIM	5[100]	
Incompétence	0	
Autorisation légale/Non-cessation de la méthode/Non-fondement	15	
Avis préjudiciel	0	

En 2011, le Comité a pris 39 décisions finales.[101, 102] Il convient de garder à l'esprit que ces décisions ne constituent que la conclusion des activités MRD du Comité et, dans ce sens, une partie de l'effort réellement consenti. En effet, chaque

100 On retrouve dans ce relevé deux décisions du Comité qui ont également été reprises dans la rubrique « Cessation partielle de la méthode » parce que la Commission BIM a suspendu totalement les autorisations après que le Comité a été saisi, alors que cette suspension devait être partiellement levée.

101 Le nombre de saisines et le nombre de décisions finales ne correspondent pas nécessairement. Par exemple, parce que la décision finale n'a pas été prise dans la période de référence de la saisine ou parce que la saisine peut donner lieu à plusieurs décisions finales. En l'espèce, c'est le second cas de figure qui a prévalu (voir la note de bas de page précédente).

102 Le Comité permanent R doit statuer définitivement dans un délai d'un mois suivant la date à laquelle il a été saisi (art. 43/4 W.I&V). Le délai a été respecté dans tous les dossiers.

autorisation MRD accordée par la VSSE et le SGRS est soumise à un contrôle de contenu, et ce sur la base d'une procédure structurée et d'une *checklist* détaillée. Le cas échéant, des questions complémentaires sont posées avant de procéder à la saisine. Par conséquent, le contrôle des autorisations MRD exige un investissement en temps considérable au Comité.

Cinq des neuf suspensions prononcées par la Commission BIM ont été levées totalement ou partiellement. En outre, le Comité a annulé totalement ou partiellement treize autorisations, sans qu'elles aient été suspendues au préalable par la Commission BIM.

Des dix-neuf cessations totales ou partielles des autorisations, cinq concernaient des dossiers du SGRS et quatorze des dossiers de la VSSE.

III.3.2. LA JURISPRUDENCE

La substance des 39 décisions finales prises par le Comité permanent R en 2011 est reprise ci-après. Les synthèses sont expurgées des données opérationnelles. Seuls sont repris les éléments qui présentent un intérêt d'un point de vue juridique.

Les décisions ont été regroupées en six rubriques :

- les exigences légales (de forme) préalables à la mise en œuvre d'une méthode ;
- la motivation de l'autorisation ;
- les exigences légales (de forme) lors de la mise en œuvre d'une méthode ;
- la légalité de la méthode concernant les techniques utilisées, les données recueillies, la durée de la mesure et la nature de la menace ;
- l'exigence de proportionnalité ;
- l'exigence de subsidiarité.

Si cela s'indiquait, certaines décisions ont été reprises dans plusieurs rubriques.

III.3.2.1. Exigences légales (de forme) préalables à la mise en œuvre d'une méthode

Aucune méthode particulière ne peut être utilisée sans l'autorisation écrite préalable du dirigeant du service. Pour les méthodes exceptionnelles, il convient en outre de présenter un projet d'autorisation et un avis conforme de la Commission BIM. Si des méthodes sont mises en œuvre sans l'autorisation écrite ou l'avis conforme, le Comité doit naturellement intervenir.

III.3.2.1.1. Absence d'autorisation écrite

Le Comité a constaté qu'un service de renseignement avait pris connaissance de données d'appel d'un numéro de téléphone mobile et fixe, alors que l'autorisation

ne concernait que le premier (dossier 2011/501a). L' « observation » de la ligne fixe a dès lors été annulée pour illégalité en raison de l'absence d'autorisation écrite du dirigeant du service.

Dans un autre dossier, le dirigeant d'un service a autorisé le repérage d'un numéro de GSM pendant six mois (dossier 2011/748). En exécution de cette autorisation, le service de renseignement a demandé à un opérateur de télécommunications de lui fournir les données d'appel visées, et à tous les opérateurs de télécommunications d'identifier les titulaires des numéros ainsi obtenus. Une telle identification constitue toutefois une méthode séparée. Aucune autorisation n'avait été donnée pour sa mise en œuvre : « *Dat derhalve voormelde vordering, voor zover ze strekt tot de identificatie van de abonnee of de gewone gebruiker van de opgespoorde nummers (oproepgegevens) niet gedekt wordt door een (rechtsgeldige) beslissing en dienvolgens onwettig is.* »[103]

La même problématique est apparue dans un troisième dossier. Le dirigeant du service avait autorisé l'identification de « *alle telefoonnummers waarvan X titularis is* » (dossier 2011/830).[104] Cependant, il ressort de la réquisition faite aux opérateurs qu'il ne leur a pas seulement été demandé d'identifier les numéros de téléphone au nom de X, mais aussi de procéder à l'identification des moyens de communications de plusieurs autres abonnés. La méthode utilisée n'était donc pas intégralement couverte par une décision écrite et motivée, et ce à peine d'illégalité de cette partie de la méthode qui, le cas échéant, sortait du cadre de la décision. « *Dat dienvolgens targets (personen, plaatsen, …) die ten gene dele voorzien zijn in een beslissing, niet op legale wijze het voorwerp van een vordering kunnen uitmaken.* »[105] En outre, il apparaît qu'alors que la décision ne mentionnait que l'identification de tous les numéros de téléphone de X., dans la réquisition aux opérateurs, il était demandé de procéder à l'identification de *tous* ces services de communications électroniques. « *Dat ook hier geen overeenstemming is tussen de beslissing (gelimiteerd tot telefoniediensten) en de uiteindelijke vordering.* »[106]

III.3.2.1.2. Autorisation donnée par le remplaçant du dirigeant du service

Le Comité permanent R s'est saisi d'un dossier (2011/406) dans lequel une méthode spécifique a été autorisée « *Voor de Administrateur-generaal, afwezig,*

---

103 « que, par conséquent, la réquisition susmentionnée, pour autant qu'elle vise l'identification de l'abonné ou de l'utilisateur habituel des numéros repérés (données d'appel), n'est pas couverte par une décision (valable) et est dès lors illégale. » (traduction libre).

104 « tous les numéros de téléphone dont X est titulaire. » (traduction libre).

105 « que ces cibles (personnes, lieux, …) qui ne sont en aucun cas prévues dans la décision ne peuvent pas légalement faire l'objet d'une réquisition. » (traduction libre)

106 « qu'ici non plus il n'y a pas de concordance entre la décision (limitée aux services de téléphonie) et la demande finale. » (traduction libre).

[naam], Adviseur ».[107] Le conseiller concerné assurait à ce moment-là la direction générale du service.

La question était de savoir si de cette manière, l'article 18/3 L.R&S était respecté. En effet, le § 1er, alinéa 2 de cet article stipule, entre autres, qu'une méthode spécifique ne peut être mise en œuvre qu'après autorisation écrite et motivée du dirigeant du service, soit « *l'Administrateur général de la Sûreté de l'Etat ou, en cas d'empêchement, l'administrateur général faisant fonction* ». Avec cette disposition, le législateur voulait garantir que la direction des services de renseignement soit toujours au courant de l'utilisation d'une méthode spécifique et de sa mise en œuvre. Bien que le conseiller concerné ait erronément signé '*voor de Administrateur-generaal*'[108], au moment même où il était Administrateur général faisant fonction, la finalité de la loi a bien été respectée. De surcroît, il apparaît clairement que l'Administrateur général était absent, si bien que dans le cadre du fonctionnement MRD, la délégation de pouvoir était justifiée. En outre, le Comité a constaté que ni dans l'A.R. du 14 janvier 1994 portant le statut de l'Administrateur général et de l'Administrateur général adjoint de la Sûreté de l'Etat, ni dans l'A.R. du 5 décembre 2006 relatif à l'Administration générale et à la Cellule d'Appui de la Sûreté de l'Etat, des règles contraignantes relatives au remplacement du dirigeant du service n'étaient mentionnées. Aucune illégalité n'a dès lors été constatée.

III.3.2.1.3. Communication préalable à la Commission BIM dans le cadre d'une méthode spécifique

Un service de renseignement était autorisé à surveiller l'accès à un lieu privé avec une caméra pendant une période limitée. Etant donné qu'il souhaitait « prolonger »[109] la méthode, le dirigeant du service a rédigé une nouvelle autorisation pour une période débutant dès l'expiration du délai précédent (dossier 2011/667). Toutefois, ce cas était particulier en ce sens que la Commission BIM n'a eu connaissance de la nouvelle « prolongation » que dans le courant de la matinée du premier jour du nouveau délai. Mais l'article 18/3 § 1er L.R&S stipule qu'une méthode spécifique ne peut être mise en œuvre qu'après avoir été portée à la connaissance la Commission BIM. La conséquence en a été qu'une éventuelle observation à partir de minuit (l'autorisation initiale de procéder à une observation expirait à ce moment-là) jusqu'à l'information par notification de la nouvelle autorisation n'était pas couverte par un mandat valable. Aussi les images enregistrées pendant cette courte période intermédiaire devaient-elles être détruites.

---

107 « Pour l'administrateur général, absent, [nom], Conseiller ».

108 « Pour l'administrateur général ». (traduction libre).

109 Contrairement aux méthodes exceptionnelles, la loi ne prévoit pas *stricto sensu* la possibilité de « prolonger « une méthode spécifique. Une fois le délai passé, une nouvelle autorisation est requise.

III.3.2.1.4. Absence d'avis conforme

Un service de renseignement souhaitait écouter une communication (art. 18/17 § 1er L.R&S) et pénétrer dans un lieu privé pour placer un appareil d'écoute (art. 18/17 § 2 L.R&S) (dossier 2011/300). Etant donné qu'il s'agissait d'une méthode exceptionnelle, l'avis conforme de la Commission BIM était requis. Cet avis faisait toutefois référence à la compétence décrite à l'article 18/17 § 2 L.R&S (et donc pas à l'écoute en tant que telle). Il ressortait aussi de la période pendant laquelle la méthode exceptionnelle pouvait être appliquée, selon la Commission BIM, que l'avis ne concernait que le placement et le retrait des dispositifs d'écoute ; pas l'écoute elle-même.

Le Comité permanent R a dès lors jugé illégale la « *gebeurlijke beslissing tot uitvoering van de methode zoals bedoeld in art. 8/17 § 1 W.I&V* ».[110]

III.3.2.1.5. Absence d'avis conforme concernant un soi-disant journaliste ?

Le service de renseignement concerné souhaitait retrouver l'identité d'un bloggeur anonyme qui, sur son site internet, répandait, entre autres, des opinions extrémistes (dossier 2011/204). Il se présentait en plus comme un journaliste. La question était de savoir si le service de renseignement devait obtenir l'avis conforme de la Commission BIM pour cette méthode, sans qu'elle ne dispose de plus de données sur la qualité présumée du bloggeur. En effet, l'article 18/3, § 1er, alinéa 3 L.R&S stipule que « *Les méthodes spécifiques ne peuvent être mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur la proposition du dirigeant du service.* »

A l'instar de la Commission BIM, le Comité a estimé que la méthode spécifique pouvait être mise en œuvre dans ce cas sans avis préalable pour ainsi vérifier l'identité du bloggeur et ensuite contrôler s'il s'agissait réellement d'un journaliste dans le sens de la loi. Si, par cette vérification, sa qualité de journaliste était confirmée, les dispositions reprises aux articles 18/2 § 3 et 18/3 § 1er, alinéa 3, L.R&S devaient être respectées.

La même question s'est posée dans un autre dossier. Un service de renseignement souhaitait retrouver l'identité des titulaires de numéros de GSM qui étaient soupçonnés de mener des activités de renseignement, mais qui opéraient peut-être sous le couvert de journalistes (dossier 2011/264). Le Comité

110 « éventuelle décision de mettre en œuvre la méthode telle que visée à l'art. 8/17 § 1er L.R&S.» (traduction libre).

a une fois de plus estimé que la méthode spécifique pouvait être mise en œuvre pour vérifier l'identité et la qualité éventuelle de journaliste de l'utilisateur.

III.3.2.1.6. Avis conforme et portée de la notion de « système informatique »

Le dirigeant d'un service souhaitait permettre l'identification de codes PUK de certains numéros de cartes SIM qui étaient en possession d'une personne suivie par son service (dossier 2011/721). Il considérait cette identification comme une méthode spécifique, à savoir « *l'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques ou du moyen de communication électronique utilisé* », tel que le définit l'article 18/7 L.R&S. Ensuite, l'idée était de créer un nouveau code PIN au moyen des codes PUK obtenus, afin « *via bijkomende BIM-methoden, de kaarten dan (kunnen) worden uitgelezen* ».[111]

Le Comité permanent R a suspendu la méthode concernée et en a examiné la légalité. Il a constaté qu'en réalité, le but n'était pas d'identifier l'abonné ou l'utilisateur des cartes SIM visées ; celui-ci était en effet déjà connu. La méthode a été mise en œuvre en vue de découvrir des PUK ou le code de déblocage unique de la puce SIM pour ensuite modifier le code PIN de la puce SIM.

Dans une carte SIM, un S(ubscriber) I(dentity ou identification) M(odule) est installé. Il constitue un circuit intégré, dans lequel, entre autres, des données informatisées et protégées sont enregistrées. Une telle puce SIM doit être considérée comme un « système informatique » au sens de l'article 18/16 L.R&S. Le législateur a en effet voulu donner la même signification à ce terme que dans la Loi du 28 novembre 2000 relative à la criminalité informatique.[112] Et lors de la confection de la Loi du 28 novembre 2000, les systèmes informatiques ont été décrits comme « *tout système permettant le stockage, le traitement ou la transmission de données. A ce propos, on pense principalement aux ordinateurs, aux cartes à puce, mais également aux réseaux et à leurs composants ainsi qu'aux systèmes de télécommunication ou à leurs composants qui font appel à la technologie de l'information.* »[113] L'obtention et l'utilisation du code PUK pour modifier et introduire le code PIN constitue dès lors une méthode exceptionnelle telle que décrite à l'article 18/16 § 1er, 1° et 2° L.R&S (« *à l'aide ou non de moyens techniques, de faux signaux, de fausses clés ou de fausses qualités 1° accéder à un système informatique ; 2° y lever toute protection quelconque ;* »). Les exigences légales relatives à l'autorisation d'une méthode exceptionnelle n'ayant pas été respectées, le Comité a mis fin à la méthode.

111 « de (pouvoir) alors lire les cartes par le biais de méthodes MRD complémentaires. » (traduction libre).
112 *Doc. parl.* Sénat 2008-2009, 4-1053/1, 54.
113 *Doc. parl.* Chambre 1999-2000, 50-213/1 et 50-214/1, 12.

III.3.2.1.7. Avis conforme en cas d'extrême urgence

Dans le cadre d'une opération en cours, le dirigeant du service a autorisé le service de renseignement concerné à procéder à l'inspection d'un lieu privé (dossier 2011/331). Il a été fait usage de la procédure d'extrême urgence, telle que décrite à l'article 18/10 § 4 L.R&S. Cette disposition permet au dirigeant du service d'autoriser la méthode exceptionnelle par écrit après avoir reçu l'avis conforme du président de la Commission BIM (et donc pas de la Commission dans son ensemble). La question tournait autour de l'avis conforme. L'autorisation écrite du dirigeant du service mentionnait seulement la réception de cet avis; il s'agissait cependant d'un avis oral. En outre, aucun projet d'autorisation écrit, ni le moindre avis écrit (à titre de confirmation du contenu concret de l'avis oral) n'était disponible.

Conformément à l'article 18/10 § 1er L.R&S, l'examen de la conformité de l'autorisation avec l'avis conforme de la Commission BIM comprend une vérification du respect des dispositions légales pour l'utilisation de la méthode exceptionnelle, des principes de proportionnalité et de subsidiarité, ainsi qu'un contrôle des mentions prescrites par l'article 18/10 § 2 L.R&S. Il n'existait pas la moindre donnée écrite vérifiable d'un tel examen et de la conclusion de conformité, si ce n'est la mention d'un avis conforme dans l'autorisation. Le Comité a jugé que ce dernier était insuffisant. Un tel procédé ne permet en effet pas au Comité permanent R d'exercer son contrôle de légalité dans tous ses aspects (c.-à-d. *in casu* le contrôle de la conformité entre (le projet de) l'autorisation d'une part, et l'avis conforme rendu, d'autre part). Déjà rien qu'en raison de son incidence sur la tâche de contrôle du Comité permanent R, ce procédé ne pouvait pas être considéré comme légal.

Le Comité a en outre remarqué que les dispositions légales et réglementaires en vigueur ne mentionnaient ni explicitement ni implicitement un quelconque projet d'autorisation oral du dirigeant du service ou un quelconque avis conforme oral de la Commission BIM. De plus, l'article 43/3 L.R&S stipule que l'ensemble des décisions, avis et autorisations doit être porté sans délai à la connaissance du Comité permanent R, et ce afin qu'il puisse exercer son contrôle de légalité. Ce qui signifie que ces décisions, avis et autorisations doivent prendre la forme d'un document.

Le Comité puisait encore un argument supplémentaire dans le fait que le législateur n'a autorisé qu'une exception très restrictive au caractère écrit, c'est-à-dire en ce qui concerne la demande par l'officier de renseignement en cas d'extrême urgence dans les cas de méthodes spécifiques visées aux articles 18/6 § 2, 18/7 § 2 en 18/8 § 2 L.R&S. Mais même une telle demande doit être confirmée par écrit dans les meilleurs délais. Par conséquent, le Comité estimait que l'on ne pouvait raisonnablement supposer que le législateur, pour ce qui concerne les méthodes exceptionnelles plus intrusives, avait voulu implicitement déroger au caractère écrit d'une décision à un ou plusieurs stades distincts.

Aussi le Comité permanent R a-t-il décidé que le caractère oral de la demande initiale et de l'avis conforme n'était pas conforme à la lettre ni à l'esprit de la loi.

III.3.2.2. Motivation de l'autorisation

III.3.2.2.1. Motivation insuffisante

Dans six dossiers, une suspension a été prononcée par la Commission BIM parce que l'autorisation du dirigeant du service n'était pas suffisamment motivée pour permettre une évaluation de la légalité, de la proportionnalité et de la subsidiarité. Dans les cinq premiers dossiers, le Comité permanent R – qui est saisi d'office quand la Commission BIM suspend une méthode – s'est rangé à cet avis et a ordonné de mettre fin à la méthode. Dans le sixième dossier, la suspension a été levée parce que le service de renseignement concerné avait fourni des informations complémentaires après la décision (justifiée) de la Commission BIM. Dans un septième dossier, pour lequel la motivation de l'autorisation était en discussion, le Comité s'est saisi d'office.

Dans le premier dossier (2011/84), une autorisation en vue de procéder à l'identification d'un abonné ou utilisateur d'un numéro de GSM a été suspendue par la Commission BIM parce que l'autorisation du dirigeant du service « *ne contient qu'une description succincte des éléments de faits justifiant la décision et par conséquent, ne permettant pas, en son état, à la Commission BIM, de procéder à la vérification des principes de subsidiarité et de proportionnalité* ». Le Comité a lui aussi dû constater que l'autorisation ne faisait pas apparaître le moindre lien entre le numéro de GSM visé et la menace : « *La décision ne démontre dès lors aucunement sa légalité, à quoi s'ajoute qu'un tel libellé ne permet nullement d'évaluer le respect les principes de subsidiarité et de proportionnalité.* »

Lorsque le GSM d'un parlementaire belge a été perdu ou volé à l'étranger, le service de renseignement concerné a voulu localiser l'appareil en utilisant une méthode spécifique (dossier 2011/192). Il a été fait référence à l' « ingérence » comme menace potentielle. La Commission BIM a cette fois suspendu la méthode parce que « *le libellé de la décision ne contient aucune description, même succincte des éléments de faits justifiant la décision.* » Le Comité est arrivé à la même constatation : l'autorisation « *ne définit pas concrètement en quoi consisterait la menace potentielle d'ingérence, en ne contient aucune description, même succincte des éléments de faits justifiant la décision.* »

Une troisième autorisation a été suspendue parce qu'elle « *onvoldoende toelaat te achterhalen of de regels van de subsidiariteit in concreto gerespecteerd zijn en het daarin opgeworpen verband met de inwendige veiligheid van de staat niet overtuigt.* »[114] (dossier 2011/307). Le Comité a ajouté la motivation suivante :

[114] « ne permet pas d'évaluer suffisamment *in concreto* le respect des règles de subsidiarité et ne convainc pas quant au lien qui y est établi avec la sûreté intérieure de l'Etat. » (traduction libre).

« Waar een toelating, zoals in casu, geen daadwerkelijk of minstens redelijkerwijs aanneembaar verband tussen een target van een methode en een potentiële bedreiging zoals bedoeld in art. 18/1 W.I&V aangeeft, doch zich stoelt op allusies, zij gebrekkig gemotiveerd is en derhalve uit legaliteitsoogpunt niet genoegzaam met redenen is omkleed. Overwegende dat een en ander evenmin een adequate toetsing toelaat van de principes van proportionaliteit en subsidiariteit. »[115]

Dans le quatrième dossier (2011/355), le service de renseignement souhaitait procéder, à la demande d'un correspondant étranger, à l'identification d'un numéro de téléphone belge, qui est apparu dans un dossier de terrorisme. L'autorisation a été suspendue parce qu'elle était imprécise sur certains points : « *l'intérêt à protéger est insuffisamment précisé ; l'identité du service étranger est insuffisamment précisée également ; aucune information n'est donnée sur l'enquête en matière de terrorisme en cours ; la proportionnalité et la subsidiarité sont insuffisamment motivées.* » Le Comité a lui aussi trouvé dans l'autorisation trop peu d'éléments permettant d'évaluer concrètement la légalité, la proportionnalité et la subsidiarité.

Dans le cinquième dossier (2011/442) – dans lequel le service de renseignement souhaitait identifier deux numéros de GSM – la Commission BIM n'a une fois de plus trouvé « *aucune description, même succincte, des éléments de fait qui la justifiaient.* » Le Comité en est arrivé à la même conclusion : la proportionnalité et la subsidiarité ne pouvaient pas être vérifiées.

Dans le dernier dossier qui a été suspendu par la Commission BIM, le dirigeant du service souhaitait autoriser une observation à l'aide d'un moyen technique (dossier 2011/724). La commission a toutefois jugé que « *telle qu'elle est libellée et, particulièrement, en ce que le degré de gravité de la menace potentielle qu'elle décrit n'est pas suffisamment précisé et justifié.* » Le Comité ne pouvait que se ranger à l'avis de la Commission BIM, au moment où elle a pris sa décision. Cependant, il ressort d'informations complémentaires orales et écrites que « *van de target, op basis van gedocumenteerde elementen, onmiskenbaar een potentiële dreiging uitgaat tegen een van de belangen vermeld in art. 7 W.I&V.* » et que « *de methode, waartoe is beslist, in verhouding staat tot de ernst van voormelde dreiging én voldoet aan de proportionaliteits- en subsidiariteitseis* ».[116] Le Comité a toutefois affirmé que « *het evenwel aangewezen ware geweest dat* ab initio*, in de beslissing zelf, meer omstandig gewag zou zijn gemaakt van de – overigens*

115 « Là où une autorisation, comme dans ce cas-ci, n'établit pas de lien effectif, ou du moins raisonnablement admissible, entre une cible d'une méthode et une menace potentielle telle que visée à l'art. 18/1 L.R&S, mais repose sur des allusions, cette autorisation est mal motivée et donc insuffisamment revêtue de motifs du point de vue de la légalité. Considérant que ceci ne permet pas davantage un contrôle adéquat des principes de proportionnalité et de subsidiarité. » (traduction libre).

116 « de la cible, sur la base d'éléments documentés, il existe indéniablement une menace potentielle contre un des intérêts cités à l'art. 7 L.R&S (et que) la méthode retenue est en rapport avec la gravité de la menace précitée et satisfait aux exigences de proportionnalité et de subsidiarité. » (traduction libre).

voorhanden zijnde – elementen die redelijkerwijze noodzakelijk waren om de inschatting van de dreiging, van de proportionaliteit en van de subsidiariteit op een adekwate manier te kunnen bewerkstelligen. Dat een beslissing tot aanwending van een methode op dit vlak voldoende zelfdragend moet zijn, op straffe van niet te voldoen aan de motiveringsverplichting en derhalve tijd en middelen te laten verloren gaan. »[117]

Enfin, le service de renseignement souhaitait obtenir les données d'appel de numéros de GSM de trois personnes différentes, ainsi que des adresses électroniques de l'une d'entre elles (dossier 2011/522). La décision était motivée comme il se doit en ce qui concerne un numéro de GSM et les adresses électroniques y afférentes. Mais tel n'était pas le cas pour les numéros de GSM des deux autres personnes. La décision n'était pas claire en ce qui concerne la menace qui devait justifier la méthode dans la mesure où elle a posé question sur la compétence du service de renseignement concerné. On ne pouvait pas non plus établir de lien entre l'utilisateur d'un numéro de GSM et les utilisateurs des deux autres numéros. Sur la base des informations initiales, le Comité permanent R n'était pas en mesure d'effectuer un contrôle de légalité. Le service de renseignement concerné a cependant transmis de la documentation complémentaire, qui établissait que les conditions légales en termes de compétence et de menace étaient bien respectées. Le Comité a dès lors décidé que la méthode était légale, mais a fait une nouvelle fois remarquer que « *het evenwel aangewezen ware geweest dat* ab initio*, in de beslissing zelf, gewag zou zijn gemaakt van die elementen die* in concreto *de bevoegdheid en de bedreiging aantonen inzake elk van de onder methode geplaatste elektronische communicatiemiddelen.* »[118]

III.3.2.2.2. Contradiction dans la motivation

Le service de renseignement concerné souhaitait procéder à l'identification de l'abonné d'un numéro de téléphone (dossier 2011/72). Cette méthode est décrite à l'article 18/7 § 1er, 1° L.R&S (« *l'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques ou du moyen de communication électronique utilisé* »). Il ressortait toutefois de cette même autorisation que l'intention était d'identifier le titulaire d'un numéro de

117 « il aurait toutefois été indiqué que dès le départ, dans la décision même, il soit fait mention de façon plus détaillée des éléments – par ailleurs disponibles – qui étaient raisonnablement nécessaires pour pouvoir évaluer la menace, la proportionnalité et la subsidiarité d'une manière adéquate. Qu'une décision d'utiliser une méthode à ce niveau doit être suffisamment « autoportante », sous peine de ne pas rencontrer l'obligation de motivation, et donc d'engendrer une perte de temps et de moyens. » (traduction libre).

118 « il aurait toutefois été indiqué que dès le départ, dans la décision même, il soit fait mention des éléments qui établissent concrètement la compétence et la menace pour chacun des moyens de communication électroniques placés dans le cadre de la méthode. » (traduction libre).

téléphone anonyme au moyen des communications passées via ce numéro. En réalité, le service souhaitait donc procéder au « *repérage des données d'appel de moyens de communications électroniques à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés* » (art. 18/8 § 1er, 1° L.R&S).

Le Comité a jugé que les motifs repris dans l'autorisation du dirigeant du service devaient étayer l'utilisation de la méthode choisie. Vu la contradiction interne apparaissant dans l'autorisation, celle-ci n'était pas dûment motivée, et la cessation de la méthode a été ordonnée.

III.3.2.3. Exigences légales (de forme) lors de la mise en œuvre d'une méthode

Une fois qu'une méthode est autorisée valablement et, par conséquent, portée à la connaissance de la Commission BIM, elle peut être mise en œuvre. Mais lors de la mise en œuvre aussi, des règles particulières doivent parfois être respectées.

III.3.2.3.1. Procédure d'extrême urgence par le recours à un opérateur

L'article 18/8 § 2 L.R&S stipule qu'en cas d'extrême urgence motivée, l'officier de renseignement peut, par une décision verbale, requérir sur-le-champ des données d'appel auprès d'un opérateur, avec l'accord verbal et préalable du dirigeant du service (dossier 2011/227). Conformément à la procédure, le dirigeant du service confirmait plus tard par écrit son accord oral préalable. Cette confirmation ne permettait cependant pas de déterminer l'identité de l'officier de renseignement qui avait demandé les informations, ne donnait aucune indication de date et de période où l'opérateur était requis et n'indiquait pas à quel moment l'autorisation orale du dirigeant du service avait été accordée. Ces données n'apparaissaient pas non plus dans quelque autre pièce dont le Comité disposait initialement, si bien qu'il était impossible de contrôler la légalité de la demande.

Au cours de la procédure, le service de renseignement concerné a néanmoins fourni des documents complémentaires, qui démontraient que toutes les conditions légales étaient remplies. Aussi le Comité permanent R a-t-il constaté que la méthode était conforme aux dispositions de la loi. Le Comité a cependant souligné qu'il était indiqué que les éléments démontrant concrètement que les formalités légales requises étaient remplies, soient d'emblée repris dans l'autorisation même.

III.3.2.3.2. Information par notification préalable du président de l'Association des journalistes professionnels

Souhaitant retracer les données d'appel d'un moyen de communication d'un journaliste professionnel, le service concerné a demandé et obtenu l'avis conforme de la Commission BIM (2011/193). L'article 18/2 § 3 L.R&S stipule

toutefois que « *cette méthode ne peut être exécutée sans que […] le président […] de l'Association des journalistes professionnels en soit averti au préalable par le président de la commission.* » Selon la Commission BIM, il ne pouvait cependant pas être établi que cette formalité avait été remplie. Renseignements pris, la Commission BIM n'avait pas informé le président ; elle ne l'a fait que plus tard. Ainsi, il apparaît que le président de la Commission BIM avait fourni « *les informations nécessaires* » au président de l'Association des journalistes professionnels après la remarque formulée par le Comité en la matière.

Etant donné que l'article 18/2 § 3 L.R&S ne précise pas la forme que doit prendre cette information au moyen d'une notification, ni ce qu'il convient de comprendre par « *les informations nécessaires* », le Comité a jugé que « *l'affirmation du Président de la Commission BIM que l'avertissement préalable a eu lieu, avec en plus, la précision du jour et de l'heure de cet avertissement préalable et que les « informations nécessaires » ont été données au Président de l'association des journalistes professionnels suffit au regard des exigences légales* ».

L'information du président concerné constitue une exigence de forme substantielle, raison pour laquelle le Comité a jugé illégale la mise en œuvre éventuelle de la méthode avant cette notification. Les données éventuellement recueillies devaient dès lors être détruites ; les données recueillies à partir de la notification pouvaient quant à elles être exploitées.

Dans un deuxième dossier quasi semblable (dossier 2011/257), il n'apparaissait pas dans l'avis conforme de la Commission BIM que le président de l'Association des journalistes professionnels était informé. Aussi le Comité permanent R a-t-il demandé un complément d'informations à la Commission BIM. Etant donné que la Commission BIM a fait savoir que le président avait reçu les « *les renseignements nécessaires* » à un moment donné, le Comité a décidé que l'exécution de la méthode spécifique était légale à partir de ce moment-là.

La problématique de l'information au moyen d'une notification est entrée en ligne de compte dans deux autres cas (dossiers 2011/761 et 2011/762) : le dirigeant d'un service avait autorisé l'observation de GSM de journalistes étrangers, reconnus comme journalistes professionnels en Belgique. Dans ses avis conformes, la Commission BIM a explicité que ces méthodes spécifiques ne pouvaient être mises en œuvre qu'après l'information du président de l'Association des journalistes professionnels. Ces informations n'ont toutefois pas eu lieu immédiatement. Le Comité permanent R a examiné le cas et a décidé ce qui suit « *Attendu qu'il échet de constater que le [service de renseignement] a mis en œuvre une méthode spécifique à l'égard d'un journaliste professionnel avant que le Président de la Commission BIM n'ait informé le Président de l'Association professionnelle des journalistes, mais aussi que le Président de la Commission BIM n'a effectué cette démarche substantielle […] plus d'un mois après la notification du projet de décision du Chef [du service de renseignement] et plus de 15 jours après l'avis conforme donné par la Commission BIM* ». Les données qui ont été recueillies avant l'information devaient par conséquent être détruites.

III.3.2.4. Légalité de la méthode concernant les techniques utilisées, les données recueillies, la durée de la mesure et la nature de la menace

Les services de renseignement ne peuvent naturellement pas mettre en œuvre une méthode ou technique comme ils l'entendent : celles-ci doivent être prévues par la loi, être parfois subordonnées à des délais, ne peuvent pas toujours être utilisées pour chaque menace ou à l'étranger, etc. Le Comité permanent R a précisé ces limites dans certaines décisions.

III.3.2.4.1. La demande rétroactive de données bancaires

Le service de renseignement concerné souhaitait recueillir diverses données bancaires, d'une part sur les six derniers mois, et d'autre part pour les six mois à venir (dossier 2011/304).

Cette méthode exceptionnelle était basée sur l'article 18/15 L.R&S, qui autorise les services de renseignement à demander des transactions bancaires « *qui ont été réalisées pendant une période déterminée* », sans que la loi ne fixe de délai maximum à cet égard. L'article 18/10 § 1er, alinéa 2, L.R&S stipule toutefois que « *la période durant laquelle la méthode exceptionnelle de recueil de données peut être appliquée ne peut excéder deux mois.* »

Le Comité permanent R a examiné la portée de ces deux dispositions.

En ce qui concerne la demande en temps réel des données bancaires (futures), le Comité a déclaré que ceci n'est possible que pour une période maximale de deux mois à compter de l'autorisation. La Loi MRD permet néanmoins la prolongation de ce délai, après évaluation.

Concernant la demande rétroactive de données bancaires, le Comité est arrivé à la conclusion que ni la loi ni les travaux préparatoires ne mentionnent une limite de temps et « *dat de periode alsdan (enkel) wordt beperkt door het beginsel van de proportionaliteit* »[119] (voir III.3.2.5.1).

Cette décision de principe a encore été confirmée à plusieurs reprises (dossiers 2011/378, 2011/435 et 2011/436).

III.3.2.4.2. Absence d'indication de la durée de la méthode

Un service de renseignement souhaitait, dans deux dossiers distincts, prendre connaissance de données d'appel d'une personne déterminée via un opérateur en télécommunications (dossiers 2011/493 et 2011/494). Les autorisations mentionnaient bien les délais dans lesquels la demande devait être formulée à l'opérateur, mais pas la période pour laquelle les données d'appel étaient

[119] « que la période est alors (seulement) limitée par le principe de proportionnalité. » (traduction libre).

demandées. Il ressortait néanmoins de l'examen du Comité permanent R que la légalité de la méthode était garantie.

III.3.2.4.3. L'autorisation entre-elle dans le cadre des menaces légales ?

Un service de renseignement souhaitait vérifier rétroactivement et pour une courte période quels numéros avaient appelé vers un GSM déterminé pour ensuite identifier les différents abonnés et titulaires (dossier 2011/609). Cette autorisation avait ceci de particulier que le GSM appartenait à un agent de renseignement du service concerné et qu'il avait donné son autorisation à cet effet. L'agent a été victime d'un incident et on voulait savoir *in fine* s'il existait un lien – bien que peu probable – entre ce fait et les dossiers traités par l'agent. En effet, « *On ne peut toutefois exclure que l'agent et le service soient victimes d'un acte d'intimidation de la part d'une organisation suivie par l'agent dans le cadre des missions qui lui ont été affectées* », selon le service concerné. Le Comité permanent R a examiné si la finalité de la méthode spécifique entrait bien dans le cadre de la mission légale du service telle que définie dans la Loi du 30 novembre 1998. Le Comité a tenu le raisonnement suivant : « *Attendu qu'il en ressort que la finalité de la méthode spécifique envisagée est surtout de vérifier que la sécurité d'un agent de [renseignement] n'a pas été compromise dans l'exercice d'une de ses missions ; Qu'une telle finalité de sécurité n'est pas, en soi, l'une des missions visées [par] la Loi R&S ; Attendu toutefois qu'en voulant vérifier si son agent a été victime ou non d'un acte d'intimidation, [le service] cherche aussi la trace d'une activité éventuelle qui pourrait menacer la sûreté intérieure de l'Etat* ».

III.3.2.4.4. La portée de la notion de « courrier »

Un service de renseignement souhaitait prendre connaissance pendant deux mois de données postales et de données d'identification de boîtes postales d'un ou plusieurs expéditeur(s) et destinataires(s) de colis confiés ou non à des opérateurs postaux (dossier 2011/659). L'article 3, 13° L.R&S définit le « *courrier* » comme « *l'envoi postal tel qu'il est défini à l'article 131, 6°, 7° et 11°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques* ». Cet article 131 de la loi du 21 mars 1991 a cependant été modifié après l'entrée en vigueur de la Loi MRD du 4 février 2010. Par l'article 5 de la Loi du 13 décembre 2010 (*M.B.* 31 décembre 2010), tant l'ordre que la définition des différentes notions ont subi des modifications. Le Comité permanent R a toutefois jugé que ces modifications n'étaient pas applicables à la notion de « courrier » retenue dans la Loi MRD du 4 février 2010. A cet effet, les définitions de l'article 131, 6°, 7° et 11°, de la loi du 21 mars 1991, telles que libellées au moment de l'entrée en vigueur de la Loi MRD du 4 février 2010, restent d'application.

III.3.2.4.5. Identification des données d'appel obtenues illégalement

Comme développé précédemment (voir III.3.2.1.1, le Comité a constaté qu'un service de renseignement avait pris connaissance des données d'appel d'un numéro de téléphone mobile et un fixe, alors que l'autorisation ne concernait que le premier. L' « observation » de la ligne fixe a par conséquent été annulée, et il s'en est suivi une interdiction d'utiliser les données recueillies. Le service de renseignement concerné n'avait dès lors pas pu autoriser l'identification des données d'appel de la ligne fixe. L'identification des données d'appel de la ligne mobile était quant à elle autorisée (dossier 2011/501b).

III.3.2.5. L'exigence de proportionnalité

Le Comité s'est prononcé à plusieurs reprises sur la question de savoir si une méthode autorisée était proportionnelle à la gravité de la menace.

III.3.2.5.1. La demande rétroactive de données bancaires

Comme mentionné précédemment, le Comité acceptait la demande rétroactive de données bancaires pour une période de plus de deux mois, à la condition que la période soit proportionnelle à la gravité de la menace. Le Comité s'est prononcé sur cette problématique dans quatre dossiers différents, qui concernaient uniquement « l'espionnage ». De manière générale, le Comité a affirmé que « *la vérification du respect des principes de proportionnalité et de subsidiarité exige néanmoins que la durée de la période du passé visée par la collecte de données bancaires soit motivée par le service de renseignement de manière telle qu'elle permette au Comité permanent R d'en apprécier la justification en fonction de la gravité de la menace potentielle ; cette appréciation doit être effectuée dans chaque cas en fonction des circonstances particulières justifiant la mise en œuvre de la méthode exceptionnelle* ».

Des données ont été respectivement demandées pour une période de six mois (dossier 2011/403), huit mois (dossier 2011/378), plus de cinq ans (dossier 2011/436) et plus de quinze ans (dossier 2011/435). En outre, le Comité a pu constater que la motivation du service de renseignement était plus élaborée et plus détaillée en fonction de la durée de la période demandée. Dans le premier cas seulement, le choix de la période n'était pas motivé. Dans ce cas-ci, le Comité a toutefois jugé que pour inventorier les transactions financières et les contacts des titulaires des comptes visés afin de découvrir leur réseau, un effort soutenu d'une durée suffisante était nécessaire. Aussi une période de six mois a-t-elle été jugée acceptable dans ce cas-ci.

III.3.2.5.2. Mise sur écoute de numéros encore inconnus

Le service concerné souhaitait procéder à l'écoute de tous les appareils téléphoniques connus d'une cible (dossier 2011/322). Il voulait aussi accorder cette autorisation pour « *numéros non encore connus et a fortiori non encore identifiés qui apparaîtraient dans le cadre de l'exécution d'une autre méthode spécifique* », mais qui étaient utilisés par la même cible.

Le Comité a examiné l'autorisation pour les numéros encore inconnus sous l'angle de la proportionnalité. Il a pu constater que le service de renseignement avait formulé très précisément la raison pour laquelle il souhaitait utiliser cette méthode. Il est apparu que même la procédure d'urgence prévue dans la loi n'était d'aucune aide dans ce cas exceptionnel. Par conséquent, le Comité a décidé que cette méthode était légale.

III.3.2.5.3. La durée de l'observation d'un lieu privé

Le service de renseignement souhaitait observer un lieu privé pendant deux mois (dossier 2011/434). Une réunion d'un groupement, qui retenait son attention, devait en principe s'y réunir. Mais la durée de cette réunion était bien entendu limitée : « *Considérant dès lors qu'une durée d'observation de deux mois excède la période au cours de laquelle l'événement à observer doit se dérouler* », la mesure n'était pas proportionnelle, si bien que la méthode a été partiellement annulée.

III.3.2.5.4. Prise de connaissance de données d'appel d'un numéro inconnu

La Commission BIM avait suspendu la prise de connaissance de données d'appel d'un GSM et l'identification subséquente des titulaires concernés (dossier 2011/474). La raison en était qu'au moment où la méthode spécifique avait été autorisée, le titulaire du GSM était connu, mais pas son numéro. Ce numéro ne pouvait être connu qu'après l'analyse des résultats de deux autres méthodes spécifiques. La Commission BIM était d'avis que de cette manière, l'autorisation du service de renseignement concerné ne permettait pas de vérifier le respect de la proportionnalité et plus particulièrement de la subsidiarité. Le Comité permanent R a toutefois jugé que dans ce dossier, il n'était pas nécessaire de connaître le numéro de GSM au préalable pour évaluer la proportionnalité « *puisque l'on connaît l'identité de son titulaire (à savoir la cible) et les circonstances qui motivent le recours à cette méthode* ».

III.3.2.6. L'exigence de subsidiarité

Quatre décisions concernaient la question de savoir si la finalité visée par une méthode pouvait aussi être atteinte d'une manière moins intrusive.

Comme déjà mentionné ci-avant, un service de renseignement souhaitait mettre en œuvre une méthode spécifique afin de retrouver la trace du GSM volé d'un parlementaire belge. Selon le Comité, l'autorisation n'était pas suffisamment motivée (voir III.3.2.2.1) et l'exigence de subsidiarité n'était pas non plus satisfaite : le but, c'est-à-dire protéger les données enregistrées dans le GSM, pouvait en effet tout aussi bien être atteint par une simple intervention de l'opérateur, et ne nécessitait donc pas l'utilisation d'une méthode spécifique.

Dans le deuxième cas, qui a aussi été abordé précédemment (voir III.3.2.5.1), le service de renseignement concerné voulait contrôler des données bancaires qui couvraient une très longue période (plus de 15 ans). Les cibles étaient soupçonnées d'espionnage en Belgique et à l'étranger. Vu qu'en l'espèce, le seul moyen de connaître le réseau et le *modus operandi* de ces personnes consistait à examiner leurs comptes bancaires depuis leur installation en Belgique, l'exigence de subsidiarité était satisfaite dans ce cas.

Dans un troisième dossier, le service de renseignement concerné voulait prendre connaissance de données d'appel de et vers un fax qui était utilisé par un centre d'études (dossier 2011/484). Il souhaitait vérifier si ce centre avait reçu une invitation à participer à une conférence internationale sur la technologie de pointe dans un pays suivi dans le cadre de la lutte contre la prolifération. Le service de renseignement a affirmé qu'il était impossible d'obtenir, dans de brefs délais, une confirmation que le centre avait effectivement reçu une invitation, et ce en ayant recours à des méthodes ordinaires. Il a dès lors estimé que l'utilisation de ces méthodes spécifiques s'imposait. Bien que le Comité permanent R ait constaté que le service de renseignement ne sortait pas de sa mission légale (en l'espèce cela concernait la lutte contre la prolifération), il a conclu que l'utilisation d'une méthode ordinaire *« ne paraît pas insurmontable en l'occurrence »*. Les faits l'ont démontré par la suite : étant donné que la méthode spécifique ne donnait aucun résultat, le service de renseignement s'est directement adressé au centre concerné. Aussi, vu le fait que le centre d'études ne constitue pas une cible du service de renseignement, mais plutôt une éventuelle victime de tentatives d'approche par certains pays, le Comité a-t-il estimé que le principe de subsidiarité n'était pas respecté.

Dans le dernier dossier, le dirigeant du service de renseignement avait autorisé, outre le repérage de données de communication, l'identification immédiate de certains numéros de téléphone (dossier 2011/830 – voir aussi III.3.2.1.1). La Commission BIM avait cependant constaté qu'elle pouvait elle-même identifier une partie des numéros via le numéro 1207 (c'est-à-dire certains numéros de téléphone fixes). Les conditions de subsidiarité n'étaient donc pas remplies. Le Comité permanent R s'est rangé à l'avis de la Commission BIM, mais a précisé que le défaut de subsidiarité de la décision ne concernait que les numéros de téléphone fixes et pas les numéros de GSM.

III.4. CONCLUSIONS

En ce qui concerne la première année de pleine opérationnalité de la Loi MRD, le Comité permanent R est en mesure de formuler les conclusions générales suivantes :

- la nouvelle mission de contrôle assignée au Comité requiert un investissement considérable en temps et en moyens, mais elle constitue clairement une plus-value, et ce à deux niveaux. D'une part, le Comité contribue à la légalité des interventions de la VSSE et du SGRS et ainsi à la protection des libertés et droits fondamentaux. D'autre part, le contrôle MRD permet d'avoir une vue plus complète du fonctionnement des services de renseignement, ce qui profite certainement à la mission de contrôle classique du Comité.
- la VSSE semble faire un usage équilibré des nouvelles compétences relatives à la mise en œuvre de méthodes particulières de renseignement. Elle n'utilise les méthodes exceptionnelles, très intrusives, dans le respect de la loi, qu'« à titre exceptionnel ». En outre, le service est attentif à la rédaction des autorisations (meilleure motivation et contextualisation), même si cela se traduit par une charge de travail administratif considérable ;
- on ne peut pas encore tirer les mêmes conclusions pour le SGRS. Nonobstant le nombre très limité d'autorisations, la rédaction de celles-ci n'était pas toujours précise, même si le service s'efforce d'y remédier. Le Comité permanent R accordera une attention particulière à ces constatations dans les prochains rapports ;
- il n'est pas encore possible de faire utilement rapport sur les « résultats obtenus » via les méthodes particulières.
- la loi n'offre pas de cadre clair, uniforme et opérationnel pour la mise en œuvre de méthodes particulières dans des situations d'extrême urgence (voir III.1.1, III.2.1.1, III.3.2.1.7 et III.3.2.3.1).

CHAPITRE IV.
LE CONTRÔLE DE L'INTERCEPTION DE COMMUNICATIONS ÉMISES À L'ÉTRANGER

Depuis le début de l'année 2011, la VSSE et le SGRS peuvent tous deux écouter des communications, en prendre connaissance et les enregistrer, mais dans des conditions très strictes (art. 18/17 § 1er L.R&S). De telles « interceptions de sécurité » requièrent en principe l'accord préalable de la Commission BIM et sont toujours soumises au contrôle juridictionnel du Comité permanent R.[120] Par ailleurs, ils ne peuvent y être autorisés que pour des méthodes mises en œuvre « *sur le territoire du Royaume* » (art. 18/1 L.R&S).

Il convient de distinguer les « interceptions MRD » de « *la recherche*[121]*, la captation, l'écoute, la prise de connaissance ou l'enregistrement, par le Service Général du Renseignement et de la Sécurité des Forces armées de toute forme de communications émises à l'étranger* ». Le SGRS peut procéder à cette forme d'écoute tant à des fins militaires dans le cadre des missions définies à l'article 11 § 2, 1° et 2°, L.R&S, que pour des motifs de sécurité et de protection des troupes belges et de celles de nos alliés lors de missions à l'étranger et de nos ressortissants établis à l'étranger (art. 11 § 2, 3° et 4°, L.R&S). Ces écoutes sont généralement désignées par l'appellation « interceptions de sécurité », mais sont soumises à un tout autre cadre de contrôle. Ce contrôle est en effet exclusivement confié au Comité permanent R, et ce à la fois avant, pendant et après les interceptions (art. 44*bis* L.R&S). Le Comité est chargé ici de faire cesser les interceptions en cours lorsqu'il apparaît que les conditions dans lesquelles elles sont effectuées ne respectent pas les dispositions légales et/ou l'autorisation ministérielle (art. 44*ter* L.R&S). Chaque année, au début du mois de décembre, le SGRS doit en effet présenter au ministre de la Défense sa liste motivée d'organisations ou d'institutions dont les communications qui feront l'objet d'interceptions dans le courant de l'année à venir, et ce dans le but d'octroyer à ces interceptions l'autorisation ministérielle. Le ministre doit prendre sa décision dans les dix jours ouvrables et la communiquer au SGRS. Ensuite, le SGRS est

120 Voir, pour de plus amples détails à cet égard, le Chapitre III du *Rapport d'activités 2010*, p. 49-71.

121 La possibilité de recherche n'a été introduite légalement qu'en 2010.

tenu de transmettre la liste et l'autorisation ministérielle y afférente au Comité permanent R. C'est au moyen de cette liste annuelle que le Comité effectue son « contrôle préalable à l'interception ».

L'an passé, le Comité a insisté sur le respect strict des délais légaux. Pour 2011, le Comité a disposé à temps des documents requis. Les descriptions de processus SIGINT[122] demandées par le Comité ont également été finalisées dans le courant de l'année 2011.[123]

Comme la loi le requiert, le Comité a également procédé, en 2011, à une visite (inopinée) des installations où le SGRS effectue ses missions d'interception. À cette occasion, le Comité a vérifié le journal de bord et a contrôlé les présences, ainsi que l'utilisation et la sécurisation des locaux.

Le Comité n'a pu constater ni l'écoute ni l'exploitation de communications qui ne correspondent pas à la liste des sources approuvées par le ministre de la Défense. L'examen du journal de bord n'a mis au jour aucune irrégularité. Le Comité a toutefois remarqué que la liste des interceptions mentionnait également un « phénomène ». Or l'écoute et la prise de connaissance de communications ne sont autorisées que si elles portent sur des « organisations et institutions » (art. 44*bis* L.R&S) et, naturellement, si elles s'inscrivent dans le cadre des missions du SGRS. Le service a souligné qu'il en tiendrait compte lors de la rédaction de son prochain plan d'écoute.

122 *Signals Intelligence*.

123 Le Comité avait déjà insisté sur ce point à plusieurs reprises. Voir également Chapitre I.1.8.

CHAPITRE V.
AVIS, ÉTUDES ET AUTRES ACTIVITÉS

Le présent chapitre s'intéresse tout d'abord à la mission consultative du Comité permanent R. En 2011, le Comité a rendu trois avis spécifiques sous la forme d'une analyse juridique, d'une proposition de résolution et d'un projet d'arrêté royal (de V.1 à V.3). Ce chapitre reprend ensuite plusieurs autres activités qui ont eu un impact non négligeable sur le fonctionnement du Comité (de V.4 à V.7).

V.1. LA RÉGLEMENTATION LÉGALE EN MATIÈRE D'ARCHIVAGE ET DE DESTRUCTION DE DONNÉES DE LA VSSE ET DU SGRS

Après un certain temps, les données recueillies et traitées n'ont généralement plus de valeur pour les services de renseignement. Il convient alors de décider de leur destruction ou de leur archivage.

Cette thématique est principalement régie par la Loi relative aux archives du 24 juin 1955 et ses arrêtés d'exécution.[124] Mais de nombreuses autres lois s'avèrent tout aussi pertinentes en la matière, particulièrement en ce qui concerne les services de renseignement : la Loi relative au traitement des données à caractère personnel du 8 décembre 1992, la Loi relative à la publicité de l'administration du 11 avril 1994, la Loi relative à la classification du 11 décembre 1998, et la Loi organique des services de renseignement et de sécurité du 30 novembre 1998.

Etant donné les implications inévitables de cette législation sur l'efficacité du fonctionnement des services de renseignement et sur la vie privée des personnes qui figurent dans les fichiers de ces services, le Comité permanent R a consacré une analyse juridique à ce thème. Elle a été transmise à la VSSE et au SGRS à la mi-septembre 2011.

---

124 L'A.R. du 18 août 2010 portant exécution des articles 1er, 5 et 6*bis* de la loi du 24 juin 1955 relative aux archives (AR Archives I) et l'A.R. du 18 août 2010 portant exécution des articles 5 et 6 de la loi du 24 juin 1955 relative aux archives (AR Archives II).

Cette analyse[125] a démontré que les différentes lois, qui régissent chacune un aspect de la problématique de la destruction et l'archivage de documents des services de renseignement, sont complémentaires et opérationnelles, car le champ d'application de la Loi relative aux archives se limite aux « archives mortes ». Le Comité permanent R a en outre estimé que les divers intérêts en jeu sont parfaitement conciliables, si les services de renseignement respectent l'esprit et la lettre des différentes dispositions discutées (par exemple, signaler en tant que tels les documents qui ne présentent plus aucune utilité et déclassifier si possible les informations). Le Comité a néanmoins prôné l'instauration d'un système où les classifications prennent fin de plein droit après un délai donné (par exemple, 30 ans pour les documents classifiés « secrets » et 50 ans pour les documents « très secrets »), à moins qu'elles ne soient explicitement renouvelées. Il convient dès lors de modifier la loi relative à la classification.

V.2. AVIS RELATIF À DES ANALYSES DE MENACES POUR DES ENTREPRISES PRIVÉES

Lors d'une enquête de contrôle conjointe menée en 2009, les Comités permanents P et R ont estimé que la communication d'évaluations en matière d'extrémisme et de terrorisme par l'Organe de coordination pour l'analyse de la menace (OCAM) à des entreprises privées ne coulait pas de source, et ce en vertu des articles 3 et 10 de la Loi du 10 juillet 2006 relative à l'analyse de la menace (L.OCAM).[126]

A la suite de la discussion parlementaire du *Rapport d'activités 2010* du Comité permanent R, les Commissions de suivi de la Chambre et du Sénat ont jugé opportun que des entreprises qui emploient des Belges à l'étranger aient également connaissance de certaines évaluations relatives à des menaces terroristes et extrémistes. Les Commissions de suivi ont dès lors demandé aux Comités d'élaborer une proposition de réglementation afin de répondre à cette préoccupation.

Les Comités ont rédigé un projet de réglementation devant permettre à l'OCAM de réaliser une évaluation ponctuelle à la demande des entreprises concernées.[127] Il reviendrait au ministre des Affaires étrangères d'apprécier si la demande motivée de l'entreprise relève de la mission légale de l'OCAM. En

---

125 La version intégrale de cette analyse est reprise à l'annexe E du présent rapport d'activités (« La réglementation légale en matière d'archivage et de destruction de données de la VSSE et du SGRS »).

126 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 42.

127 Pour remédier à cette problématique, il n'était pas nécessaire de modifier la Loi du 10 juillet 2006. Les Comités ont proposé d'insérer un « Chapitre I*bis* » dans l'Arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace.

outre, ce projet prévoit la possibilité d'informer les entreprises des résultats de certaines évaluations, et ce dans le respect de la confidentialité des informations classifiées. Ce projet a été transmis aux présidents de la Chambre et du Sénat.

V.3. PROPOSITION DE RÉSOLUTION EN MATIÈRE DE PROTECTION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

A la mi-2011, le Comité a présenté à la Commission de suivi du Sénat son enquête de contrôle « *sur la manière dont les services de renseignement belges envisagent la nécessité de protéger les systèmes d'information et de communication contre des interceptions et cyberattaques d'origine étrangère* » (voir II.2). Cette enquête a entre autres révélé que les menaces auxquelles les systèmes d'information et de communication belges sont exposés peuvent porter atteinte à la sécurité et aux intérêts fondamentaux de l'État. Elle a également mis au jour l'absence de stratégie fédérale globale en matière de protection des systèmes d'information et de communication.

A la suite de la discussion des résultats de l'enquête, la Commission sénatoriale a exprimé son intention de porter cette situation à l'attention du gouvernement. Elle a demandé au Comité de rédiger une note en la matière.

Dans cette note, il est demandé au gouvernement d'élaborer une stratégie fédérale pour la protection des systèmes d'information et de communication, de créer à cette fin une agence, et de désigner une autorité qui serait chargée de la certification et de l'homologation des systèmes qui traitent des informations sensibles. L'accord gouvernemental du 1er décembre 2011 a formulé ces demandes de la manière suivante : « *Afin de donner suite aux recommandations du Comité R, le Gouvernement élaborera une stratégie fédérale de sécurité des réseaux et systèmes d'information, dans le respect de la protection de la vie privée* ».

V.4. DOSSIERS D'INFORMATION

Outre les enquêtes de contrôle, le Comité permanent R ouvre également des « dossiers d'information ». Ces dossiers visent à apporter une réponse structurée à des éléments relatifs au fonctionnement des services de renseignement et de l'OCAM émanant de sources diverses.[128] Ces dossiers et la manière dont ils sont

[128] Le Comité permanent R peut ouvrir un dossier d'information pour des raisons très diverses : une plainte a été déposée et le Comité permanent R souhaite exclure le plus rapidement possible l'absence manifeste de fondement. La direction d'un service de renseignement fait état d'un incident et le Comité souhaite contrôler comment cet incident a été traité. Autre

traités présentent l'avantage d'offrir un large suivi du secteur du renseignement avec un minimum d'exigences de forme. Si de tels dossiers révèlent des indices de dysfonctionnement ou des aspects du fonctionnement des services de renseignement qui requièrent un examen approfondi, le Comité procède naturellement à l'ouverture d'une enquête de contrôle. En revanche, s'il apparaît clairement qu'une telle enquête n'apporterait aucune plus-value au regard des objectifs du Comité permanent R, le dossier d'information est clôturé.

En 2011, le Comité s'est penché, dans ce cadre, sur différents incidents isolés au sein des services de renseignement (par exemple des incidents de sécurité), sur certains aspects du fonctionnement du service Protection de la VSSE, et sur la problématique de l'appartenance à une bande criminelle de motards à la lumière de la réglementation en matière d'habilitations de sécurité.

V.5. LA CONFÉRENCE DES ORGANES DE CONTRÔLE EUROPÉENS ET LE *EUROPEAN NETWORK OF NATIONAL INTELLIGENCE REVIEWERS* (ENNIR)

La *7e Conférence des commissions parlementaires de contrôle des services de renseignements et de sécurité des États membres de l'Union européenne, de la Norvège et de la Suisse* s'est tenue les 27 et 28 octobre 2011 à Berlin. Quelque vingt délégations ont participé à cette conférence. Les débats ont été menés autour de thèmes tels que les défis des services de renseignement vingt ans après la Guerre froide ; le droit à l'information des parlementaires dans le cadre des activités des services de renseignement ; le contrôle parlementaire des activités de renseignement (concurrence ou complémentarité du contrôle administratif et parlementaire, compétences, moyens, etc.) ; le contrôle parlementaire à l'échelle nationale comparé à la collaboration internationale entre services de renseignement.

La délégation belge a expliqué les étapes entreprises dans le cadre de la réalisation du *European Network of National Intelligence Reviewers (ENNIR)*.[129] Ce projet initié par le Comité permanent R porte sur la création d'un réseau (sous la forme d'un site Internet commun) d'échange d'informations entre les commissions parlementaires et/ou les organes de contrôle des services de

exemple : les médias signalent un évènement et le Comité souhaite déterminer si ces faits sont conformes à la réalité et s'ils relèvent d'une problématique plus générale, etc.

129 Auparavant, les différents participants s'étaient montrés prêts à collaborer à la poursuite de la mise en œuvre de cette initiative dans le courant de l'année 2011. Voir à cet égard COMITÉ PERMANENT R, *Rapport d'activités 2010*, 81-82 et Annexe D. La création d'ENNIR a également été abordée lors de la *EU Speakers Conference* qui s'est tenue du 3 au 5 avril 2011 au parlement belge (www.europarl.europa.eu/webnp/cms/pid/1593).

renseignement et de sécurité dans l'Union européenne. Lors de cette conférence, la délégation, composée de deux sénateurs de la Commission de suivi et de représentants du Comité permanent R, a également présenté un projet de « *Guidelines* ». Dans la « Déclaration de Berlin », les différents participants ont déclaré qu'ils acceptaient de participer activement à cette initiative belge et de contribuer à son développement. Le site Internet *(www.ennir.be*) est actif depuis le 12 décembre 2011. Une brochure a été envoyée à tous les États membres de l'Union européenne, à la Norvège et à la Suisse afin de promouvoir le réseau. Cette campagne de promotion a porté ses fruits, puisque dans l'intervalle, outre la Belgique, les Pays-Bas, le Luxembourg et le Portugal ont formellement promis de collaborer à cette initiative, tandis que de nombreux autres pays ont également manifesté leur intérêt.

V.6. COLLABORATION À UNE ÉTUDE EUROPÉENNE EN MATIÈRE DE CONTRÔLE PARLEMENTAIRE DES SERVICES DE RENSEIGNEMENT

Pour le compte du Parlement européen, le *Geneva Centre for the Democratic Control of Armed Forces (DCAF)* et l'*European University Institute (EUI)* ont mené une étude sur la « *Surveillance parlementaire des agences de sécurité et de renseignement dans l'Union européenne* ».[130] Cette étude évalue la surveillance des services nationaux de renseignement et de sécurité par les parlements et les organes de contrôle non parlementaires spécialisés. Son objectif consistait à identifier des *good practices* de manière telle que le Parlement européen puisse améliorer sa propre surveillance d'Europol, d'Eurojust, de Frontex et de Sitcen.

Le Comité permanent R a participé étroitement à cette étude. Il a d'abord été invité à répondre à un questionnaire détaillé sur ses missions, ses compétences et ses moyens. Le Comité a également fait partie du *Project advisory board* et a fait part de ses réflexions, en cette qualité, concernant plusieurs autres contributions à l'étude.[131]

---

130 A. WILLS et M. VERMEULEN, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 2011, 442 p. (http://www.europarl.europa.eu/activities/committees/studies.do?language=EN).

131 La Belgique a été choisie avec onze autres pays pour décrire de manière plus détaillée le déroulement du contrôle parlementaire et spécialisé des services de renseignement. Voir à cet égard W. VAN LAETHEM, « Parliamentary And Specialised Oversight Of Security And Intelligence Agencies In Belgium», in A. WILLS et M. VERMEULEN (eds.), *Parliamentary Oversight Of Security And Intelligence Agencies In The European Union*, 2011, 191-203.

V.7. EXPERT DANS DIVERS FORUMS

Comme les années précédentes, le Comité permanent R a été sollicité à plusieurs reprises en tant qu'expert dans le cadre de forums nationaux et internationaux.

Au niveau international, le Comité a répondu, début mai 2011, à l'invitation de l'*Open Society Justice Initiative* à Genève et a participé à une conférence à huis clos, au cours de laquelle la position d'information des organes de contrôle a été examinée en profondeur.

Dans le prolongement, le Comité a répondu, en décembre 2011, à une invitation de la *Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* (CTIVD) néerlandaise, du *Geneva Centre for the Democratic Control of Armed Forces* (DCAF) et du *Clingendael Institute* et a expliqué, avec un nombre restreint d'autres organes de contrôle européens, l'organisation pratique du contrôle des services de renseignement à une délégation des Balkans (« *Strenghtening Intelligence Oversight in the Western Balkans* », La Haye).

À la mi-mars, le Comité a organisé une réunion de travail à huis clos à La Haye avec ses collègues des organes de contrôle néerlandais, norvégien et suédois, en vue d'un échange mutuel de *best practices*.

Le Comité permanent R a également participé à l'organisation de la *Community of Interest on the Practice and Organization of Intelligence (COI POI*[132]*)* qui s'est tenue à Anvers (octobre 2011), avec pour thème central l'« *Analytic Management for Surprise and Crisis Response* ». La contribution du représentant du Comité permanent R s'intitulait « *Oversight Perspectives on Surprise and Crisis Response* ».

Au niveau bilatéral, le Comité a pris part au *Groupe européen de recherche sur l'éthique du renseignement (GERER)*. Ce groupe de travail a été créé à l'initiative de l'*École française de Saint-Cyr Coëtquidan* et l'École royale militaire (ERM), et bénéficie du soutien de la *Fondation Saint-Cyr.* Composé d'universitaires et de professionnels (représentants des services de renseignement français (militaire) et belges, du Comité permanent R, etc.), ce groupe entend mener une réflexion sur la relation entre l'éthique et le renseignement. Les travaux de ce groupe ont donné lieu à une première publication en 2011.[133]

Au niveau national, le Comité permanent R a veillé au redémarrage du *Belgian Intelligence Studies Centre* (*BISC*). Ce centre d'études sur le renseignement souhaite rapprocher les services de renseignement et de sécurité de la communauté scientifique, et contribuer à la résolution des questions sociales dans le domaine du renseignement. Dans cette optique, le BISC a organisé deux après-midis d'études sur les thèmes suivants : « Services de

132 Voir à cet égard COMITÉ PERMANENT R, *Rapport d'activités 2008*, 86.

133 Groupe européen de recherche en éthique et renseignement (GERER), sous la direction de T. PICHEVIN, Éthique et renseignement. *La difficile cohabitation du bien et de la nécessité*, Paris, Éditions ESKA, 2011, 141.

renseignement et de sécurité : histoire et perspective » (mars 2011) et « Renseignement et éthique : oxymore » (décembre 2011).

Enfin, les travaux menés dans le cadre du Groupe de travail Analyse se sont poursuivis. Composé de représentants de la VSSE et du SGRS, et fort du soutien du Comité permanent R, ce groupe de travail s'est penché sur les propositions relatives à la formation (de base et avancée) des analystes tant pour le service de renseignement civil que militaire.

V.8. SÉANCE ACADÉMIQUE

En 2011, la traditionnelle séance académique annuelle du Comité permanent R était consacrée au contrôle des méthodes de recueil des données. Trois niveaux ont été abordés dans ce cadre. Rémi Récio, délégué général de la *Commission nationale de contrôle des interceptions de sécurité* (CNCIS), a expliqué la manière dont le contrôle des interceptions est organisé outre-Quiévrain. Pour une perspective internationale, le Comité a pu faire appel au *Rapporteur spécial de l'ONU sur la protection des droits de l'homme dans le cadre de la lutte contre le terrorisme*, prof. Martin Scheinin. Peter De Smet, conseiller au Comité permanent R, a présenté les résultats des quatre premiers mois de mise en œuvre de la loi MRD.

CHAPITRE VI.
LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Parallèlement aux enquêtes de contrôle, le service d'Enquêtes R du Comité permanent R effectue également, à la demande des autorités judiciaires, des enquêtes sur des membres des services de renseignement soupçonnés d'avoir commis un crime ou un délit. Cette compétence est décrite à l'article 40, alinéa 3 de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace. La loi du 10 juillet 2006 relative à l'analyse de la menace élargit cette compétence aux crimes et délits imputés à des membres de l'Organe de coordination pour l'analyse de la menace (OCAM). En ce qui concerne les membres des autres « services d'appui », cette disposition s'applique uniquement à l'obligation de communiquer à l'OCAM tout renseignement pertinent (art. 6 et 14 L.OCAM).

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le directeur du service d'Enquête R sont soumis à la surveillance du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a alors aucune autorité sur eux. Le président du Comité permanent R doit toutefois veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle. Les raisons sont évidentes : l'organe de contrôle est avant tout à la disposition du Parlement. Cette mission pourrait être mise en péril si l'organe consacrait une trop grande partie de son temps à des dossiers judiciaires. Le président peut, le cas échéant, se concerter avec les autorités judiciaires quant à la participation des membres du service d'Enquêtes R à des enquêtes pénales (art. 61*bis* L.Contrôle). Le nombre restreint d'enquêtes pénales n'a encore jamais rendu cette concertation nécessaire.

Dans les situations où le service d'Enquêtes R effectue des enquêtes pénales, le directeur doit remettre un rapport au Comité permanent R au terme de chaque enquête. Dans ce cas, « *le rapport se limite aux informations qui sont nécessaires à l'accomplissement par le Comité permanent R de ses missions* » (art. 43, alinéa 3, L.Contrôle).

En 2011, la plupart des missions judiciaires menées par le service d'Enquêtes R concernaient un dossier ouvert auprès des autorités judiciaires de Liège. Le service d'Enquêtes R a enquêté avec la police judiciaire fédérale de Liège sur une

éventuelle implication d'un ou de plusieurs membres d'un service de renseignement dans des faits punissables.

En outre, à la fin de l'année 2011, le service d'Enquêtes R a été chargé par le parquet fédéral d'une mission dans le cadre d'une information judicaire relative à une suspicion de fraude dans le chef d'un agent de renseignement.

CHAPITRE VII.
LE GREFFE DE L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ

Le président du Comité permanent R assure également la présidence de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité.[134] La fonction de greffe est exercée par le greffier (ou son suppléant) et par l'administration du Comité permanent R.

L'Organe de recours est compétent pour les contentieux qui portent sur des décisions dans quatre domaines : les habilitations de sécurité, les attestations de sécurité qui doivent octroyer l'accès à des lieux où se trouvent des documents classifiés, les attestations de sécurité qui permettent l'accès à des lieux précis faisant l'objet de menaces et, enfin, les avis de sécurité. L'Organe de recours intervient également en tant que « juge d'annulation » contre des décisions d'autorités publiques ou administratives lorsqu'elles exigent des avis ou des attestations de sécurité pour un secteur, un lieu ou un évènement donné.[135]

Ces activités de l'Organe de recours ont un impact direct tant sur le budget que sur le personnel du Comité permanent R. En effet, tous les frais de fonctionnement sont supportés par le Comité permanent R, qui met à disposition non seulement le président et le greffier, mais aussi le personnel administratif nécessaire, qui doit se charger des tâches chronophages liées à la préparation, au traitement et au règlement des recours.

Ce chapitre mentionne les chiffres relatifs à la nature des décisions contestées, la qualité des autorités compétentes et des requérants, ainsi que la nature des décisions de l'Organe de recours dans le cadre des différentes procédures de recours. À des fins de comparaison, les chiffres de ces deux dernières années sont également indiqués.

En 2011, le nombre de recours et de décisions a légèrement diminué par rapport à 2010 : 71 recours contre 83 et 70 décisions contre 85. Aucune tendance marquante ne s'est dégagée de l'ensemble. Enfin, l'on peut encore mentionner

---

134 En son absence, la présidence est assurée par le conseiller du Comité permanent R qui a en outre la qualité de magistrat.

135 Pour plus de détails, voir COMITÉ PERMANENT R, *Rapport d'activités 2006*, 87-115.

qu'à la mi-2011, l'Organe de recours a reçu la visite du secrétaire du *Security Vetting Appeals Panel* britannique. Il a donné un exposé sur la manière dont le recours contre les screenings de sécurité négatifs est organisé en Grande-Bretagne. La comparaison entre les deux systèmes s'est révélée intéressante.

Tableau 1. Autorités de sécurité concernées

	2009	2010	2011
ANS	18	36	21
VSSE	2	3	2
SGRS	19	33	39
DGCC	0	0	0
AFCN	5	5	7
Police fédérale	1	0	1
Police locale	0	0	0
Commission aéroportuaire locale[136]	3	5	1
Inconnu	0	1	0
TOTAL	**48**	**83**	**71**

Tableau 2. Nature des décisions contestées

	2009	2010	2011
Habilitations de sécurité			
Confidentiel	7	13	14
Secret	18	38	31
Très secret	7	9	9
Total habilitations de sécurité	32	60	54
Refus	25	47	32
Retrait	5	12	21
Habilitation pour une durée limitée	1	1	0

136 Dans chaque aéroport, la Direction générale du Transport aérien a désigné une commission aéroportuaire locale. À titre de mesure transitoire, cette commission délivre des avis de sécurité aux personnes qui doivent disposer d'un badge d'identification au sein de l'aéroport. Vu l'A.R. du 22 mars 2011 modifiant l'Arrêté royal du 3 juin 2005 modifiant l'Arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations de sécurité (*MB* 2 mai 2011), ces commissions sont compétentes pour les demandes de badges d'identification formulées avant le 31 décembre 2011.

	2009	2010	2011
Habilitation pour un niveau inférieur	1	0	1
Pas de décision dans les délais	0	0	0
Pas de décision dans les nouveaux délais	0	0	0
Total habilitations de sécurité	32	60	54
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	**32**	**60**	**54**
Attestations de sécurité documents classifiés			
Refus	4	1	0
Retrait	0	0	0
Pas de décision dans les délais	0	0	0
Attestations de sécurité lieu ou évènement			
Refus	9	14	14
Retrait	0	0	0
Pas de décision dans le délai	0	0	0
Avis de sécurité	0	0	0
Avis négatif	6	8	3
« Révocation » d'un avis positif	0	0	0
Actes normatifs d'une autorité administrative		0	0
Décision d'une autorité publique d'exiger des attestations	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des attestations	0	0	0
Décision d'une autorité administrative d'exiger des avis	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des avis	0	0	0
SOUS-TOTAL ATTESTATIONS ET AVIS	**16**	**23**	**17**
TOTAL DÉCISIONS CONTESTÉES	**48**	**83**	**71**

Tableau 3. Nature du requérant

	2009	2010	2011
Fonctionnaire	3	10	4
Militaire	19	31	37
Particulier	26	39	29
Personne morale	0	3	1

Tableau 4. Langue du requérant

	2009	2010	2011
Francophone	28	39	32
Néerlandophone	20	44	39
Germanophone	0	0	0
Autre langue	0	0	0

Tableau 5. Nature des décisions interlocutoires prises par l'Organe de recours[137]

	2009	2010	2011
Demande du dossier complet (1)	48	82	68
Demande d'informations complémentaires (2)	6	13	5
Audition d'un membre d'une autorité (3)	1	12	4
Décision du président (4)	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (5)	14	31	24
Soustraction d'informations du dossier par le service de renseignement (6)	0	0	0

(1) L'Organe de recours peut demander l'intégralité du dossier d'enquête aux autorités de sécurité. Comme ce dossier contient davantage de données que le rapport d'enquête seul, cette requête est systématique.
(2) L'Organe de recours peut également demander tout complément d'informations qu'il juge nécessaire pendant la procédure.
(3) L'Organe de recours peut décider d'entendre les membres des services de renseignement et de police ou des autorités de sécurité qui ont participé à l'enquête ou à la vérification de sécurité.
(4) Le président de l'Organe de recours peut décider que le membre du service de renseignement garde secrètes certaines données pendant son audition.
(5) Si le service de renseignement concerné le requiert, l'Organe de recours peut décider que certaines informations soient retirées du dossier qui sera communiqué au requérant.
(6) Si l'information concernée provient d'un service de renseignement étranger, c'est le service de renseignement belge qui décide si elle peut être communiquée. Il s'agit d'un aspect de l'application de la « règle du tiers service ».

137 Le « nombre de décisions interlocutoires » (tableau 5), « la manière dont le requérant fait usage de ses droits de défense » (tableau 6), ou encore la « nature des décisions de l'Organe de recours » (tableau 7) ne correspond pas nécessairement au nombre de requêtes introduites (voir tableaux 1 à 4). En effet, certains dossiers ont par exemple déjà été ouverts en 2010, alors que la décision n'est tombée qu'en 2011.

Tableau 6. Manière dont le requérant fait usage de ses droits de défense

	2009	2010	2011
Consultation du dossier par le requérant /l'avocat	32	70	48
Audition du requérant /avocat[138]	45	79	55

Tableau 7. Nature des décisions de l'Organe de recours

	2009	2010	2011
Habilitations de sécurité			
Irrecevable	1	0	5[139]
Sans objet	0	0	1
Non fondé	15	30	29
Fondé (octroi partiel ou complet)	11	29	19
Devoir d'enquête complémentaire par l'autorité	0	0	1
Délai supplémentaire pour l'autorité	0	1	0
Attestations de sécurité documents classifiés			
Irrecevable	0	0	0
Sans objet	0	0	0
Non fondé	0	0	0
Fondé (octroi)	0	0	0
Attestations de sécurité lieu ou évènement			
Irrecevable	0	1	1
Sans objet	0	0	0
Non fondé	6	7	7
Fondé (octroi)	4	8	4
Avis de sécurité			
Non compétent	1	0	0
Irrecevable	0	0	0
Sans objet	1	1	0
Avis négatif	2	7	0
Avis positif	2	1	3

138 Dans le cadre de certains dossiers, le requérant/avocat est auditionné à plusieurs reprises.
139 Dans les cinq cas, le recours a été introduit tardivement.

	2009	2010	2011
Actes normatifs d'une autorité administrative			
Irrecevable	0	0	0
Sans objet	0	0	0
Fondé	0	0	0
Non fondé	0	0	0
TOTAL	**43**	**85**	**70**

CHAPITRE VIII.
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

VIII.I. COMPOSITION DU COMITÉ PERMANENT R

La composition du Comité permanent R n'a subi aucune modification en 2011. La présidence a été assurée par Guy Rapaille (F), avocat général près la cour d'appel de Liège. Les deux fonctions de conseiller ont été remplies par Gérald Vande Walle (F), fonctionnaire, et Peter De Smet, substitut du procureur général près la cour d'appel de Gand.[140]

Aucun remaniement n'est à noter au sein du service d'Enquêtes R. L'effectif de ce service, dirigé par Pierre Nivelle, est dès lors resté à 6 équivalents temps plein.

Enfin, le cadre du personnel administratif du Comité permanent R, placé sous la direction du greffier Wouter De Ridder, n'a pas été élargi et comptait toujours un total de 16 personnes. Un juriste a toutefois été employé durant neuf mois sur une base contractuelle.

VIII.2. RÉUNIONS AVEC LA OU LES COMMISSION(S) DE SUIVI

Dans le courant de l'année 2011, quatre réunions ont eu lieu avec la Commission de suivi du Sénat, à laquelle le Comité permanent R présente ses rapports et qui exerce le contrôle final sur son fonctionnement. Ces réunions ont porté sur différentes enquêtes de contrôle clôturées. Une réunion a eu lieu avec la Commission de suivi commune P et R, durant laquelle le *Rapport d'activités 2010* du Comité permanent R a été discuté.[141]

La composition de la Commission sénatoriale a subi des modifications à la fin 2011. À la présidence du Sénat et, partant, de la Commission sénatoriale de suivi, Sabine de Bethune (CD&V) a succédé à Danny Pieters (NV-A), qui est

---

140 Malgré un appel lancé dans le Moniteur (*MB* 3 décembre 2010), les présidents suppléants et les deux deuxièmes conseillers suppléants n'ont pas encore été désignés.

141 *Doc. parl.* Sénat 2010-11, n° 5-1080/1, et *Doc. parl.* Chambre 2010-11, n° 53-1695/1.

toutefois resté membre[142] en remplacement de Liesbeth Homans (NV-A). Armand De Decker (MR), Philippe Mahoux (PS) et Dirk Claes (CD&V) font également partie de cette commission. La commission, dans sa nouvelle composition, a visité le nouveau siège du Comité dans le bâtiment du Forum à la mi-décembre 2011.

VIII.3. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

Les articles 52 à 55 L.Contrôle stipulent les cas où et la manière dont le Comité permanent R et le Comité permanent P doivent organiser des réunions communes. Ces réunions poursuivent un double objectif: l'échange d'informations et la discussion des enquêtes de contrôle communes. En 2011, six réunions communes ont eu lieu. L'ordre du jour de ces réunions portait, entre autres, sur l'extension de la compétence d'évaluation de l'OCAM à l'égard des entreprises privées et sur l'éventuel caractère opposable du secret de l'enquête pénale au contrôle du Comité permanent R. Toutes les enquêtes communes portaient sur des aspects du fonctionnement de l'OCAM.[143]

VIII.4. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Pour l'année d'activité 2011, le Comité permanent R a bénéficié d'une dotation de 4,5 millions d'euros contre 4 millions d'euros en 2010. Cette hausse s'est justifiée par les nouvelles tâches résultant de la Loi MRD et par l'augmentation de la charge de travail de ces dernières années dans le cadre de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. En outre, en 2011, le Comité a déménagé son siège vers le « Forum », un complexe dont la Chambre des Représentants est propriétaire. Les travaux d'adaptation requis en matière de sécurisation du nouveau site, le déménagement proprement dit et le fait que le Comité a dû continuer à s'acquitter du loyer des anciens locaux durant un semestre ont engendré un surcoût unique considérable. Ce coût additionnel a été porté au budget 2011 et financé en partie (avec l'accord de la Commission de la comptabilité de la Chambre) avec le boni que le Comité a réalisé durant l'année d'activité 2009.[144]

---

142 *Annales* Sénat, 2010-11, 10 novembre 2011, n° 5-34, 38-39.

143 Voir Chapitre II.4, chapitre II.5 et chapitre II.8.

144 Lors de la réunion du 22 novembre 2011, le président du Comité permanent R a commenté les comptes 2010, l'adaptation budgétaire 2011 et le budget 2012. Voir *Doc. parl.* Chambre 2011-12, n° 53K2015/1, 21 et suiv.

VIII.5. DÉMÉNAGEMENT VERS LE NOUVEAU BÂTIMENT DU FORUM

En 2011, le Comité permanent R a déménagé de la rue de la Loi vers le nouveau bâtiment du Forum du Parlement situé rue de Louvain. Ce déménagement s'est fait à la demande du Parlement, qui souhaitait ainsi réaliser des économies d'échelle et réduire les coûts: d'une part, en réunissant au sein d'un même bâtiment différentes institutions émargeant au budget des dotations et, d'autre part, en créant des possibilités de synergie entre les institutions et avec le Parlement (par exemple, en recourant à l'imprimerie du Parlement, en collaborant plus étroitement avec la bibliothèque, etc.).

Le déménagement, qui a eu lieu fin mars, a fait l'objet de nombreux préparatifs, entre autres afin de garantir autant que possible la continuité des activités du Comité. Lors du déménagement proprement dit, il a en outre fallu veiller en permanence à la protection des documents classifiés.

Le déménagement s'est déroulé sans incident, et le Comité est redevenu opérationnel en très peu de temps.

Aujourd'hui, le Comité dispose d'une infrastructure moderne qui satisfait à toutes les normes en matière de protection et de conservation des documents classifiés.

VIII.6. FORMATION

Vu l'intérêt pour l'organisation, le Comité permanent R encourage ses collaborateurs à suivre des formations générales (informatique, gestion, etc.) ou propres au secteur. Concernant cette dernière catégorie, un ou plusieurs membres (du personnel) du Comité ont assisté aux journées d'étude mentionnées ci-dessous.

DATE	TITRE	ORGANISATION	LIEU
2011	Hautes études de sécurité et de défense	IRSD	Bruxelles
27 janvier 2011	Séance académique – Contrôle des méthodes de recueil des données	Comité permanent R	Bruxelles
15 février 2011	Menace terroriste et réponse institutionnelle	IRSD|ERM	Bruxelles
16 février 2011	Single Table lunch – Meeting with Mr Stephen Hutchins – director of Security European Commission	ECSA	Bruxelles

DATE	TITRE	ORGANISATION	LIEU
21 février 2011	Woordvoerders, persattachés en communicatieverantwoordelijken	Politeia|Kortom|VVSG	Bruxelles
1er mars 2011	Services de renseignement et de sécurité : histoire et perspective	Belgian Intelligence Studies Centre (BISC)	Bruxelles
17 et 18 mars 2011	Meeting – Intelligence Oversight Committees (Suède, Norvège, Belgique et Pays-Bas)	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)	La Haye
25 mars 2011	De Wapenwet en zijn praktijk	KU Leuven|UGent	Louvain
4 avril 2011	Usages et mésusages du fichier STIC par les forces de l'ordre	Métis	Paris
27 avril 2011	L'utilisation de Google dans l'enquête policière – Faire des recherches sur Internet : qu'est-il possible et qu'est-il permis ?	Police judiciaire fédérale|Politeia	Bruxelles
27 avril 2011	Le Printemps arabe en question	IRSD	Bruxelles
3 mai 2011	La loi sur la vie privée dans la pratique policière quotidienne	Politeia|Commission de la protection de la vie privée	Hélécine
4 – 5 mai 2011	Workshop – Open Society Justice Initiative	DCAF|Open Society Institute (OSI)	Montreux
9 mai 2011	Les procédures de création et de contrôle des fichiers des organes de renseignement	Métis	Paris
13 mai 2011	Le point sur l'archivage électronique	JuriTIC|CRIDS|FUNDP	Namur
19 mai 2011	Défis et opportunités pour l'agenda de l'énergie nucléaire et le régime de non-prolifération	IRSD	Bruxelles
16 juin 2011	The importance of a secure work environment	ECSA	Bruxelles
20 – 24 juin 2011	Forum interdépartemental – Optimalisation de la sécurité dans l'exécution des tâches policières en rationalisant l'usage d'une contrainte proportionnée	Police fédérale|(Police judiciaire Arlon)	Arlon
7 septembre 2011	Activités de renseignement et activités de police	Fastes, Police de Liège	Liège
22 septembre 2011	Militaire uitgaven belicht	Vlaams Vredesinstituut|i.s.m. Vlaams Parlement	Bruxelles
22 septembre 2011	Hautes études Police, Justice et Sécurité d'Entreprise – session 2011-2012	ECSA|ULg|UGent	Bruxelles

DATE	TITRE	ORGANISATION	LIEU
26 septembre 2011	Aux origines d'un renseignement européen. Les coopérations françaises en matière de renseignement au début de la guerre froide	Métis	Paris
30 septembre 2011	Cloud Law or Legal Cloud ?	JuriTIC|CRIDS|FUNDP	Bruxelles
10 octobre 2011	De la guerre froide à un monde durable – Mikhaïl Gorbatchev	SRIW|ULg	Liège
14 octobre 2011	11e journée BTS (DJO) – Une ouverture vers des alternatives dans l'utilisation des MPR…	Police fédérale (Direction des opérations de police judiciaire)|ERM	Bruxelles
16-18 octobre 2011	GFF – COI/POI	VSSE|SGRS|Comité permanent R	Anvers
17 octobre 2011	Incidents AMOK	École nationale des officiers (ERM)	Bruxelles
17-19 octobre 2011	4th International Risk Assessment and Horizon Scanning Symposium (IRAHSS 2011)	National Security Coordination Secretariat	Singapour
24-28 octobre 2011	10th Annual Combined Technical Surveillance Countermeasures Working Group	ACCI|SHAPE	SHAPE
27-28 octobre 2011	7th Conference of Parliamentary Committees for Oversight of Intelligence and Security Services EU	G10-Commission|Deutsche Bundestag	Berlin
14 novembre 2011	Figures du renseignement européen	Métis	Paris
16 novembre 2011	Meeting – EU SitCen	ECSA	Bruxelles
17 novembre 2011	Assises de l'Intelligence stratégique	Agence de Stimulation économique|Cercle de Wallonie	Seraing
21 novembre 2011	The Navy in the 21st Century	IRSD	Bruxelles
23 novembre 2011	Cinquième anniversaire du Conseil consultatif de la magistrature	CCM|SPF Justice	Bruxelles
23 novembre 2011	UK – SECURITY & DEFENCE CAPABILITIES Exhibition 2011	UK Trade and Investment Section of UK Embassy Brussels	Bruxelles
28 novembre 2011	Incidents AMOK – concept tactique	École nationale des Officiers|Police fédérale|ERM	Bruxelles

DATE	TITRE	ORGANISATION	LIEU
30 novembre 2011	De gerechtelijke hervorming	Koninklijke Vlaamse Academie van België	Bruxelles
1er décembre 2011	Renseignement et éthique : un oxymore ?	IRSD|BISC	Bruxelles
2 décembre 2011	International Conference – Strengthening Intelligence Oversight in the Western Balkans	CTIVD|DCAF|Clingendael Institute	La Haye
6 décembre 2011	Entre toge et uniforme – les conséquences de l'arrêt Salduz pour la police la justice et le barreau	Politeia|Fédération royale des officiers et hauts fonctionnaires de la police belge	Wépion
16 décembre 2011	Human Resources Management en Leiderschap in de publieke sector	KU Leuven	Louvain
19 décembre 2011	Le contrôle politique du renseignement en Europe	Métis	Paris

CHAPITRE IX.
RECOMMANDATIONS

À la lumière des enquêtes de contrôle clôturées en 2011, le Comité permanent R formule les recommandations suivantes. Elles portent plus particulièrement sur la protection des droits que la Constitution et la loi confèrent aux personnes (IX.1), sur la coordination et l'efficacité des services de renseignement, de l'OCAM et des services d'appui (IX.2) et, enfin, sur l'optimalisation des possibilités de contrôle du Comité permanent R (IX.3).

IX.1. RECOMMANDATIONS RELATIVES À LA PROTECTION DES DROITS QUE LA CONSTITUTION ET LA LOI CONFÈRENT AUX PERSONNES

IX.1.1. DESTRUCTION ET ARCHIVAGE DES DOCUMENTS DES SERVICES DE RENSEIGNEMENT ET DÉCLASSIFICATION AUTOMATIQUE[145]

La destruction et/ou l'archivage éventuels de documents de services de renseignement sont étroitement liés aux « *droits que la Constitution et la loi confèrent aux personnes* ». Cette problématique est régie par un grand nombre de dispositions légales. Le Comité permanent R a constaté que les différents intérêts en jeu sont parfaitement conciliables, à condition de tenir compte de la distinction entre les archives « vivantes » et les archives « mortes ». Le Comité s'est néanmoins montré en faveur d'un système où les classifications prennent fin de plein droit après un délai donné – par exemple, 30 ans pour les documents classifiés « secrets » et 50 ans pour les documents « très secrets » –, à moins qu'elles ne soient explicitement renouvelées. Ceci exige une modification de la loi relative à la classification.

[145] Voir Chapitre V.1. La réglementation légale en matière d'archivage et de destruction de données de la VSSE et du SGRS.

IX.1.2. RECOMMANDATION DANS LE CADRE DE L'INTERCEPTION DE COMMUNICATIONS ÉTRANGÈRES[146]

Le plan d'écoute du SGRS stipule que seules des organisations et institutions peuvent être prises comme cibles, pas des phénomènes. Comme l'énonce clairement l'article 44*bis* L.R&S.

IX.2. RECOMMANDATIONS RELATIVES À LA COORDINATION ET À L'EFFICACITÉ DES SERVICES DE RENSEIGNEMENT, DE L'OCAM ET DES SERVICES D'APPUI

IX.2.1. RECOMMANDATIONS RELATIVES À L'AUDIT EFFECTUÉ AU SEIN DU SGRS[147]

Dans le cadre de l'audit mené au sein du SGRS, le Comité permanent R a formulé plusieurs recommandations relatives aux conditions organisationnelles requises pour une affectation adéquate des moyens (IX.2.1.1), à la gestion et la direction du personnel (IX.2.1.2), aux flux d'informations et aux TIC (IX.2.1.3), et enfin à la gestion des risques (IX.2.1.4). À cet égard, le Comité a distingué les « recommandations de changement » (recommandations qui sont essentielles au bon fonctionnement du SGRS et qui impliquent une profonde modification de la méthode de travail actuelle ou de l'organisation) des « recommandations d'amélioration » (recommandations qui entrent davantage dans les détails d'une matière, où la méthode de travail ne doit pas subir de modifications fondamentales, mais plutôt être perfectionnée et améliorée). Ces deux types de recommandations complémentaires sont brièvement expliqués ci-dessous.

IX.2.1.1. Recommandations relatives aux conditions organisationnelles requises pour une affectation adéquate des moyens

– la fonction Personnel et Organisation (fonction P&O) du SGRS doit être renforcée d'urgence. Ce renforcement est une recommandation de changement et constitue donc une condition *sine qua non* pour que la mise en œuvre d'autres recommandations ait une chance de succès ;

146 Voir Chapitre IV. Le contrôle de l'interception de communications émises à l'étranger.
147 Voir Chapitre II.1. Audit au sein du service de renseignement militaire.

- le Comité recommande qu'un processus récurrent soit lancé pour définir des objectifs clairs formulés conformément aux critères SMART, en termes de produits à fournir et de *Service Level Agreements* (SLA) ;
- il convient de déterminer quelle est la collaboration opportune et requise entre et au sein des divisions en vue de la réalisation de ces objectifs. En outre, les utilisateurs et les « clients » externes et internes doivent pouvoir évaluer les produits et les SLA proposés ;
- la définition des produits et des SLA doit également passer par l'estimation de l'investissement humain requis en termes de temps et de compétences ;
- la gestion des compétences au sein du SGRS et l'harmonisation des tâches, fonctions et compétences requièrent une approche plus professionnelle ;
- le Comité permanent R estime que la créativité est un atout précieux pour un service de renseignement et doit être stimulée[148] ;
- pour chaque objectif, il convient d'établir un planning et de désigner les acteurs concernés, ainsi que la méthode de suivi. Il s'agit d'une recommandation de changement ;
- tous les plans de collecte doivent mentionner quelles sont les informations requises pour être en mesure d'élaborer les produits et qui peut fournir ces informations. Dans cette optique, il convient de désigner un gestionnaire de l'information et de faciliter la recherche automatisée dans les fichiers ;
- chaque division doit informer son propre personnel *et* le personnel d'autres divisions de « qui » dispose de « quelle » information et de « ce qui » peut être mis à disposition ;
- il convient d'intégrer un mécanisme de *feedback* pour tous les produits fournis. Les clients internes et externes doivent être systématiquement sondés à cet égard, afin d'avoir une meilleure vision de leurs besoins et de ce qu'ils peuvent attendre du SGRS ;
- le SGRS et la Direction générale *Material Resources* des Forces armées doivent, en fonction des budgets disponibles, tenter en permanence d'améliorer les moyens de fonctionnement et les conditions de travail. Dans ce cadre, il convient de mettre clairement l'accent sur les moyens TIC, sans pour autant négliger les aspects liés à la sécurité (sécurisation des documents, de l'infrastructure et des personnes).

IX.2.1.2. Recommandations relatives à la gestion et à la direction du personnel du SGRS

- le Comité permanent R recommande la rédaction de descriptions claires des fonctions ;

[148] Par exemple, via des cercles d'amélioration ou d'un « intrapreneuriat » (ce terme désigne l'entrepreneuriat à l'intérieur de l'organisation).

- il convient de revoir complètement la formation (permanente), de dresser la liste des compétences actuelles et requises, d'établir un plan de formation et d'inventorier l'offre de formations interne et externe[149] ;
- le Comité permanent R estime que la création d'une « branche renseignement »[150] peut résoudre (en partie) un certain nombre des problèmes constatés et engendrer un réel changement ;
- il convient de remédier aux nombreuses différences administratives et pécuniaires qui existent entre les différents groupes du personnel au sein du SGRS et entre ceux du SGRS et d'autres services du secteur du renseignement (VSSE et OCAM). Ces différences nuisent en effet à une bonne gestion du personnel ;
- il convient de porter une attention particulière au coaching, à l'accompagnement et au soutien du personnel du SGRS, et ce en tenant compte de leur situation spécifique ;
- dans le cadre de la fonction P&O (renforcée), le Comité permanent R recommande la création d'une cellule à laquelle le personnel civil peut s'adresser pour régler les problèmes spécifiques liés à son statut et à sa situation ;
- l'évaluation du personnel du SGRS s'appuie actuellement sur un cadre réglementaire qui dépasse ce service. La fonction P&O doit veiller à ce que les évaluations soient correctement effectuées et encadrées. Il convient également de décrire la manière dont se déroulera l'évaluation, par objectif et par produit à fournir ;
- le Comité permanent R recommande de traiter les inégalités de statut du personnel du SGRS. À cet égard, il est préférable de suivre une « logique fonctionnelle » plutôt qu'une « logique de groupe ». La fonction d'analyse requiert ici une attention prioritaire, puisque les différences sont les plus nombreuses et que les risques de discontinuité sont les plus importants ;
- le Comité recommande la création, au sein du SGRS, d'une fonction ayant pour mission principale « la gestion de la communication interne ».

IX.2.1.3. Recommandations en matière de flux d'informations et de TIC

- le Comité permanent R estime que le nouveau système *RFI (Request for Information)* améliorera (considérablement) le traitement et le suivi des demandes d'information. Le Comité recommande au SGRS d'examiner

[149] En ce qui concerne la formation certifiée pour le personnel civil statutaire du statut Camu, il convient de se concerter avec la DG HR et le SPF Personnel et Organisation afin de voir s'il est possible de créer des « fonctions » étroitement liées au travail d'analyse et de renseignement et/ou d'élaborer des formations certifiées adaptées.

[150] La question est bien entendu de savoir quels éléments une telle branche « renseignement » devrait réunir. L'audit n'avait pas pour objectif d'apporter une réponse définitive à cette question, qui requiert une étude distincte.

seulement après une période-test si une réorganisation supplémentaire s'impose toujours. Dans l'intervalle, le SGRS peut se concentrer sur l'aspect technique du système de gestion RFI, sans être d'emblée confronté à des questions organisationnelles ;
- le Comité recommande de poursuivre et d'accélérer autant que possible l'intégration de la collecte de données et des banques de données ;
- le SGRS doit prendre diverses initiatives pour être en mesure de gérer le volume important de données et de documentation. Il convient tout d'abord de déterminer quelles sont les informations nécessaires à la réalisation des objectifs et des produits à fournir. En outre, il convient de veiller à une bonne collaboration entre les services de collecte et les bureaux d'analyse. Enfin, il convient d'investir dans les moyens humains et les TIC absolument nécessaires ;
- de manière générale, le Comité recommande d'investir suffisamment de moyens dans les technologies de l'information et la communication (TIC), et ce plus rapidement que ce qui est prévu dans les plans d'investissement.

IX.2.1.4. Recommandations en matière de gestion des risques

- le Comité recommande de prendre des mesures pour limiter les risques en matière de discontinuité de l'exercice de fonctions et de perte de connaissances. Plus particulièrement, il convient de mener une gestion prévisionnelle du personnel, d'envisager la création d'une « branche renseignement » (où la perte de connaissances est moins importante et où les personnes peuvent être remplacées plus rapidement), et d'investir davantage (et de nouveau) dans les TIC ;
- il est recommandé que le SGRS s'intéresse de près à la gestion des connaissances. Des instructions claires doivent être élaborées de manière à identifier les connaissances existantes, évaluer leur pertinence, et prendre des mesures pour les stocker, les conserver et les diffuser. Le Comité recommande également la désignation, au sein de chaque division, d'un gestionnaire des connaissances en appui à la gestion des connaissances ;
- le Comité permanent R estime que le risque résultant d'une « définition pragmatique de priorités »[151] est limité, mais que la vigilance doit être de mise. Un recrutement adéquat et un système élaboré de descriptions de fonctions peuvent davantage circonscrire ce risque ;
- le Comité permanent R recommande que le SGRS œuvre au développement de la gestion des risques.

[151] À cet égard, l'attention se porte en priorité sur les aspects bien maîtrisés, tandis que pour des raisons pragmatiques, l'on s'attache moins aux aspects qui ne le sont pas autant.

IX.2.2. RECOMMANDATIONS RELATIVES À LA LOI MRD[152]

IX.2.2.1. Procédure d'extrême urgence pour les méthodes spécifiques et exceptionnelles

Pour toutes les méthodes spécifiques et exceptionnelles, il convient de prévoir une procédure d'extrême urgence qui autorise les services à réagir immédiatement à des menaces imminentes, tout en permettant un contrôle approfondi.

IX.2.2.2. Désignation de suppléants pour la Commission BIM

Il convient de procéder, dans les meilleurs délais, à la désignation de membres suppléants pour la Commission BIM. Ces nominations sont absolument nécessaires pour garantir la continuité du contrôle administratif des méthodes particulières de renseignement.

IX.2.2.3. Identification des utilisateurs des moyens de communication en tant que méthode spécifique

En matière d'identification des utilisateurs de certains moyens de communication, tels que les GSM, le Comité permanent R estime qu'il conviendrait de réfléchir à l'opportunité de maintenir cette mesure dans la catégorie des méthodes spécifiques. Alors que le caractère intrusif d'une telle méthode est ressenti comme faible à très faible, cette mesure est soumise aux mêmes exigences contraignantes que toutes les autres méthodes spécifiques, qui peuvent pourtant représenter une plus grande atteinte à la vie privée. Étant donné le recours massif à de telles méthodes, ces services se voient confrontés à une lourde charge administrative.

IX.2.3. RECOMMANDATIONS RELATIVES À LA SÉCURITÉ DE L'INFORMATION[153]

IX.2.3.1. Politique de sécurité en matière de cyberattaques

Toute une série d'initiatives ont été élaborées en matière de sécurité de l'information, et ce tant en Belgique que dans le cadre de l'Union européenne et

[152] Ces recommandations découlent des constatations faites dans le cadre du contrôle juridictionnel du Comité permanent R sur les méthodes particulières de renseignement (voir Chapitre III).

[153] Voir Chapitre II.2. La protection des systèmes de communication contre d'éventuelles interceptions et cyberattaques étrangères.

de l'OTAN.[154] Le Comité permanent R estime que pour notre pays, il est non seulement important de bien coordonner ces initiatives, mais aussi de les intégrer effectivement dans une politique de sécurité relative aux cyberattaques menées contre les intérêts nationaux. À cet égard, il est indispensable de créer une agence capable de coordonner les activités en matière de sécurité de l'information.

IX.2.3.2. Élargissement des compétences du SGRS et de la VSSE

En vertu de Loi MRD, le SGRS a pour nouvelle mission «*dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense nationale gère, de neutraliser l'attaque et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque*» (art. 11 § 1er, 2° L.R&S). Le Comité permanent R recommande toutefois de prévoir la même possibilité en cas d'attaques de systèmes informatiques d'autres services publics ou de l'infrastructure critique nationale. La VSSE pourrait être chargée de cette mission.

IX.2.3.3. Du personnel qualifié en suffisance

Le Comité permanent R a constaté un manque criant de personnel qualifié pour effectuer la mission relative à la sécurité de l'information au sein des services de renseignement. Il recommande de donner enfin à ces services les moyens leur permettant de recruter le personnel requis.

IX.2.3.4. Du matériel sécurisé en suffisance pour le traitement des informations sensibles et classifiées

Le Comité permanent R recommande la plus grande prudence dans le choix des équipements techniques sécurisés qui seront utilisés pour traiter les informations sensibles et classifiées. Le Comité reprend les recommandations du *Livre blanc de la Plateforme de concertation sur la sécurité de l'information*, et recommande que les équipements techniques soient évalués, certifiés et homologués – en termes de fiabilité et de sécurité – selon des critères et procédures qui répondent aux normes de l'Union européenne.

En outre, le Comité permanent R recommande que l'octroi de marchés à des fournisseurs de matériel de ce type soit assorti d'une obligation de disposer d'une habilitation de sécurité. L'enquête de sécurité préalable devrait porter une attention particulière aux liens éventuels de ces fournisseurs avec certains services de renseignement étrangers.

---

154 Voir, par exemple, le *Livre blanc pour une politique nationale de la sécurité de l'information*, la *politique de cyberdéfense de l'OTAN* et le *Programme européen de protection des infrastructures critiques*.

IX.2.3.5. Des moyens techniques en suffisance pour la certification et l'homologation

Le Comité permanent R considère également le manque de moyens techniques de certification et d'homologation comme un problème grave pour la sécurité de l'information. Aussi recommande-t-il de prévoir les moyens nécessaires pour enfin permettre la certification et l'homologation des systèmes utilisés en Belgique dans le traitement des informations classifiées, et ce sans devoir dépendre d'autorités et de services étrangers.

IX.2.4. RECOMMANDATIONS RELATIVES À L'OCAM ET À SES SERVICES D'APPUI[155]

IX.2.4.1. Un point de contact central établi

Certains services d'appui de l'OCAM sont dépourvus d'un point de contact central reconnu en tant que tel. Bien que les experts issus de ces services comblent en partie cette lacune, il n'en reste pas moins que la traçabilité des flux d'informations et l'organisation de la communication d'office de renseignements ne sont absolument pas garanties. Les Comités permanents P et R estiment que des efforts non négligeables doivent être consentis à court terme en la matière.

IX.2.4.2. Une vision claire des flux d'informations

Le point de contact central au sein de chaque service d'appui de l'OCAM devrait disposer d'une vision globale des renseignements et/ou des évaluations échangés. En outre, la traçabilité des renseignements devrait être garantie dans chaque service.

IX.2.4.3. Accusés de réception et degrés d'urgence

L'enquête de contrôle a démontré que les obligations énoncées à l'article 11 §§ 2 et 3 AR.OCAM concernant l'envoi d'accusés de réception et le respect des degrés d'urgence n'ont pas toujours été respectées. Les Comités ont estimé que si ces obligations ne représentent aucune plus-value pour les services, la réglementation doit être adaptée en ce sens. Sinon, l'Arrêté royal doit être affiné de manière à intégrer la possibilité réglementaire de ne pas répondre en l'absence

[155] Les six premières recommandations découlent des constatations faites dans le cadre de l'enquête de contrôle « Les flux d'informations entre l'OCAM et ses services d'appui » (voir Chapitre II.4). La septième recommandation résulte de l'enquête conjointe relative à « Une visite de travail prévue à l'étranger par l'OCAM » (voir Chapitre II.5). La dernière recommandation émane des deux enquêtes.

d'information. Les Comités ont par ailleurs estimé qu'il fallait distinguer clairement les destinataires des messages envoyés « pour info » des destinataires dont une (ré)action est attendue.

IX.2.4.4. Confusion concernant les différentes procédures d'embargo

Il convient de dissiper toute confusion entre les procédures d'embargo visées aux articles 11 et 12 L.OCAM et des procédures similaires découlant, par exemple, de la Loi sur la Fonction de police.

IX.2.4.5. « Opérationnalisation » de la plateforme d'information et de communication sécurisée

Les Comités permanents P et R recommandent de développer une vision d'avenir pour la plateforme d'information et de communication sécurisée et cryptée, et de lever à court terme toute une série d'obstacles pour enfin rendre opérationnelles les connexions prévues.

IX.2.4.6. Clarification de la notion de « renseignements pertinents »

Certains services d'appui éprouvent des difficultés à interpréter concrètement la notion de « renseignements pertinents ». Il convient de clarifier ce concept, éventuellement au sein de groupes de travail communs.

IX.2.4.7. Confusion concernant l'identité de l'OCAM

Il est recommandé que l'OCAM veille toujours à ce que son identité unique ne prête pas à confusion. Contrairement au SGRS et à la VSSE, l'OCAM n'est pas un service de renseignement. Il est dès lors essentiel qu'il y prête une attention active et systématique dans sa communication et son fonctionnement, et ce tant en Belgique qu'à l'étranger. Dans ce cadre, il est recommandé que l'OCAM fasse preuve d'une extrême prudence lorsqu'il souhaite entreprendre des missions à l'étranger et qu'il délimite rigoureusement ses voyages d'études.

IX.2.4.8. La « mission à l'étranger » de l'OCAM

En ce qui concerne la relation entre l'OCAM et les deux services de renseignement, le SGRS remet en question le mandat de l'OCAM à l'étranger, tandis que la VSSE oppose des objections à des contacts entre l'OCAM et des services de renseignement étrangers. Les services concernés devraient clarifier davantage la question. Il est toutefois plus important que le Comité ministériel du renseignement et de la sécurité édicte enfin une directive en la matière, et ce en exécution de l'article 8, 3° L.OCAM.

IX.2.5. RECOMMANDATIONS RELATIVES À LA LUTTE CONTRE LA PROLIFÉRATION ET LA PROTECTION DU PSE[156]

Le Comité permanent R recommande à la VSSE de passer d'une approche réactive et *ad hoc* à une approche plus proactive dans la lutte contre la prolifération, tout en veillant à effectuer davantage d'analyses stratégiques tenant compte des aspects « intérêts économiques » et « ingérence » éventuelle de services (de renseignement) étrangers. De telles analyses requièrent une bonne position d'information, qui ne peut être atteinte que par l'intensification des contacts avec les administrations, les entreprises, les laboratoires et les centres de recherche belges, ainsi que par la conclusion d'accords de coopération avec les instances concernées par la lutte contre la prolifération.[157] Dans cette même optique, le Comité recommande aux analystes et agents opérationnels actifs dans le domaine de la protection du PSE, d'une part, et de la prolifération, d'autre part, de se réunir pour élaborer une méthodologie commune. Cette mesure doit également contribuer à ce que la VSSE puisse adopter un point de vue univoque à l'égard des instances politiques compétentes.

Enfin, le Comité réitère la recommandation du Sénat qui vise à inscrire dans la loi organique des services de renseignement et de sécurité une compétence spécifique en matière de contrôle de la légalité des activités des services de renseignement étrangers sur notre territoire.[158]

IX.2.6. ÉCHANGE DIRECT D'INFORMATIONS ENTRE LES SERVICES DE POLICE ET DE RENSEIGNEMENT[159]

Le Comité permanent R recommande la mise en place d'une concertation structurée entre les services de renseignement, d'une part, et les services de police (fédérale et locale), d'autre part, afin d'échanger des données par le biais de procédures bien définies. L'absence d'un accord de coopération entre ces services constitue sans aucun doute une défaillance dans notre système de sécurité. Le Comité permanent R a déjà attiré l'attention sur ce point à plusieurs reprises par le passé.[160]

---

156 Voir Chapitre II.2. La protection des systèmes de communication contre d'éventuelles interceptions et cyberattaques étrangères.

157 Par exemple, avec le SPF Affaires étrangères, l'Administration des douanes et accises, la CANPAN et les autorités régionales compétentes en la matière.

158 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 128.

159 Voir Chapitre II.3. La position d'information et les actions des services de renseignement concernant Lors Doukaev.

160 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 131 ; *Rapport d'activités 2007*, 75 et *Rapport d'activités 2009*, 86-87.

Avant d'envisager la création d'une banque de données sur le terrorisme et le radicalisme, le Comité permanent R recommande d'élaborer rapidement un système d'échange d'informations entre les services de police et de renseignement.

IX.2.7. COORDINATION DE LA REPRÉSENTATION DES SERVICES DE SÉCURITÉ DANS DES FORUMS INTERNATIONAUX[161]

Les Comités permanents P et R demandent d'examiner la faisabilité d'une structure spécifique susceptible de se charger de la coordination et/ou la représentation des différents services belges qui participent à des forums ou réunions au niveau international dans le cadre de la lutte contre le terrorisme et l'extrémisme. Plus particulièrement, le Comité ministériel du renseignement et de la sécurité peut prendre une initiative en l'espèce, et le Collège du renseignement et de la sécurité peut à son tour être désigné pour veiller à son exécution.

Une telle structure n'est naturellement pas destinée aux forums qui s'adressent spécifiquement à un ou plusieurs services précis.

IX.2.8. UN CODE DE DÉONTOLOGIE POUR LES AGENTS DE LA VSSE[162]

Le Comité permanent R recommande qu'en exécution de l'article 17 de l'A.R. du 13 décembre 2006 portant le statut des agents des services extérieurs de la VSSE, cette dernière élabore un(e) (proposition de) code de déontologie et le soumette à l'approbation du ministre de la Justice.

Ce code doit clairement décrire en quoi consiste le devoir de neutralité et de discrétion des agents de la VSSE. En outre, il convient de veiller au respect strict de ce code de déontologie par une application rapide et systématique de la procédure disciplinaire en cas de non-respect. Cette procédure disciplinaire ne peut pas être confondue avec une enquête de sécurité, qui a sa finalité propre.

---

161 Voir Chapitre II.8. La représentation belge à des réunions internationales en matière de terrorisme.

162 Voir Chapitre II.7. Plainte d'un membre de la VSSE et de son épouse.

IX.3. RECOMMANDATIONS RELATIVES À L'EFFICACITÉ DU CONTRÔLE

IX.3.1. DÉCLARATION SPONTANÉE DES PROBLÈMES AUX ORGANES DE CONTRÔLE

L'OCAM et les services d'appui doivent informer spontanément les Comités permanents P et R lorsqu'ils estiment observer, dans leurs relations mutuelles, des dysfonctionnements structurels en matière de légalité, d'efficacité et de coordination.

IX.3.2. CONTRÔLE DU JOURNAL DE BORD RELATIF AUX INTERCEPTIONS ÉTRANGÈRES[163]

Le Comité permanent R recommande que les pages du journal de bord relatif aux interceptions soient paraphées d'avance par le dirigeant de service ou par un officier qu'il désigne.

[163] Voir Chapitre IV. Le contrôle de l'interception de communications émises à l'étranger.

ANNEXES

ANNEXE A.
APERÇU DES PRINCIPALES RÉGLEMENTATIONS RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2011 AU 31 DÉCEMBRE 2011)

Loi 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité- Traduction allemande, *M.B.* 10 mars 2011

Loi 9 février 2011 modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace, *M.B.* 29 mars 2011

Loi 11 avril 2011 ouvrant des crédits provisoires pour les mois d'avril, mai et juin 2011, *M.B.* 26 avril 2011

Loi 30 mai 2011 contenant le budget général des dépenses pour l'année budgétaire 2011, *M.B.* 16 juin 2011

Loi 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, *M.B.* 15 juillet 2011

A.R. 1er juin 2011 modifiant l'arrêté royal du 13 décembre 2006 portant le statut des agents des services extérieurs de la Sûreté de l'État, *M.B.* 22 juin 2011

A.R. 17 octobre 2011 relatif aux attestations de sécurité pour le secteur nucléaire et réglant l'accès aux zones de sécurité, aux matières nucléaires ou aux documents nucléaires dans certaines circonstances particulières – Erratum, *M.B.* 25 novembre 2011

A.R. 17 octobre 2011 portant sur la catégorisation et la protection des documents nucléaires – Erratum, *M.B.* 25 novembre 2011

A.R. 17 octobre 2011 relatif à la catégorisation et à la définition de zones de sécurité au sein des installations nucléaires et des entreprises de transport nucléaire – Erratum, *M.B.* 25 novembre 2011

A.R. 17 octobre 2011 relatif à la protection physique des matières nucléaires et des installations nucléaires – Erratum, *M.B.* 25 novembre 2011

A.R. 2 décembre 2011 concernant les infrastructures critiques dans le sous-secteur du transport aérien, *M.B.* 27 décembre 2011

A.R. 21 décembre 2011 portant désignation des membres du Comité ministériel du renseignement et de la sécurité, *M.B.* 28 décembre 2011

A.M. 4 avril 2011 modifiant l'arrêté ministériel du 4 mai 2007 relatif au stage et à la formation des agents des services extérieurs de la Sûreté de l'Etat, *M.B.* 15 avril 2011

A.M. 20 octobre 2011 relatif à la procédure de vérification de sécurité pour tous les membres du personnel de la SA de droit public A.S.T.R.I.D. et de ses sous-traitants, *M.B.* 28 novembre 2011

Sélection comparative néerlandophone de juristes (renseignement) (m/f) (niveau A) pour le Ministère de la Défense (ANG11007), *M.B.* 2 septembre 2011

Emploi vacant de directeur adjoint de l'Organe de coordination pour l'analyse de la menace (Loi du 10 juillet 2006, *M.B.* du 20 juillet 2006) – Appel aux candidats, *M.B.* 13 septembre 2011

Personnel – Désignation pour assurer la fonction d'administrateur général de la Sûreté de l'État, *M.B.* 26 octobre 2011

Ordre judiciaire – Désignation en qualité de directeur de l'Organe de coordination pour l'analyse de la menace, *M.B.* 2 décembre 2011

Extrait de l'arrêt n° 145/2011 du 22 septembre 2011 : *En cause* : les recours en annulation totale ou partielle de la loi du 4 février 2010 relative aux méthodes de recueil de données par les services de renseignement et de sécurité, introduits par l'"Orde van Vlaamse balies' et Jo Stevens et par l'ASBL 'Liga voor Mensenrechten', *M.B.* 12 décembre 2011

ANNEXE B.
APERÇU DES PRINCIPALES PROPOSITIONS DE LOIS, DES PROJETS DE LOIS, DES RÉSOLUTIONS ET DES DÉBATS PARLEMENTAIRES RELATIFS AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2011 AU 31 DÉCEMBRE 2011)

Sénat

Décisions de la Commission parlementaire de concertation, *Doc. Parl.*, Sénat, 2010-2011, n° 5-82/6

Proposition de loi modifiant le Code de la nationalité belge, *Doc. Parl.*, Sénat, 2010-2011, n° 5-736/1

Proposition de budget pour l'année 2011 de la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité (Commission BIM – C-BIM), *Doc. Parl.,* Sénat, 2010-2011, nos 5-792/1 à 5-792/3

Rapport sur le Contrôle des activités d'Europol par le Parlement européen en association avec les parlements nationaux, *Doc. Parl.*, Sénat, 2010-2011, n° 5-774/1

Conférence des Présidents des parlements de l'Union européenne (Bruxelles, 3-5 avril 2011), *Doc. Parl.*, Sénat, 2010-2011, n° 5-1033/1

Proposition de budget pour la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité (Commission BIM – C-BIM), *Doc. Parl.*, Sénat, 2011-12, n° 5-1386/1

Envoi à la Commission chargée du suivi du Comité permanent de contrôle des services de renseignement et de sécurité du rapport semestriel sur l'application des méthodes spécifiques et exceptionnelles par les services de renseignement et de sécurité et le contrôle effectué sur celles-ci par le Comité permanent R pour la période du 1er septembre 2010 au 31 décembre 2010, *Ann. parl.,* Sénat, 2010-2011, 27 janvier 2011, n° 5-11, p. 58

Discussion du Rapport d'activités 2009 du Comité permanent de contrôle des services de renseignements et de sécurité, (Doc. 5-545), *Ann. parl.,* Sénat, 2010-2011, 24 février 2011, n° 5-13, p. 38

Discussion sur la proposition de budget pour l'année 2011 de la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité (Commission BIM – C-BIM) (Doc. 5-792), *Ann. parl.,* Sénat, 2010-2011, 31 mars 2011, n° 5-19, p. 35

Envoi à la Commission chargée du suivi du Comité permanent de contrôle des services de renseignement et de sécurité du rapport d'activités 2010 du Comité permanent R, *Ann. parl.,* Sénat, 2011-2012, 11 octobre 2011, n° 5-33, p. 26

Nomination d'un membre de la commission chargée du suivi du Comité permanent de contrôle des services de renseignements et de sécurité (Comité permanent R), *Ann. parl.,* Sénat, 2011-2012, 10 novembre 2011, n° 5-34, p. 38

Chambre des Représentants

Projet de loi modifiant la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire et modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *Doc. Parl.,* Chambre, 2010-2011, nos 53-1005/001 à 53-1005/005, *C.R.I.,* Chambre, 2010-2011, 17 février 2011, n° 53-19, p. 80

Proposition de loi modifiant le Code de la nationalité belge afin de rendre l'acquisition de la nationalité belge neutre du point de vue de l'immigration, *Doc. Parl.*, Chambre, 2010-2011, nos 53-476/007 et 53-476/010

Décisions de la Commission parlementaire de concertation, *Doc. Parl.*, Chambre, 2010-2011, n° 53-82/006

Projet de loi modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace, *Doc. Parl.*, Chambre, 2010-2011, n° 53-802/002

Proposition de loi modifiant le Code pénal, en vue de sanctionner la déstabilisation mentale des personnes et l'abus de la situation de faiblesse des personnes, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1217/001

Contrôle des activités d'Europol par le Parlement européen en association avec les parlements nationaux, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1255/001

Projet de loi ouvrant des crédits provisoires pour les mois d'avril, mai et juin 2011, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1280/001

Proposition de résolution concernant la lutte contre les cyberattaques et les cyberguerres, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1289/001

Proposition de loi modifiant la législation en matière de reconnaissance du culte islamique, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1327/001

Projet de loi concernant les infrastructures critiques, les autres points d'intérêt fédéral et les points d'intérêt local, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1357/001

Projet du budget général des dépenses pour l'année budgétaire 2011, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1348/001

Conférence des Présidents des parlements de l'Union européenne Bruxelles, 3-5 avril 2011, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1497/001

Projet de loi relatif à la protection des témoins menacés, *Doc. Parl.*, Chambre, 2010-2011, n^{os} 53-1472/001, 53-1472/003 et 53-1472/004

Proposition de résolution relative à la lutte contre les chaînes satellitaires, stations de radio et sites Internet islamiques qui diffusent une propagande haineuse anti-occidentale sur le territoire belge et européen, *Doc. Parl.*, Chambre, 2010-2011, n° 53-1518/001

Proposition de loi insérant les articles 442*quater* et 442*quinquies* dans le Code pénal, en vue de sanctionner la déstabilisation mentale des personnes et les abus de la situation de faiblesse des personnes ; Proposition de loi étendant la protection pénale des personnes vulnérables contre la maltraitance et la malmenance ; Proposition modifiant le Code pénal et le Code d'instruction criminelle en ce qui concerne la protection des personnes vulnérables ; Proposition de loi modifiant le Code pénal, en vue de sanctionner la déstabilisation mentale des personnes et l'abus de la situation de faiblesse des personnes, *Doc. Parl.*, Chambre, 2010-2011, n^{os} 53-0080/007 et 53-0080/008

Projet de loi de finances pour l'année budgétaire 2012, *Doc. Parl.*, Chambre, 2011-2012, n° 53-1933/001

Projet de loi portant des dispositions diverses, *Doc. Parl.*, Chambre 2011-2012, n° 53-1952/001

Projet de loi contenant le budget des voies et moyens de l'année budgétaire 2012, *Doc. Parl.*, Chambre, 2011-2012, n° 53-1943/001

Projet du budget général de dépenses pour l'année budgétaire 2012 – Première partie, *Doc. Parl.*, Chambre, 2011-2012, n° 53-1944/001

Projet de loi modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (802/1), *Ann. parl.,* Chambre, 2010-2011, 27 janvier 2011, n° 53-15, p. 53

La situation en Libye : exposés du premier ministre, du vice-premier ministre et ministre des Affaires étrangères et des Réformes institutionnelles et du ministre de la Défense, et échange de vues, *C.R.I.,* Chambre, 2010-2011, 18 mars 2011, n° 162, p. 1

Discussion sur la proposition de résolution concernant la situation en Libye (1308/1-2), *Ann. parl.,* Chambre, 2010-2011, 21 mars 2011, n° 53-24, p. 1

Discussion des budgets et comptes de la Chambre et des institutions financées par une dotation – comptes de l'année budgétaire 2009 – ajustement du budget 2010 – propositions budgétaires pour l'année 2011 (1440/1) ; Chambre des Représentants : budget modifié de l'année budgétaire 2011 (1452/1), *Ann. parl.,* Chambre, 2010-2011, 19 mai 2011, n° 53-35, p. 37

Proposition de loi modifiant le Code pénal, en vue de sanctionner la déstabilisation mentale des personnes et l'abus de la situation de faiblesse des personnes (1217/1-2), *Ann. parl.,* Chambre, 2010-2011, 15 juin 2011, n° 53-39, p. 1

Proposition de loi modifiant la législation en ce qui concerne la suppression de la Sûreté de l'État (894/1-2), *Ann. parl.,* Chambre, 2010-2011, 23 juin 2011, n° 53-41, p. 82

ANNEXE C.
APERÇU DES INTERPELLATIONS, DES DEMANDES D'EXPLICATIONS ET DES QUESTIONS ORALES ET ÉCRITES RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2011 AU 31 DÉCEMBRE 2011)

Sénat

Demande d'explications de Z. Khattabi au ministre de la Justice sur 'la mise en isolement et les conditions de détention de M. Nizar Trabelsi' (*C.R.I.,* Sénat, 2010-2011, 19 janvier 2011, n° 5-25, p. 11, Q. n° 5-296)

Question écrite d'A. Van dermeersch au ministre de la Défense sur la 'cybercriminalité – situation en Belgique – cyberdéfense' (Sénat, 2010-2011, 27 janvier 2011, Q. n° 5-894)

Question écrite d'A. Van dermeersch à la ministre de l'Intérieur sur la 'cybercriminalité – situation en Belgique – cyberdéfense' (Sénat, 2010-2011, 27 janvier 2011, Q. n° 5-895)

Question écrite de B. Anciaux au ministre pour l'Entreprise et la Simplification sur 'l'espionnage économique et industriel – mesures – concertation européenne' (Sénat, 2010-2011, 27 janvier 2011, Q. n° 5-966)

Question écrite de B. Anciaux au ministre de la Justice sur le 'terrorisme – mesures récentes – collaboration internationale' (Sénat, 2010-2011, 27 janvier 2011, Q. n° 5-976)

Question écrite de B. Anciaux à la ministre de l'Intérieur sur la 'police – achat de dispositifs d'écoute – fuites vers l'étranger' (Sénat, 2010-2011, 1er février 2011, Q. n° 5-1114)

Demande d'explications de B. Anciaux à la ministre de l'Intérieur sur 'la sécurisation de nos aéroports contre les attaques terroristes' (*Ann. parl.,* Sénat, 2010-2011, 8 février 2011, 5-32, p. 8, Q. n° 5-370)

Question écrite de B. Anciaux au ministre de la Justice sur le 'terrorisme – raids policiers – évaluation – résultats' (Sénat, 2010-2011, 8 février 2011, Q. n° 5-1220)

Question écrite de B. Anciaux au ministre de la Justice sur la 'Sûreté de l'État – fonctionnement – contrôle parlementaire' (Sénat, 2010-2011, 8 février 2011, Q. n° 5-1226)

Question écrite de B. Anciaux à la ministre de l'Intérieur sur la 'Sûreté de l'État – fonctionnement – contrôle parlementaire' (Sénat, 2010-2011, 8 février 2011, Q. n° 5-1227)

Demande d'explications de B. Anciaux au secrétaire d'État à la Mobilité sur 'l'entreprise de sécurité opérant à l'aéroport de Zaventem et dans d'autres endroits stratégiques de notre pays' (*Ann. parl.,* Sénat, 2010-2011, 9 février 2011, n° 5-35, p. 4, Q. n° 5-372)

Question écrite de B. Anciaux à la ministre de l'Intérieur sur 'l'aéroport de Zaventem – sociétés de sécurité – adjudication' (Sénat, 2010-2011, 11 février 2011, Q. n° 5-1329)

Question écrite de B. Anciaux au ministre de la Défense sur le 'Service général du renseignement et de la sécurité des forces armées – fonctionnement – contrôle parlementaire' (Sénat, 2010-2011, 15 février 2011, Q. n° 5-1350)

Question écrite d'A. De Croo à la ministre de l'Intérieur sur les 'écoutes téléphoniques – statistiques – coût – transparence' (Sénat, 2010-2011, 18 février 2011, Q. n° 5-1379)

Question écrite d'A. De Croo à la ministre de l'Intérieur sur les 'services de renseignement et parquets – écoutes téléphoniques – fréquence – Skype' (Sénat, 2010-2011, 18 février 2011, Q. n° 5-1381)

Question écrite de F. Dewinter à la ministre de l'Intérieur sur les 'groupements extrémistes et subversifs – critères – liste' (Sénat, 2010-2011, 18 février 2011, Q. n° 5-1386)

Demande d'explications de F. Boogaerts au ministre de la Justice sur 'les menaces terroristes' (*Ann. parl.,* Sénat 2010-2011, 23 février 2011, n° 5-43, p. 9, Q. n° 5-295)

Demande d'explications de K. Vanlouwe au ministre de la Justice sur 'l'inertie de la Sûreté de l'État concernant l'affaire d'espionnage dans le bâtiment européen du Juste Lipse' (*Ann. parl.,* Sénat, 2010-2011, 23 février 2011, n° 5-43, p. 12, Q. n° 5-305)

Demande d'explications de F. Bellot au ministre de la Justice sur 'le recours par la justice aux traducteurs et aux interprètes jurés dans le cadre d'enquêtes pénales' (*Ann. parl.,* Sénat, 2010-2011, 2 mars 2011, n° 5-46, p. 5, Q. n° 5-441)

Demande d'explications de B. Anciaux au ministre de la Justice sur 'l'affaire Swift et les prétendues tentatives de la soustraire à la justice' (*Ann. parl.,* Sénat, 2010-2011, 2 mars 2011, n° 5-46, p. 14, Q. n° 5-475)

Question écrite de B. Anciaux au ministre de la Justice sur 'la lutte contre les organisations d'extrême droite' (Sénat, 2010-2011, 10 mars 2011, Q. n° 5-1702)

Demande d'explications de B. Anciaux au ministre de la Justice sur 'l'avis du Parquet et de la Sûreté de l'État dans le cadre d'un dossier concernant une société de sécurité et de gardiennage' (*Ann. parl.,* Sénat, 2010-2011, 30 mars 2011, n° 5-57, p. 14, Q. n° 5-592)

Demande d'explications de B. Laeremans au ministre de la Justice sur 'le dossier concernant les six assassinats politiques attribués à M. Belliraj' (*Ann. parl.,* Sénat, 2010-2011, 30 mars 2011, n° 5-57, p. 18, Q. n° 5-602)

Question écrite de D. Claes au ministre de la Justice sur les 'informateurs – indemnisation – nombres' (Sénat, 2010-2011, 30 mars 2011, Q. n° 5-1920)

Question écrite de B. Anciaux au ministre de la Justice sur les 'dispositifs d'écoute belges – fuites éventuelles vers un service de renseignement d'une puissance étrangère – mesures' (Sénat, 2010-2011, 8 avril 2011, Q. n° 5-2058)

Question écrite d'Y. Buysse au ministre de la Justice sur les 'Comités permanents P et R – secret de l'instruction – overruling' (Sénat, 2010-2011, 5 mai 2011, Q. n° 5-2232)

Demande d'explications de B. Laeremans au ministre de la Justice sur 'le cadre linguistique de la Sûreté de l'État' (*Ann. parl.,* Sénat, 2010-2011, 11 mai 2011, n° 5-67, p. 23, Q. n° 5-765)

Question écrite d'A. De Croo au vice-premier ministre et ministre des Finances sur la 'Cellule de traitement des informations financières (CTIF) – compétence de contrôle – terrorisme et extrémisme' (Sénat, 2010-2011, 26 mai 2011, Q. n° 5-2390)

Question écrite d'A. De Croo au ministre de la Justice sur la 'Cellule de traitement des informations financières (CTIF) – compétence de contrôle – terrorisme et extrémisme'' (Sénat, 2010-2011, 26 mai 2011, Q. n° 5-2391)

Question écrite de B. Anciaux au vice-premier ministre et ministre des Finances sur le 'terrorisme – financement au départ de la Belgique – utilisation d'argent provenant d'allocations sociales' (Sénat, 2010-2011, 26 mai 2011, Q. n° 5-2412)

Question écrite de B. Anciaux au ministre de la Justice sur le 'terrorisme – financement au départ de la Belgique – utilisation d'argent provenant d'allocations sociales' (Sénat, 2010-2011, 26 mai 2011, Q. n° 5-2413)

Question orale de B. Anciaux au ministre de la Défense sur 'le malaise des services de renseignements de l'armée' (*Ann. parl.,* Sénat, 2010-2011, 16 juin 2011, n° 5-26, p. 14, Q. n° 5-210)

Question écrite de R. Miller au ministre des Affaires étrangères sur 'la présence éventuelle de mercenaires belges en Libye' (Sénat, 2010-2011, 1er juillet 2011, Q. n° 5-2664)

Question écrite de B. Tommelein au ministre de la Justice sur la 'Sûreté de l'État – conférences de prêcheurs de haine à l'étranger – présence de concitoyens – chiffres et répression' (Sénat, 2010-2011, 16 septembre 2011, Q. n° 5-3076)

Question orale de D. Pieters au ministre de la Justice sur 'l'installation de la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données' (*Ann. parl.,* Sénat, 2011-2012, 1er décembre 2011, n° 5-37, p. 14, Q. n° 5-317)

Question écrite de B. Anciaux au premier ministre sur le 'Comité ministériel du renseignement et de la sécurité – règles de confidentialité – sujets traités – contrôle parlementaire' (Sénat, 2011-12, 23 décembre 2011, Q. n° 5-4617)

Question écrite de K. Vanlouwe au premier ministre sur les 'attaques et délinquance informatiques – protection informatique – politique fédérale – observations du Comité R' (Sénat, 2011-12, 23 décembre 2011, Q. n° 5-4291)

Question écrite de B. Anciaux au ministre de la Justice sur 'l'espionnage – services de renseignement – évolution – prévention' (Sénat, 2011-12, 28 décembre 2011, Q. n° 5-4703)

Question écrite de B. Anciaux au ministre de la Défense sur 'l'espionnage – services de renseignement – évolution – prévention' (Sénat, 2011-12, 28 décembre 2011, Q. n° 5-4934)

Question écrite de K. Vanlouwe au ministre de la Défense sur les 'attaques et délinquance informatiques – protection informatique – organisation du Traité de l'Atlantique Nord (OTAN) – Computer Emergency Response Team (CERT) – cas particulier de la Défense' (Sénat, 2011-12, 28 décembre 2011, Q. n° 5-4320)

Question écrite de K. Vanlouwe à la ministre des Classes moyennes sur les 'attaques et délinquance informatiques – protection informatique – Computer Emergency Response Team (CERT) – situation spécifique du Service public fédéral de Programmation Politique scientifique' (Sénat, 2011-12, 28 décembre 2011, Q. n° 5-4321)

Chambre des Représentants

Question de T. Veys au ministre de la Justice sur 'l'association islamique radicale 'De Middenweg' – contacts avec des intégristes musulmans à l'étranger' (*Q.R.,* Chambre, 2010-2011, 14 janvier 2011, n° 13, p. 33, Q. n° 44)

Question de T. Veys au ministre de la Justice sur 'l'organisation 'European Council for Fatwa and Research'' (*Q.R.,* Chambre, 2010-2011, 14 janvier 2011, n° 13, p. 35, Q. n° 45)

Question de T. Veys au ministre de la Justice sur 'le mouvement étudiant islamique radical 'The Union of Arab Students in Europe'' (*Q.R.,* Chambre, 2010-2011, 14 janvier 2011, n° 13, p. 41, Q. n° 48)

Question de D. Ducarme au ministre de la Justice sur 'l'audit sur la Sûreté de l'État' (*Q.R.,* Chambre, 2010-2011, 14 janvier 2011, n° 13, p. 47, Q. n° 177)

Questions jointes de S. De Wit et S. Becq au ministre de la Justice sur 'l'incident survenu entre un juge d'instruction et le personnel de la prison de Saint-Gilles' (*C.R.I.,* Chambre, 2010-2011, 18 janvier 2011, COM 94, p. 28, Q. n^{os} 2108 et 2129)

Question de K. Calvo à la ministre de l'Intérieur sur 'la délivrance de certificats de sécurité par l'AFCN' (*C.R.I.,* Chambre, 2010-2011, 26 janvier 2011, COM 107, p. 19, Q. n° 2315)

Question de C. Brotcorne à la ministre de l'Intérieur sur 'la sécurité de nos aéroports' (*C.R.I.,* Chambre, 2010-2011, 27 janvier 2011, PLEN 15, p. 32, Q. n° 017)

Question de R. Terwingen au ministre pour l'Entreprise et la Simplification sur 'la rétention des données' (*C.R.I.,* Chambre, 2010-2011, 1er février 2011, COM 113, p. 1, Q. n° 1298)

Question de P. Dedecker à la ministre des PME sur 'l'action juridique des Archives générales de l'État contre le décret flamand sur les archives' (*C.R.I.,* Chambre, 2010-2011, 1er février 2011, COM 111, p. 3, Q. n° 2096)

Questions jointes de S. Van Hecke à la ministre de l'Intérieur sur 'la sécurité des systèmes d'écoute de la police fédérale' (*C.R.I.,* Chambre, 2010-2011, 8 février 2011, COM 121, p. 5, Q. n^{os} 2278 et 2279)

Questions jointes de D. Bacquelaine et B. Schoofs au ministre de la Justice sur 'l'installation d'une école musulmane radicale à Borgerhout' (*C.R.I.,* Chambre, 2010-2011, 22 février 2011, COM 139, p. 25, Q. n^{os} 2547 et 2587)

Question de J. Boulet au ministre de la Justice sur 'les dispositifs d'écoute au sein du bâtiment Juste Lipse' (*C.R.I.,* Chambre, 2010-2011, 22 février 2011, COM 139, p. 31, Q. n° 2578)

Questions jointes de T. Francken, K. Temmerman, R. Madrane et J. Galant au secrétaire d'État au Budget sur 'les émeutes au centre 127*bis* à Steenokkerzeel et en particulier dans l'enceinte même de ce centre' (*C.R.I.,* Chambre, 2010-2011, 22 février 2011, COM 140, p. 27, Q. n^{os} 2900, 2928, 2935 et 2946)

Question de B. Schoofs au ministre de la Justice sur 'les nouveaux projets de l'Exécutif des Musulmans' (*C.R.I.,* Chambre, 2010-2011, 3 mars 2011, PLEN 21, p. 31, Q. n° 132)

Question d'A. Colen au ministre des Affaires étrangères sur 'l'attentat terroriste à Moscou' (*C.R.I.,* Chambre, 2010-2011, 16 mars 2011, COM 158, p. 19, Q. n° 2338)

Questions jointes de D. Thiéry et S. Bracke au ministre de la Défense sur 'la protection des systèmes d'information de l'État face aux récentes attaques subies par la France' (*C.R.I.,* Chambre, 2010-2011, 16 mars 2011, COM 161, p. 34, Q. n^{os} 3280 et 3345)

Question de M. Gerkens à la ministre des PME sur le 'financement de l'étude sur l'assassinat de Julien Lahaut' (*Q.R.,* Chambre, 2010-2011, 22 mars 2011, n° 23, p. 171, Q. n° 107)

Question d'E. Thiébaut à la ministre de l'Intérieur sur 'l'arrestation d'islamistes soupçonnés de terrorisme à Anvers et Bruxelles' (*Q.R.,* Chambre, 2010-2011, 23 mars 2011, n° 23, p. 239, Q. n° 235)

Question de P. Luykx à la ministre de l'Intérieur sur 'la menace terroriste potentielle' (*C.R.I.,* Chambre, 2010-2011, 24 mars 2011, PLEN 25, p. 29, Q. n° 181)

Question d'E. Thiébaut au ministre de la Justice sur 'l'arrestation d'islamistes soupçonnés de terrorisme à Anvers et Bruxelles' (*Q.R.,* Chambre, 2010-2011, 29 mars 2011, n° 24, p. 66, Q. n° 385)

Question de T. Veys à la ministre de l'Intérieur sur 'l'association environnementale GroenFront!' (*Q.R.,* Chambre, 2010-2011, 6 avril 2011, n° 25, p. 35, Q. n° 58)

Question de L. Dierick à la ministre de l'Intérieur sur 'le dépistage des jeunes en situation de radicalisation' (*Q.R.,* Chambre, 2010-2011, 6 avril 2011, n° 25, p. 55, Q. n° 244)

Question de G. Gilkinet à la ministre de l'Intérieur sur les 'départements – études – financement' (*Q.R.,* Chambre, 2010-2011, 14 avril 2011, n° 26, p. 73, Q. n° 250)

Question de R. Madrane au ministre de la Justice sur 'la signature à Maastricht d'une déclaration visant à harmoniser plus étroitement les initiatives et efforts en matière de lutte contre la cybercriminalité avec les ministres luxembourgeois et néerlandais' (*C.R.I.,* Chambre, 2010-2011, 27 avril 2011, COM 205, p. 4, Q. n° 3853)

Question de J. Van Esbroeck à la ministre de l'Intérieur sur 'la visite en Belgique de Pakistanais liés à des groupes terroristes' (*C.R.I.,* Chambre, 2010-2011, 27 avril 2011, COM 204, p. 6, Q. n° 3930)

Question de S. Smeyers au ministre de la Justice sur 'l'arrestation de deux Belges d'origine rwandaise' (*C.R.I.,* Chambre, 2010-2011, 27 avril 2011, COM 205, p. 39, Q. n° 3958)

Questions jointes d'E. Thiébaut, I. De Meulemeester et J. Van Esbroeck à la ministre de l'Intérieur sur 'l'éventuelle menace terroriste pour notre pays suite à la mort du dirigeant d'Al-Qaïda, Oussama Ben Laden' (*C.R.I.,* Chambre, 2010-2011, 4 mai 2011, COM 217, p. 28, Q. n^{os} 4394, 4402 et 4411)

Question d'O. Maingain au ministre de la Justice sur 'la protection des systèmes d'information de l'État face aux récentes attaques subies par la Belgique et la France' (*C.R.I.,* Chambre, 2010-2011, 4 mai 2011, COM 219, p. 17, Q. n° 3891)

Question de S. Lahaye-Battheu au ministre de la Justice sur 'l'analyse des risques d'évasion lors du transfert de détenus de la prison au palais de justice' (*C.R.I.,* Chambre, 2010-2011, 4 mai 2011, COM 219, p. 21, Q. n° 4002)

Questions jointes d'I. De Meulemeester, P. Dewael, W. De Vriendt et D. Van der Maelen au ministre des Affaires étrangères sur 'la mort d'Oussama Ben Laden' (*C.R.I.,* Chambre, 2010-2011, 4 mai 2011, COM 220, p. 37, Q. n^{os} 4344, 4375, 4386 et 4405)

Questions jointes de C. Bastin et I. De Meulemeester au premier ministre sur 'les conséquences de la mort d'Oussama Ben Laden' (*C.R.I.,* Chambre, 2010-2011, 5 mai 2011, PLEN 31, p. 1, Q. n° 265 et 266)

Questions jointes d'A. Ponthier, G. Kindermans, C. Bastin, W. De Vriendt et D. Van der Maelen au ministre de la Défense sur 'les conséquences de la mort d'Oussama Ben Laden' (*C.R.I.*, Chambre, 2010-2011, 5 mai 2011, PLEN 31, p. 24, Q. n^{os} 277, 278, 279, 280 et 282)

Questions jointes de G. Annemans et P. Dewael au ministre de la Justice sur 'le profil des ressortissants sur lesquels la Sûreté de l'État enquête' (*C.R.I.,* Chambre, 2010-2011, 5 mai 2011, PLEN 31, p. 12, Q. n^{os} 273 et 274)

Question de S. Bracke au ministre de la Justice sur 'le transit d'armes vers l'Iran' (*Q.R.,* Chambre, 2010-2011, 6 mai 2011, n° 28, p. 182, Q. n° 407)

Question de K. Calvo à la ministre de l'Intérieur sur 'la nouvelle centrale nucléaire de Borssele' (*C.R.I.,* Chambre, 2010-2011, 18 mai 2011, COM 234, p. 19, Q. n° 4723)

Questions jointes de P. Vanvelthoven, E. Thiébaut, K. Calvo, C. Fonck et L. Dierick à la ministre de l'Intérieur sur 'les stress tests des centrales nucléaires' (*C.R.I.,* Chambre, 2010-2011, 19 mai 2011, PLEN 35, p. 1, Q. n^{os} 307, 308, 309, 310 et 311)

Question de J. Van Esbroeck à la ministre de l'Intérieur sur 'la visite en Belgique d'un prêcheur de haine' (*C.R.I.,* Chambre, 2010-2011, 25 mai 2011, COM 244, p. 9, Q. n° 4756)

Question de K. Van Vaerenbergh au ministre de la Justice sur 'les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées' (*C.R.I.,* Chambre, 2010-2011, 7 juin 2011, COM 255, p. 13, Q. n° 4855)

Question de P. Dewael au ministre de la Justice sur 'la lutte contre les bandes de motards violentes' (*C.R.I.,* Chambre, 2010-2011, 16 juin 2011, PLEN 40, p. 16, Q. n° 391)

Questions jointes de K. Grosemans, P. Moriau et G. Kindermans au ministre de la Défense sur 'le rapport annuel du Comité R concernant les services de renseignement de l'armée' (*C.R.I.,* Chambre, 2010-2011, 16 juin 2011, PLEN 40, p. 22, Q. n^{os} 394, 395 et 396)

Question de S. Bracke au ministre de la Défense sur les 'menaces visant le territoire belge' (*Q.R.,* Chambre, 2010-2011, 23 juin 2011, n° 33, p. 138, Q. n° 75)

Question de Z. Genot au ministre de la Justice sur 'la reconnaissance des mosquées bruxelloises par le SPF Justice' (*C.R.I.,* Chambre, 2010-2011, 28 juin 2011, COM 277, p. 6, Q. n° 5436)

Questions jointes de D. Geerts et F. De Man au ministre de la Défense sur 'le Service général du renseignement et de la sécurité' (*C.R.I.,* Chambre, 2010-2011, 29 juin 2011, COM 279, p. 4, Q. n^{os} 5317 et 5318)

Question de B. Somers au premier ministre sur 'l'augmentation des migrations d'asile et la nécessité de réinstaurer une task force' (*C.R.I.,* Chambre, 2010-2011, 30 juin 2011, PLEN 42, p. 8, Q. n° 428)

Question d'E. Jadot à la ministre de l'Intérieur sur 'les avancées faites sur le sujet de la sécurité d'information – la position du département de l'Intérieur' (*Q.R.,* Chambre, 2010-2011, 7 juillet 2011, n° 42, p. 65, Q. n° 410)

Question d'A. Colen au ministre des Affaires étrangères sur les 'musulmans qui se sont rendus en Libye pour y participer aux combats' (*Q.R.* Chambre, 2010-2011, 12 juillet 2011, n° 35, p. 34, Q. n° 228)

Question de P. Logghe à la ministre de l'Intérieur sur les 'écoles islamiques saoudiennes' (*Q.R.,* Chambre, 2010-2011, 12 juillet 2011, n° 35, p. 215, Q. n° 183)

Question de K. Grosemans au ministre des Pensions sur le 'financement de groupes terroristes par l'argent des pensions belges' (*Q.R.,* Chambre, 2010-2011, 18 juillet 2011, n° 36, p. 150, Q. n° 81)

Question de S. Smeyers à la ministre des Affaires sociales sur le 'filtrage des demandeurs d'asile par la Sûreté de l'État' (*Q.R.,* Chambre, 2010-2011, 2 août 2011, n° 37, p. 245,
Q. n° 65)

Question de D. Dumery au ministre des Affaires étrangères sur 'le projet européen 'Virtuoso'' (*Q.R.,* Chambre, 2010-2011, 11 août 2011, n° 38, p. 15, Q. n° 271)

Question de P. Dedecker au ministre pour l'Entreprise sur 'l'obligation de collaboration imposée aux entreprises internet' (*Q.R.,* Chambre, 2010-2011, 15 septembre 2011, n° 40, p. 216, Q. n° 156)

Questions jointes de S. De Wit, J. Galant, B. Schoofs, C. Van Cauter, S. Van Hecke, S. Verherstraeten et L. Musin au ministre de la Justice sur 'les causes des nombreuses évasions qui se sont produites dans les prisons belges cette année' (*C.R.I.,* Chambre, 2010-2011, 4 octobre 2011, COM 303, p. 5, Q. n^{os} 5879, 5914, 6265, 6269, 6298, 6307, 6324, 6387 et 6388)

Questions jointes de J. Van Esbroeck et A. Ponthier à la ministre de l'Intérieur sur 'un agent frappé lors du contrôle d'une personne en burqa' (*C.R.I.,* Chambre, 2010-2011, 5 octobre 2011, COM 307, p. 27, Q. n^{os} 6337 et 6376)

Question de S. Van Hecke au ministre de la Justice sur 'une association d'aide, couverture pour les services de renseignement' (*C.R.I.,* Chambre, 2011-2012, 12 octobre 2011, COM 309, p. 44, Q. n° 6099)

Question de N. Lanjri au secrétaire d'État au Budget sur les 'demandeurs d'asile – programmes de réinstallation' (*Q.R.,* Chambre, 2011-2012, 17 octobre 2011, n° 43, p. 143, Q. n° 157)

Question de B. Schoofs au ministre de la Justice sur 'la présence d'intégristes musulmans au sein du conseil de rédaction de la Moslim Televisie en Radio Omroep' (*C.R.I.,* Chambre, 2011-2012, 18 octobre 2011, COM 313, p. 51, Q. n° 6477)

Question d'E. Jadot au ministre de la Justice sur 'la présence d'une organisation de renseignement pakistanaise sur le sol belge et le suivi y étant accordé par les services de la Sûreté' (*Q.R.,* Chambre, 2011-2012, 26 octobre 2011, n° 44, p. 56, Q. n° 588)

Question de N. Lanjri au secrétaire d'État à l'Intégration sociale sur 'l'OTAN – décision de ne pas autoriser l'implantation d'un centre d'accueil aux abords du SHAPE' (*Q.R.,* Chambre, 2011-2012, 4 novembre 2011, n° 45, p. 161, Q. n° 87)

Question de K. Grosemans au ministre de la Défense sur 'les Standard Operating Procedures' (*C.R.I.,* Chambre, 2011-2012, 9 novembre 2011, COM 331, p. 4, Q. n° 6666)

Questions jointes de D. Ducarme au ministre de la Justice sur 'la mutinerie au sein de la prison d'Andenne' (*C.R.I.,* Chambre, 2011-2012, 23 novembre 2011, COM 343, p. 24, Q. n^{os} 7146 et 7147)

Question de C. Van Cauter au ministre de la Justice sur le 'SPF Justice – frais de personnel' (*Q.R.,* Chambre, 2011-2012, 5 décembre 2011, n° 48, p. 235, Q. n° 621)

Question de J. Van Esbroeck à la ministre de l'Intérieur sur 'l'extrémisme islamiste dans les petites agglomérations et communes' (*Q.R.,* Chambre, 2011-2012, 5 décembre 2011, n° 48, p. 315, Q. n° 640)

ANNEXE D.
LA DÉCLARATION DE BERLIN DE LA CONFÉRENCE DES ORGANES DE CONTRÔLE EUROPÉENS[164]

7^{e} conférence
des commissions parlementaires de contrôle des services de renseignements
et de sécurité des États membres de l'Union européenne,
ainsi que de Norvège et de Suisse

Berlin
les **27** et **28** octobre **2011**

Déclaration de Berlin

Les participants à la 7° conférence des commissions parlementaires de contrôle des services de renseignements et de sécurité des États membres de l'Union européenne, ainsi que de Norvège et de Suisse,

164 Cette déclaration n'est disponible qu'en français, allemand et anglais.

Considérant l'importance du contrôle parlementaire des services de renseignements et de sécurité dans la sauvegarde des droits fondamentaux et des principes de l'État de droit en Europe ;

Conscients que l'acceptation par le grand public des activités déployées par les services de renseignements et de sécurité et la confiance en ces services dépendent aussi de l'efficacité du contrôle exercé par les parlementaires ;

Conscients du rôle majeur joué par les services de renseignements et de sécurité dans les décisions de politique étrangère et de sécurité prises par les États membres de l'Union européenne ;

Conscients de la contribution apportée par les activités des services de renseignements et de sécurité à la protection des régimes démocratiques en Europe face aux menaces terroristes ;

Vu les conclusions des conférences de Rome, Bucarest, Lisbonne, Tallinn, Bruxelles et Berlin ;

Déclarent ce qui suit :

1) Plus de 20 ans après la fin de la Guerre froide et 10 ans après les attentats de New York et Washington, les services de renseignements et de sécurité sont confrontés à maints défis, au rang desquels figurent notamment les menaces que fait peser le terrorisme international sur l'État de droit démocratique ;
2) Dans un État de droit démocratique, les activités des services de renseignements et de sécurité doivent s'accompagner d'un devoir d'information et de contrôle parlementaire venant s'ajouter à la tutelle du ministre responsable, au contrôle du pouvoir judiciaire et à celui exercé par l'opinion publique ;
3) Les droits d'immixtion dont sont investis les services de renseignements et de sécurité pour maintenir et assurer la sécurité des citoyens européens imposent de soumettre ces services à un contrôle efficace en vue de sauvegarder les normes de l'État de droit. Il incombe dès lors d'investir les organes de contrôle parlementaire des services de renseignements et de sécurité des compétences adéquates et de leur assurer une dotation appropriée en termes de ressources humaines et matérielles ;
4) Face à l'internationalisation croissante de la coopération entre services de renseignements et de sécurité et à l'échange d'informations qu'induit cette évolution, il est nécessaire d'améliorer le contrôle parlementaire des services de renseignements et de sécurité en la matière ;
5) Nous prenons acte de la création à l'initiative de la Belgique d'un réseau d'expertise européen relatif au contrôle des services de renseignements. Baptisé ENNIR (European Network of National Intelligence Reviewers), ce réseau basé sur un site internet a pour objet premier d'améliorer le contrôle démocratique des activités des services de renseignements et de sécurité et de permettre un meilleur échange entre les organes de contrôle ainsi mis en réseau. Nous soutenons la mise en œuvre de l'initiative belge, appelée à déboucher sur la constitution volontaire d'une plateforme la plus large d'échange d'expertise et d'expériences ;
6) Nous convenons de la nécessité et de l'utilité d'un échange d'informations intensif entre les États membres de l'UE, la Norvège et la Suisse dans le domaine du contrôle des services de renseignements et de sécurité ;

ANNEXE E.
LA RÉGLEMENTATION LÉGALE EN MATIÈRE D'ARCHIVAGE ET DE DESTRUCTION DE DONNÉES DE LA VSSE ET DU SGRS

Après un certain temps, les données recueillies et traitées n'ont généralement plus de valeur pour les services de renseignement. Il convient alors de décider de leur destruction ou de leur archivage.

Cette problématique est principalement régie par la Loi relative aux archives du 24 juin 1955 et ses arrêtés d'exécution.[165] Mais de nombreuses autres lois s'avèrent tout aussi pertinentes en ce qui concerne les services de renseignement : la Loi relative au traitement des données à caractère personnel du 8 décembre 1992, la Loi relative à la publicité de l'administration du 11 avril 1994, la Loi relative à la classification du 11 décembre 1998, et la Loi organique des services de renseignement du 30 novembre 1998.

Etant donné les implications inévitables de l'application de cette législation sur l'efficacité du fonctionnement des services de renseignement et sur la vie privée des personnes qui figurent dans les fichiers de ces services, le Comité permanent R a décidé de consacrer une brève analyse juridique à ce thème.

1. Portée de la Loi relative aux archives

La Loi relative aux archives régit différents aspects : le moment où et la manière dont les archives[166] doivent être déposés aux Archives de l'État (article 1er) et deviennent dès lors publiques dans certains cas (article 3), leur éventuelle destruction (articles 2 et 5), et la surveillance des documents qui n'ont pas été déposés aux Archives de l'État (article 6).

Jusque récemment, le versement obligatoire des documents aux Archives de l'État s'appliquait uniquement aux « *documents de plus de cent ans* ». Cette disposition a toutefois été modifiée en 2009[167] : désormais, les « *documents datant de plus de trente ans* » sont accessibles au public dans l'enceinte des Archives de l'État.[168]

Cela signifie-t-il que les services de renseignement doivent désormais verser aux Archives de l'État tous les documents datant de 30 ans ? Certainement pas. Le champ d'application de la Loi relative aux archives se limite en effet aux archives « mortes » ou statiques. En effet : « *Il ressort des différentes dispositions de la loi relatives aux archives que la mission de service public des Archives de l'État consiste à conserver les archives statiques [nous soulignons] des différents producteurs d'archives et à les rendre accessibles au*

165 L'A.R. du 18 août 2010 portant exécution des articles 1er, 5 et 6*bis* de la loi du 24 juin 1955 relative aux archives (AR Archives I) et l'Arrêté royal du 18 août 2010 portant exécution des articles 5 et 6 de la loi du 24 juin 1955 relative aux archives (AR Archives II).

166 Cette notion n'est pas définie dans la Loi relative aux archives.

167 Loi du 6 mai 2009, *MB* 19 mai 2009.

168 Le raccourcissement du délai à 30 ans a été assorti d'une période transitoire de 10 ans, par laquelle les administrations de l'État ont jusqu'au 23 septembre 2020 pour appliquer la nouvelle réglementation (art. 6*bis* Loi Archives et art. 2-3 AR Archives I). Les documents vieux de 100 ans en date du 23 septembre 2010 doivent être transférés aux Archives de l'État dans le courant de l'année (art. 3, alinéa 2 AR Archives I).

public ».[169] Il s'agit des archives dont une administration estime qu'elles ne présentent plus aucune utilité pour son fonctionnement. Les archives « vivantes » ou dynamiques (à savoir les documents susceptibles de présenter encore un intérêt et d'être utilisés[170]) ne relèvent pas de la Loi relative aux archives.[171]

Il est tout à fait évident qu'un document qu'une autorité utilise toujours comme outil de travail ne peut pas relever du champ d'application de la Loi relative aux archives. Sinon, une administration serait obligée de céder les documents dont elle a besoin dans le cadre de ses missions légales et d'en faire préalablement des copies le cas échéant.

Le fait que cette administration conserve de tels documents dans ce qu'elle appelle éventuellement ses « archives » ne change rien. Ce n'est que lorsque l'utilité pratique des documents « archivés » diminue au fil des ans que le détenteur peut souhaiter se défaire de certains documents superflus, soit en les détruisant, soit en les transférant dans des archives « mortes ». Dès cet instant (et pas avant), les dispositions de la Loi relative aux archives entrent en application. En effet, les documents qui ne présentent plus aucune utilité pour l'autorité concernée peuvent rester ou devenir intéressants en raison de leur valeur scientifique ou historique.[172]

Concrètement, cela signifie que :

- les documents dont un service public estime qu'ils ne présentent plus aucune utilité pour son fonctionnement *et*[173] qui ont plus de 30 ans *doivent* être versés aux Archives de l'État (art. 1er, alinéas 1er et 2, L.Archives) ; ces documents sont en principe publics (art. 3 L.Archives) ;
- les documents dont un service public estime qu'ils ne présentent plus aucune utilité pour son fonctionnement *et* qui ont moins de 30 ans *peuvent* être versés aux Archives

169 Avis du Conseil d'État du 23 février 2010 (*MB* 22 octobre 2010, 62835).

170 Les notions d'archives « vivantes » ou dynamiques constituent en quelque sorte un paradoxe. Tant que des documents sont « vivants » (c'est-à-dire peuvent être ou sont utilisés dans le cadre du fonctionnement du service concerné), ils ne font effectivement pas partie des archives de ce service, mais des documents de travail.

171 Voir Avis du 23 février 2010 (*MB* 22 octobre 2010, 62832 et suiv.) et Avis du 4 mai 2010 (*MB* 23 septembre 2010, 58713 et suiv.) du Conseil d'État. Le Conseil d'État a formulé ses avis principalement dans le contexte d'une discussion amorcée depuis longtemps par les autorités fédérales et les entités fédérées à propos de la répartition des compétences en matière de gestion des archives. Selon le Conseil d'État, les autorités fédérales ne peuvent pas édicter de réglementation qui porte sur les documents de travail (les archives « vivantes ») des autorités qui relèvent de la compétence des entités fédérées. Cependant, l'approche du Conseil d'État s'applique également en dehors du contexte de cette question de compétence (voir note de bas de page 4).

172 Pour le Conseil d'État, ce n'est qu'à ce moment-là qu'il peut s'avérer légitime de laisser une autre autorité (en l'espèce les Archives de l'État) décider du sort de ces documents (Avis du 23 février 2010 du Conseil d'État (*MB* 22 octobre 2010, 62832).

173 Avant la modification de la loi en 2009, il était évident que les documents qui avaient atteint la limite d'âge stipulée dans la loi (à savoir 100 ans) étaient d'emblée considérés comme de véritables archives, dans le sens où ils n'étaient plus utiles au fonctionnement du service concerné. Il n'était dès lors pas nécessaire d'opérer une distinction entre les deux critères. Depuis la modification de la loi en 2009, où le délai a été ramené de 100 à 30 ans, il est toutefois souhaitable d'insister sur l'importance de ces deux critères. Il se peut en effet que des documents datant de 30 ans soient encore utiles au fonctionnement de certains services, comme les services de police et de renseignement ou l'administration pénitentiaire. La « destination que l'autorité confère à un document » et son « âge » doivent dès lors être considérés comme deux critères appréciables séparément et cumulables.

de l'État (art. 1er, alinéa 3, L.Archives) ; ces documents peuvent être consultés selon les modalités définies par le Roi (art. 4 L.Archives) ;
- les documents dont un service public estime qu'ils ne présentent plus aucune utilité pour son fonctionnement ne peuvent être détruits qu'avec l'autorisation de l'archiviste général du Royaume (art. 5 L.Archives)[174] ;
- les archives qui reposent aux Archives de l'État ne peuvent pas être détruites sans le consentement de l'autorité d'origine (art. 2 L.Archives) ;
- les documents (archives) qui sont conservés par une administration de l'État sont sous la surveillance de l'archiviste général du Royaume (art. 6 L.Archives).

Cependant, des règles particulières s'appliquent aux services de renseignement. Avant de les analyser, deux aspects de la législation relative aux archives sont examinés de près.

1.1. Dispense(s) de transfert

Plusieurs autorités (dont le ministère de la Défense, et donc le SGRS[175]) sont « dispensées du transfert » de leurs archives de moins de 50 ans.[176] La bonne conservation et la consultation publique de ces archives doivent toutefois être garanties dans les mêmes conditions que dans les Archives de l'État. La dispense s'applique de plein droit, mais se limite donc à une dispense du transfert requis au sens strict. En d'autres termes, elle concerne uniquement le lieu de conservation, et non le caractère accessible ou non des archives. Le SGRS peut donc conserver ses archives de moins de 50 ans, mais devra veiller à ce que le public puisse consulter les archives de plus de 30 ans dans les mêmes conditions que dans les Archives de l'État.

L'article 10 de l'AR Archives I semble prévoir une autre dispense : à la demande de l'autorité détentrice de l'archive, l'archiviste général du Royaume peut accorder une dispense de transfert pour un délai renouvelable de dix ans si *« le service public demandeur peut démontrer l'utilité administrative de ces archives »*. À l'instar du Conseil d'État, le Comité permanent R estime que cette disposition va à l'encontre de la Loi relative aux archives.[177] Elle implique en effet que cette loi s'applique également aux documents qu'une

---

174 En effet, l'archiviste du Royaume peut décider qu'une destruction n'est pas souhaitable parce que les documents doivent être conservés dans les Archives de l'État en raison de leur valeur scientifique, historique ou sociale.

175 Le ministre de la Justice ou la VSSE ne sont pas expressément mentionnés et ne sont donc pas dispensés.

176 Art. 9 AR Archives I.

177 En dépit des remarques formulées par le Conseil d'État, le Roi a maintenu son interprétation large de la Loi relative aux archives : « *La définition large de la notion d'archives est maintenue dans le projet d'arrêté en raison du fait que les missions des Archives de l'État s'étendent nécessairement aussi aux archives vivantes. Les Archives de l'État ne peuvent exercer judicieusement leurs tâches vis-à-vis des archives mortes que dans la mesure où elles peuvent exercer la surveillance [nous soulignons] sur la manière dont les archives sont conservées alors qu'elles possèdent encore une utilité administrative et par conséquent sont encore vivantes. […] C'est pour la même raison que la compétence des Archives de l'État en matière de destruction d'archives vivantes [nous soulignons] est maintenue* ». (Rapport au Roi précédant l'AR du 18 août 2010, *MB* 23 septembre 2010, 58712.) Cependant, les dispositions des arrêtés d'exécution indiquent également que le Roi souhaitait étendre aux archives « vivantes » le champ d'application de la Loi relative aux archives. Ainsi la notion d'« archives » a-t-elle fait

administration utilise encore pour accomplir sa mission légale. Il serait absolument aberrant qu'un service (de renseignement) doive « prouver » à un archiviste que certains documents peuvent présenter une utilité pour l'exécution de sa mission légale (en l'espèce, garantir la sécurité de l'État).[178]

1.2. Surveillance par l'archiviste du Royaume

L'article 6 de la Loi relative aux archives octroie à l'archiviste du Royaume la compétence d'exercer une surveillance sur les documents conservés par une administration d'État. Le Comité estime que cette disposition fait une nouvelle fois référence aux « archives mortes » qui n'ont pas encore été versées aux Archives de l'État, par exemple parce que les documents en question ont moins de 30 ans.

Le Roi a une nouvelle fois donné une interprétation large à cette disposition en autorisant également la surveillance des archives « vivantes » des administrations (cette surveillance porte sur la conservation, le classement et l'accessibilité des documents). En effet, les services sont tenus de permettre à l'archiviste du Royaume d'accéder à leurs archives (c.-à-d. à toute la documentation vu le champ d'application étendu que le Roi a conféré à la Loi relative aux archives).[179] À cet égard, il est toutefois stipulé que les procédures et mesures de sécurité requises sont adoptées pour lui octroyer l'accès aux archives qui ont fait l'objet d'une classification ou qui contiennent des données à caractère personnel, et ce dans le respect de la législation en vigueur.[180] Concrètement, cela signifie que la surveillance ne porte pas sur le contenu des documents, mais uniquement sur les conditions dans lesquelles les « archives » sont conservées, et que le service de renseignement concerné peut exiger que l'archiviste dispose des habilitations ou attestations de sécurité requises (il se rend effectivement dans des zones classifiées).

2. Règles particulières pour la VSSE et le SGRS[181]

2.1. Documents administratifs *versus* archives

En ce qui concerne la publicité/consultation éventuelle de certains documents disponibles au sein des services de renseignement, il convient également de tenir compte de la Loi

---

l'objet d'une définition très vaste, à savoir : « *tous les documents qui, quels que soient leur date […] sont destinés, par leur nature, à être conservés par une autorité publique […] dans la mesure où ces documents ont été reçus ou produits dans l'exercice de ses activités, de ses fonctions ou pour maintenir ses droits et obligations (nous soulignons)* » (art. 1er AR Archives I et art. 1er AR Archives II).

178 Cette dispense figurait déjà à l'article 3 de l'A.R. initial du 12 décembre 1957 concernant l'exécution de la loi du 24 juin 1955 relative aux archives. À l'époque, il s'agissait toutefois d'un automatisme : les documents qui présentaient un intérêt administratif indiscutable ne devaient pas être transférés. Ainsi, le Roi déterminait précisément le champ d'application de la Loi relative aux archives : un document qui présente encore un intérêt administratif ne peut pas faire partie des Archives de l'État, quel que soit son âge.

179 Art. 10 AR Archives II.

180 Art. 10 AR Archives II.

181 La réglementation exposée ci-après ne s'applique que partiellement aux documents qui reposent à l'OCAM.

relative à la publicité de l'administration (LPA).[182] Cette loi stipule les conditions dans lesquelles les documents administratifs[183] peuvent être consultés par le public. La question est donc de savoir quelle est la relation entre la LPA et les règles en matière de publicité et de consultation de la Loi relative aux archives.

Le principe de base étant que dès que des documents administratifs se trouvent dans les Archives de l'État (ou les Archives de l'État dans les provinces) parce qu'ils devaient y être versés (en d'autres termes, parce qu'ils ont plus de 30 ans), leur publicité/consultation éventuelle est régie conformément aux dispositions de la Loi relative aux archives, et non plus de la Loi relative à la publicité de l'administration.[184] Il en va de même pour les documents administratifs du SGRS qui ont plus de 30 ans, mais qui n'ont pas encore été transférés dans les Archives de l'État.[185]

En revanche, la publicité/consultation éventuelle des documents administratifs de moins de 30 ans est régie conformément aux dispositions de la Loi du 11 avril 1994. Il s'agit alors de documents administratifs qui (1) soit présentent toujours une utilité pour le fonctionnement du service et ne sont donc pas des archives ; (2) soit ne présentent plus aucune utilité pour le fonctionnement du service et ont été déposés dans des archives ; (3) soit ne présentent plus aucune utilité pour le fonctionnement du service et ont été volontairement versés aux Archives de l'État.[186] Pour ces documents, ce n'est donc pas l'archiviste du Royaume qui décide de leur publicité, mais bien le service même.[187] Comme pour les documents administratifs qui présentent toujours une utilité, la publicité peut être refusée si l'une des exceptions de la loi peut être invoquée. Par exemple, pour les services de renseignement, il peut s'agir de « *la sûreté ou la défense nationale* » (art. 6 § 1er, 4° LPA) ou des « *intérêts visés à l'article 3 de la loi du 11 décembre 1998* » (art. 6 § 2, 4° LPA).

---

182 Loi relative à la publicité de l'administration du 11 avril 1994, *MB* 30 juin 1994.

183 Cette notion est définie de manière très large : toute information, sous quelque forme que ce soit, dont une autorité administrative dispose (art. 1er, alinéa 2, 2° LPA).

184 C'est ce qui ressort de l'art. 11, alinéa 4 de la Loi relative à la publicité de l'administration. Voir *Doc. parl.* Chambre 1992-93, n° 1112/1, 22.

185 En vertu de l'article 9 AR Archives I, le SGRS est dispensé de transférer ses archives de moins de 50 ans aux Archives de l'État, du moins dans la mesure où leur bonne conservation, leur accessibilité, etc. restent garanties et où le public peut consulter ces archives dans les mêmes conditions qu'aux Archives de l'État. Nonobstant cette dispense de transfert, les autres dispositions de la Loi relative aux archives restent d'application sur toutes les archives du SGRS de plus de 30 ans.

186 Le fait que l'article 11, alinéa 1er LPA stipule que la LPA s'applique également aux documents administratifs qui « sont déposés dans des archives » peut prêter à confusion. La notion d'archives doit ici être comprise dans le sens d'archives autres que les Archives de l'État ou les Archives de l'État dans les provinces. Les services peuvent en effet décider à un moment donné que les documents administratifs qui ne présentent plus aucun intérêt soient conservés dans des archives (en gestion propre ou non), dans l'attente d'un transfert (obligatoire) vers les Archives de l'État. La Loi du 11 avril 1994 reste également d'application sur les documents administratifs dans ces archives afin d'éviter que des documents soient soustraits à la publicité par leur dépôt aux archives de l'autorité concernée (*Doc. parl.* Chambre 1992-93, n° 1112/1, 22).

187 Voir F. SCHRAM, « Archief en openbaarheid van bestuur » dans R. OPSOMMER e.a. (eds.), *De archivaris, de wet en de rechtbank*, Brugge, die Keure, 2004, 16-17.

2.2. Destruction de données à caractère personnel

L'article 21 L.R&S stipule qu'un service de renseignement peut conserver les données à caractère personnel qu'il traite[188] aussi longtemps qu'il l'estime nécessaire aux finalités pour lesquelles elles sont enregistrées.[189] Mais comme l'article précise aussi explicitement qu'il convient de tenir compte des dispositions légales relatives aux Archives de l'État, il n'y a aucune contradiction : dès que les données à caractère personnel ne présentent plus aucune utilité pour le service (que ce soit après un an ou seulement après 40 ans), l'archiviste général du Royaume doit donner son accord à une éventuelle destruction. S'il s'oppose à une destruction, il incombe de nouveau au service de renseignement concerné de décider si ces données sont conservées dans ses propres archives (pour la VSSE, cette possibilité n'est envisageable que pour des documents de moins de 30 ans) ou versées aux Archives de l'État (obligatoire pour les documents de plus de 30 ans).

2.3. Destruction de données (à caractère personnel) inexactes

Cette règle générale (destruction possible uniquement moyennant l'accord de l'archiviste du Royaume) admet une exception : l'article 16 § 2, 1° de la Loi relative au traitement des données à caractère personnel (entre autres) stipule que les données à caractère personnel inexactes doivent être rectifiées ou supprimées. En l'espèce, l'on peut difficilement demander l'approbation de l'archiviste du Royaume. Dans ce cas, les données à caractère personnel ne sont pas détruites parce qu'elles ne présentent plus aucune utilité, mais parce qu'elles sont incorrectes. D'un point de vue historique et scientifique, il est également important que toute donnée erronée disparaisse des fichiers de données.

2.4. Destruction de données (à caractère personnel) classifiées

Un problème se pose si les services de renseignement souhaitent détruire des archives classifiées qui ne présentent plus aucune utilité pour leur fonctionnement.[190] En principe, l'archiviste du Royaume doit approuver une telle destruction. Par conséquent, pour être en mesure d'apprécier leur valeur historique ou scientifique, il doit prendre connaissance du contenu de ces documents. Cela suppose qu'il est titulaire d'une habilitation de sécurité correspondante. En effet, la loi relative à la classification (qui est ultérieure à la Loi relative aux archives et doit être considérée comme *lex specialis)* ne prévoit pas d'exception pour l'archiviste du Royaume.[191]

---

188 Ce règlement ne porte donc que sur les données à caractère personnel. En droit, il n'y a toutefois aucune différence de traitement avec les données non personnelles : dès qu'elles ne présentent plus aucune utilité pour le service de renseignement, l'archiviste décide de leur sort.

189 En principe, ces données doivent être détruites d'une manière ou d'une autre après un certain délai qui suit le dernier traitement. Ce délai doit être fixé par le Roi. Comme le Comité l'a déjà fait remarquer à plusieurs reprises, ce délai n'a pas encore été fixé.

190 Ce n'est pas parce que des données ne sont plus utiles pour le service qu'automatiquement la classification n'est plus fondée. Le document peut effectivement donner une indication des modes opératoires toujours en vigueur.

191 De telles exceptions s'appliquent toutefois aux magistrats de parquet, aux membres de la Cellule de traitement des informations financières, et aux membres de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité (art. 8 L.C&HS).

2.5. Le transfert d'informations classifiées vers les Archives de l'État

Le transfert et le stockage de documents classifiés vers les Archives de l'État impliquent d'une part qu'un certain nombre de ses collaborateurs disposent de l'habilitation de sécurité requise et, d'autre part, qu'il soit satisfait à toutes les mesures de sécurité matérielles et procédurales.

En outre, l'accès à ces documents doit être limité aux titulaires d'une habilitation de sécurité. Ces personnes ne peuvent pas rapporter publiquement leurs éventuelles constatations.

2.6. La protection de l'identité des informateurs

La protection de l'identité des informateurs est essentielle pour un service de renseignement. Cette préoccupation s'est également traduite dans la Loi du 30 novembre 1998 : l'article 13 stipule que les services de renseignement doivent veiller à la « *sécurité des données ayant trait aux sources humaines* ». Cette obligation, qui figurait initialement à l'article 18 L.R&S, avait pour but d'instaurer un « véritable contrat de confiance »[192] entre l'informateur et le service de renseignement, même s'il n'exige pas l'anonymat. Il s'agissait de garantir ce principe de confiance par la classification de l'identité de la source. Cette piste n'a pas été retenue parce que la Loi relative à la classification avait déjà été votée par la Chambre à l'époque.[193] Concrètement, cela signifie que l'obligation énoncée (aujourd'hui) à l'article 13 ne peut être respectée qu'en classifiant les données relatives à l'identité. Dans ce cas, l'identité d'une source est une « donnée à caractère personnel classifiée » à laquelle s'appliquent les règles exposées ci-dessus.

2.7. Données figurant dans des dossiers de sécurité ou de vérification

L'article 25 de la Loi relative à la classification énonce une disposition spécifique pour la destruction des données (à caractère personnel) qui ont été recueillies dans le cadre d'une vérification de sécurité ou d'une enquête de sécurité. Bien que cette disposition englobe différentes hypothèses, l'on y trouve un dénominateur commun : les « données à caractère personnel » (c'est-à-dire les données personnelles), voire le dossier complet, doivent être détruites dès qu'elles ne sont plus utiles aux fins pour lesquelles les données ont été recueillies ou pour lesquelles le dossier a été constitué. Comme la Loi relative à la classification constitue une *lex specialis* en regard de la Loi relative aux archives, l'archiviste n'intervient pas dans la destruction.

2.8. Destructions de données MRD obtenues illégalement

Enfin, l'article 43/6 L.R&S contient une disposition spécifique pour la destruction des données qui ont été recueillies sur la base d'une méthode spécifique ou exceptionnelle de

192 *Doc. parl.* Sénat, 1997-98, n° 758/3, 11.

193 *Doc. parl.* Sénat 1997-98, n° 758/3, 18 et *Doc. parl.* Sénat 1997-98, n° 758/10, 157. L'article 3 de la Loi relative à la classification ne fait pourtant pas mention de la « protection des sources ».

recueil de données mise en œuvre illégalement. Si le Comité permanent R constate une telle illégalité, les données recueillies doivent être détruites. Cette disposition ne fait pas explicitement référence à la Loi relative aux archives. En outre, cette situation ne concerne pas la destruction de données qui ne présentent plus aucune utilité pour les services de renseignement (article 21 L.R&S). De ce point de vue, il est logique que la destruction ne soit pas tributaire de l'autorisation de l'archiviste du Royaume.

3. Conclusion et recommandations

Cette analyse démontre que les différentes lois, qui régissent chacune un aspect de la problématique de la destruction et l'archivage de documents des services de renseignement, sont complémentaires et opérationnelles, car le champ d'application de la Loi relative aux archives (comme indiqué par le Conseil d'État) se limite aux « archives mortes ». Déclarer la Loi relative aux archives applicable aux « archives vivantes », c'est créer un imbroglio inexploitable et inextricable tant sur le plan juridique que pratique.

Si les services de renseignement respectent l'esprit et la lettre des différentes dispositions discutées (par exemple, signaler en tant que tels les documents qui ne présentent plus aucune utilité et déclassifier si possible les informations), les différents intérêts en jeu sont alors parfaitement conciliables. Le Comité permanent R peut, le cas échéant, ouvrir une enquête de contrôle en la matière.

Il n'empêche que le Comité plaide en faveur de l'instauration d'un système où les classifications prennent fin de plein droit après un délai donné (par exemple, 30 ans pour les documents classifiés « secrets » et 50 ans pour les documents « très secrets »), et ce à moins qu'elles ne soient explicitement renouvelées. Ceci exige une modification de la loi relative à la classification.

RAPPORT D'ACTIVITÉS 2011
ACTIVITEITENVERSLAG 2011

Quis custodiet ipsos custodes?

Quis custodiet ipsos custodes? is een publicatiereeks die een bijdrage wil leveren tot het bevorderen van een geïnformeerde discussie over de werking, de bevoegdheden en de controle op de inlichtingen- en veiligheidsdiensten en op het inlichtingenwerk. In deze reeks worden o.m. wetenschappelijke studies, de activiteitenverslagen van het Vast Comité I en verslagboeken van colloquia opgenomen.

Redactie

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Leuvenseweg 48 bus 5, 1000 Brussel (02 286 29 88).

Reeks verschenen in deze reeks

1) D. Van Daele en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Vast Comité I, *Activiteitenverslag 2006,* 2007, 147 p.
3) Vast Comité I, *Activiteitenverslag 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe,* 2010, 220 p.
5) Vast Comité I, *Activiteitenverslag 2008*, 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Vast Comité I, *Activiteitenverslag 2009*, 2010, 127 p.
8) Vast Comité I, *Activiteitenverslag 2010*, 2011, 119 p.
9) Vast Comité I, *Activiteitenverslag 2011*, 2012, 134 p.

ACTIVITEITENVERSLAG 2011

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de inlichtingen-
en veiligheidsdiensten

intersentia
Antwerpen – Cambridge

Voorliggend *Activiteitenverslag 2011* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 8 mei 2012.

(*getekend*)
Guy Rapaille, voorzitter
Gérald Vande Walle, raadsheer
Peter De Smet, raadsheer
Wouter De Ridder, griffier

Activiteitenverslag 2011
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

ISBN 978-94-000-0313-2
D/2012/7849/49
NUR 823

INHOUD

LIJST VAN AFKORTINGEN

ADIV	Algemene Dienst inlichting en veiligheid van de Krijgsmacht
BIM	Bijzondere inlichtingenmethoden
BIM-commissie	Bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door inlichtingen- en veiligheidsdiensten
BIM-Wet	Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten
BS	Belgisch Staatsblad
BSC	*Balanced Score Card*
CANVEK	Commissie van advies voor de niet-verspreiding van kernwapens
CERT	*Computer Emergency Response Team*
CRIV	Compte Rendu Intégral – Integraal Verslag
ENNIR	*European Network of National Intelligence Reviewers*
FOD	Federale overheidsdienst
Parl.St.	Parlementaire Stukken van Kamer en Senaat
Hand.	Handelingen
HUMINT	*Human intelligence*
ICT	*Information and Communication Technologies*
IMINT	*Image intelligence*
K.B.	Koninklijk besluit
KB C&VM	Koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
KB OCAD	Koninklijk besluit van 28 november 2006 tot uitvoering van de Wet van10 juli 2006 betreffende de analyse van de dreiging
M.B.	Ministerieel besluit
MCIV	Ministerieel Comité voor inlichting en veiligheid
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open source intelligence*
RFI	*Request for Information*

SIGINT	*Signals intelligence*
Sv.	Wetboek van Strafvordering
Vast Comité I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten
Vr. en Antw.	Schriftelijke vragen en antwoorden (Kamer of Senaat)
VSSE	Veiligheid van de Staat
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.C&VM	Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
WEP	Wetenschappelijk en economisch potentieel
W.OCAD	Wet van 10 juli 2006 betreffende de analyse van de dreiging
W.Toezicht	Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse

WOORD VOORAF

De redactie van een jaarverslag vormt de ideale gelegenheid om terug te blikken op de eigen werking: Welke zijn de realisaties? Waar lagen de accenten? Werden de beoogde doelstellingen bereikt? Terugblikkend op 2011, zijn er heel wat zaken die bijzondere aandacht verdienen. In dit voorwoord selecteren we er vier.

Vooreerst was er de audit bij de Algemene Dienst inlichting en veiligheid. Nadat de Veiligheid van de Staat in 2009 grondig werd doorgelicht door het Vast Comité I, was het vorig jaar de beurt aan de militaire inlichtingendienst. De uitvoering van een dergelijke audit is arbeidsintensief en heeft derhalve heel wat capaciteit geëist van het Comité. Zowel de Begeleidingscommissie van de Senaat, de minister van Defensie alsook de ADIV erkenden de meerwaarde van de auditresultaten in termen van verbetering van de effectiviteit en de efficiëntie (zie II.1 en IX.2.1).

Rome is niet op één dag gebouwd en dat geldt ook voor het *European Network of National Intelligence Reviewers*, kortweg ENNIR, een initiatief van het Comité en zijn Senatoriële Begeleidingscommissie. Dit via een website aangestuurd informatie-uitwisselingsplatform voor Europese toezichthouders op inlichtingen- en veiligheidsdiensten, werd opnieuw concreter: de website staat *online* (www.ennir.be) en verschillende landen zegden reeds hun medewerking toe (zie V.5). In 2012 zal verder worden gewerkt aan de uitbouw van dit netwerk dat moet toelaten interessante informatie en *best practices* uit te wisselen.

Van geheel andere orde was de verhuis van het Vast Comité I naar het nieuwe Forum-gebouw. De goede voorbereidingen maakten dat de hele operatie vlekkeloos verliep (zie VIII.5). Uiteraard rendeerde de investering van mensen en middelen die met deze verhuis gepaard ging niet rechtstreeks in termen van 'controle op de inlichtingendiensten'. Ongetwijfeld zullen de vernieuwde werkomgeving en de directe nabijheid van de belangrijkste partner van het Comité – met name het Parlement – een positief effect hebben op onze toekomstige werking.

Bovenal echter was 2011 het eerste jaar waarin de Wet op de bijzondere inlichtingenmethoden volledig van kracht was (zie III). Voor het eerst konden de Veiligheid van de Staat en de Algemene Dienst inlichting en veiligheid specifieke én uitzonderlijke bevoegdheden aanwenden. Met de benoeming van de leden van de BIM-commissie was daarenboven – naast de jurisdictionele controle door het Vast Comité I – ook het administratieve toezicht operationeel. Een voorwoord is uiteraard niet de plaats om een evaluatie te maken van dergelijke complexe wetgeving. Toch zijn wij van oordeel dat het afgelopen jaar heeft aange-

toond dat de BIM-wet effectief werkt én werkzaam is: de inlichtingendiensten passen de methoden toe, zonder daarbij in excessen te vervallen en de dubbele, externe controle bewijst zijn waarde als waarborg voor de rechten en vrijheden van personen. Die sterke controle was trouwens één van de voornaamste redenen waarom het Grondwettelijk Hof – op één bepaling na – de volledige BIM-wet intact liet in zijn arrest van 22 september 2011. Dit betekent evenwel niet dat de huidige regeling perfect is; verbeteringen en verfijningen zijn zeker mogelijk. Het Comité zal niet nalaten waar nodig aanbevelingen in die zin te formuleren. Daarnaast zal het blijvend investeren in zijn nieuwe, jurisdictionele opdracht in deze uitermate belangrijke materie.

Guy Rapaille,
Voorzitter van het Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

1 juni 2012

HOOFDSTUK I.
DE OPVOLGING VAN DE AANBEVELINGEN VAN HET VAST COMITÉ I

Eén van de voornaamste taken van het Vast Comité I bestaat er in om ten behoeve van de wetgever en de uitvoerende macht aanbevelingen te formuleren die in het bijzonder betrekking hebben op de rechtmatigheid, de coördinatie en de doelmatigheid van het optreden van de twee Belgische inlichtingendiensten, van het OCAD en – in beperkte mate – van diens ondersteunende diensten. De aanbevelingen die het Comité in 2011 formuleerde, zijn opgenomen in het laatste hoofdstuk van dit activiteitenverslag. In dit inleidende hoofdstuk worden de belangrijkste initiatieven opgesomd die de diverse actoren namen in de lijn van voorgaande aanbevelingen van het Vast Comité I. Tevens wordt extra de aandacht gevestigd op aanbevelingen die het Comité essentieel acht, maar die desondanks nog niet werden geïmplementeerd.

I.1. INITIATIEVEN EN REALISATIES IN DE LIJN VAN DE DIVERSE AANBEVELINGEN

Het Vast Comité I kon vaststellen dat er in 2011 werk was gemaakt van de implementatie van enkele belangrijke aanbevelingen.

I.1.1. IMPLEMENTATIE VAN DE AANBEVELINGEN IN HET KADER VAN DE AUDIT VAN DE VSSE

Het Vast Comité I voerde in 2008-2009 een audit uit bij de Veiligheid van de Staat. Het eindverslag bevatte 31 aanbevelingen, verdeeld over vier thema's (leiderschap, informatiehuishouding, werkprocessen en kwaliteitstevredenheid).[2] In november 2010 vroeg de Begeleidingscommissie van de Senaat aan het Vast Comité I om aan te duiden welke van die aanbevelingen naar zijn oordeel primordiaal waren. Het

[2] VAST COMITÉ I, *Activiteitenverslag 2009*, 5-23 en 81-83.

Comité maakte daarop een selectie aan de hand van vier principes van goed beheer. Aan de betrokken dienst werd een stand van zaken gevraagd.

Een eerste principe vormde '*het vastleggen van doelstellingen na consultatie van de opdrachtgevers en belanghebbenden en vastleggen van de middelen*'. Met betrekking tot de in dat kader geformuleerde aanbevelingen kon het Comité vaststellen dat de VSSE tijdig haar Strategisch Plan 2011, de nodige operationele plannen, het personeelsplan en het budget had gefinaliseerd. Daarenboven werden diverse initiatieven gelanceerd die tot doel hadden om de opdrachtgevers en belanghebbenden nauwer bij de werking van de VSSE te betrekken. Wel kon door budgettaire beperkingen het personeelsplan niet volledig worden gerealiseerd. Diverse projecten – zoals bijvoorbeeld het initiatief dat tot doel heeft om de 'klanten' van de analysediensten te bevragen en dat rond het verloop van de evaluatiecyclus in de binnendiensten – hebben hieronder geleden.

Een tweede principe was het '*vertalen van doelstellingen in werkprocessen en het vastleggen van risico's*'. De VSSE heeft diverse werkprocessen opgelijst en een aanvang genomen met de beschrijvingen ervan. Verder werden de risico's die te maken hebben met kritieke bedrijfsprocessen beschreven en maatregelen ter beheersing ervan vastgelegd. Het Comité merkte wel op dat, omwille van een gebrek aan omkadering, het beschrijven van de werkprocessen trager verliep dan gepland. De zogenaamde *Key Performance Indicators*, die meten hoe de werkprocessen verlopen, waren nog niet uitgewerkt.

Het '*inzetten van middelen om de doelen te bereiken en goed beheer van deze middelen*' was het derde principe op basis waarvan het Comité zijn selectie uit de vele aanbevelingen maakte. In dit kader kon vastgesteld worden dat de noodzakelijke functiebeschrijvingen met daaraan gekoppeld de vereiste competenties, waren opgesteld. Tevens werd in vorming geïnvesteerd, weliswaar vooral in het kader van de loopbaanontwikkeling van de medewerkers. Wel oversteeg de wijze waarop de vorming werd aangepakt het loutere reglementaire kader niet. Verder werden een aantal initiatieven ontwikkeld waarbij aandacht werd besteed aan het waardenkader van de VSSE, waaronder het belang van de interne samenwerking. Inzake kennismanagement stond een project in de steigers en werden specifieke *tools* ter beschikking gesteld. Door een tekort aan middelen kon echter nog geen afzonderlijke cel worden gecreëerd die dit kennismanagement effectief moet ondersteunen.

Ten slotte wenste het Comité een zicht te krijgen op de stand van zaken met betrekking tot het '*opvolgen van de externe en interne situatie om de organisatie bij te sturen (feedback-mechanisme)*'. Deze monitoring gebeurt via een aantal instrumenten die door de VSSE zelf werden aangemaakt. De (ICT-)middelen ontbreken echter om deze verder uit te werken. De VSSE had ook de intentie om de realisatie van de visie en strategie van haar directie door middel van een *Balanced Score Card* (BSC) op te volgen. Dit instrument moet evolueren tot een echte managementstool waarmee de diverse processen kunnen opgevolgd worden. In het BSC-project is echter weinig vooruitgang geboekt.

Concluderend kon het Comité vaststellen dat de Veiligheid van de Staat de aanbevelingen zeker ter harte heeft genomen en ze in de praktijk heeft trachten om te zetten. Zo werden voor alle aanbevelingen stappen ter verbetering gezet. Wel was de vooruitgang meestal traag en dit veelal door een gebrek aan middelen. Ten slotte bleek dat voor sommige aanbevelingen de aanpak vrij formalistisch was. Dit had onder meer te maken met het reglementaire kader waarbinnen de VSSE moet functioneren. Het Vast Comité I achtte het wel aangewezen dat de Veiligheid van de Staat zou bepalen welke risico's dreigen ingevolge de vertraagde uitvoering en welke correctieve maatregelen noodzakelijk zijn.

I.1.2. AANPASSING VAN DE INFORMATIEPOSITIE AAN DE NODEN VAN DE BEVOEGDE OVERHEDEN INZAKE ERKENNINGSAANVRAGEN VAN GELOOFS-GEMEENSCHAPPEN

In zijn activiteitenverslag over het werkingsjaar 2009 beval het Comité de VSSE aan te waken over het systematisch actualiseren van de door haar verzamelde data met betrekking tot geloofsgemeenschappen. Dit in het kader van de informatiebehoefte van de minister van Justitie die op zijn beurt de regionale overheden moet adviseren bij erkenningsaanvragen van geloofsgemeenschappen.[3]

Midden 2011 stelde de VSSE een dienstnota op inzake de behandeling van dergelijke erkenningsaanvragen. Hierbij werd tevens aangekondigd dat de agenten die werken rond het islamitisch radicalisme maatregelen hadden genomen om aan de bemerking van het Comité tegemoet te komen.

I.1.3. DUIDELIJKE RICHTLIJNEN INZAKE *HUMINT*

Het Vast Comité I heeft geregeld aanbevelingen geformuleerd in verband met de informantenwerking. Zo had het Comité er zich onder meer over verwonderd dat de richtlijnen inzake *HUMINT* verspreid lagen over diverse directieven, documenten of cursussen. Gelet op het belang van de informantenwerking had de VSSE reeds in 2009 aangekondigd dat het werk zou maken van een globale, interne regeling.[4]

In 2011 werd dit werk gefinaliseerd met '*Instructies over het werken met menselijke bronnen*' en een dienstnota over '*de evaluatie van de informatie aangeleverd door menselijke bronnen*'. Het Comité benadrukt de inhoudelijke waarde van beide documenten die alle aspecten van de informatenwerking omvatten. Deze richtlijnen gaan uit van de administrateur-generaal van de VSSE. Het Comité

3 VAST COMITÉ I, *Activiteitenverslag 2009*, 87.
4 VAST COMITÉ I, *Activiteitenverslag 2009*, 35-36 en 84-85.

wijst er evenwel op dat de verplichting om richtlijnen uit te vaardigen inzake de werking met menselijke bronnen sinds januari 2011 rust op het Ministerieel Comité voor inlichting en veiligheid (art. 18 W.I&V.).

I.1.4. *REQUEST FOR INFORMATION*-SYSTEEM BIJ DE ADIV

Het Comité moest vaststellen dat vijf jaar na de ontdekking van een belangrijke lacune in het informatiebeheersysteem van de ADIV, overwegingen van budgettaire aard en interne weerstanden belet hadden om hieraan te verhelpen. Deze situatie was zeker van aard om de goede uitvoering van de opdrachten van de ADIV in het gedrang te kunnen brengen. Het Vast Comité I beval dan ook nadrukkelijk aan dat de dienst hieraan zou remediëren.[5]

Naar aanleiding van de audit (zie II.1), kon het Comité vaststellen dat de ADIV in september 2011 het zogenaamde *Request for Information*-systeem invoerde. Dit systeem moet een antwoord bieden op de eerder vastgestelde problemen.

I.1.5. ACTIEPLAN VAN DE ADIV NAAR AANLEIDING VAN DE AUDIT

In 2010 opende het Comité een audit over de militaire inlichtingendienst. Deze kon midden 2011 worden afgesloten (zie II.1) met tal van aanbevelingen (zie IX.2.1). De ADIV stelde onmiddellijk een actieplan op om effectief werk te maken van de implementatie van die aanbevelingen. Zo werd onder meer een *task force* opgericht die wekelijks bijeenkomt en werkt rond zes thema's: processen, personeel, vorming, investeringen, veiligheid en diversen. Momenteel loopt de eerste fase van dit actieplan. Die bestaat uit de analyse, inventarisatie en screening van de probleemgebieden.

I.1.6. HET HOREN VAN GEWEZEN LEDEN VAN INLICHTINGENDIENSTEN

Tot in 2010 konden enkel in dienst zijnde leden van de inlichtingendiensten door het Vast Comité I gedagvaard worden voor verhoor. Het Comité kon deze mogelijkheid niet aanwenden in hoofde van voormalige leden van de VSSE of de ADIV. Ingevolge de aanbeveling van het Comité[6] werd die mogelijkheid bij Wet van 9 februari 2011 (*BS* 29 maart 2011) ingeschreven in artikel 48 W.Toezicht.

---

5 VAST COMITÉ I, *Activiteitenverslag 2010*, 41-42 en 105.
6 VAST COMITÉ I, *Activiteitenverslag 2009*, 88.

I.1.7. STRATEGIE IN VERBAND MET INFORMATIEVEILIGHEID

In zijn '*onderzoek naar de houding van de Belgische inlichtingendiensten tegenover de noodzaak om de informatiesystemen te beschermen tegen intercepties en cyberaanvallen uit het buitenland*' (zie II.2) stelde het Comité een grote versnippering vast van het beleid rond de veiligheid van informatiesystemen. Daarom schaarde het zich achter de besluiten van het '*Witboek voor een nationaal beleid voor de informatieveiligheid*'. Het Vast Comité I beval ook aan dat er een federale strategie zou worden uitgewerkt en dat er snel een agentschap zou worden opgericht dat de activiteiten rond informatieveiligheid kan coördineren (zie IX.2.3). Welnu, in het Regeerakkoord van 1 december 2011 werd volgende passage opgenomen: '*De regering zal, met eerbied voor de privacy, een federaal veiligheidsbeleid inzake informatienetwerken en -systemen uitwerken en zo de aanbevelingen van het Comité I volgen*.'

I.1.8. PROCESBESCHRIJVING *SIGINT*

In het kader van zijn specifieke controletaak inzake de interceptie van buitenlandse communicatie door de ADIV (zie Hoofdstuk IV), had het Comité aangedrongen op een uitgewerkte procesbeschrijving.[7] De procesbeschrijvingen werden inmiddels gefinaliseerd. Ze zullen onder meer toelaten de wettelijke verificaties op een meer performante manier te laten verlopen.

I.2. EEN HERNEMING VAN EERDERE AANBEVELINGEN

Artikel 35, 3° W.Toezicht geeft het Vast Comité I de opdracht verslag te doen aan de Kamer van Volksvertegenwoordigers en aan de Senaat '*wanneer het vaststelt dat, bij het verstrijken van een termijn die het redelijk acht, geen gevolg werd gegeven aan zijn besluiten of dat de genomen maatregelen niet passend of ontoereikend zijn*'. Het Vast Comité I maakt van deze mogelijkheid alleen gebruik indien het van oordeel is dat aanbevelingen die essentieel zijn voor de vrijwaring van fundamentele rechten, voor een optimale werking van de inlichtingendiensten en het OCAD of voor een goed functionerend toezicht, zonder aanwijsbare reden onbeantwoord zijn gebleven.

Het Comité vraagt opnieuw bijzondere aandacht voor de wijze waarop (persoons)gegevens door de ADIV of de VSSE worden overgezonden aan buiten-

7 Zie VAST COMITÉ I, *Activiteitenverslag 2009*, 88.

landse zusterdiensten. Het Comité heeft namelijk in het kader van zijn BIM-controle (zie hoofdstuk III) kunnen vaststellen dat de Belgische inlichtingendiensten geregeld worden bevraagd door buitenlandse diensten. De (controle op deze) informatiestroom is echter onvoldoende geregeld.[8]

[8] Zie eerder VAST COMITÉ I, *Activiteitenverslag 2006*, 132; *Activiteitenverslag 2007*, 73; *Activiteitenverslag 2008*, 6 en 109-110; *Activiteitenverslag 2009*, 4 en 106-107 en *Activiteitenverslag 2010*, 3-4. Zie in diezelfde zin ook de aanbevelingen uit: United Nations General Assembly, Human Rights Council, *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including their oversight*, Report of the special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin SCHEININ, 17 May 2010, A/HRC/14/46, in het bijzonder *'31 – 35 Good practices on intelligence sharing and cooperation'*, 26-29.

HOOFDSTUK II.
DE TOEZICHTONDERZOEKEN

In 2011 ontving het Vast Comité I 25 nieuwe klachten of aangiften van particulieren. Na verificatie van een aantal objectieve gegevens, wees het Comité 19 klachten of aangiften af omdat ze kennelijk niet gegrond waren (art. 34 W.Toezicht) of omdat het Comité onbevoegd was voor de opgeworpen vraag. In die laatste gevallen werden de klagers zo mogelijk doorverwezen naar de bevoegde instantie. Ook de twee klachten die eind 2010 nog hangende waren, gaven geen aanleiding tot een onderzoek. Inzake drie nieuwe klachten of aangiften werd een toezichtonderzoek geopend; voor de drie resterende klachten uit 2011 werd nog nagegaan of er voldoende redenen zijn om tot een onderzoek over te gaan.

Naast de drie 'klachtonderzoeken' opende het Vast Comité I in 2011 een ander toezichtonderzoek en dit op initiatief van de Voorzitter van de Senaat.

In 2011 werden tien onderzoeken afgesloten. In wat volgt, worden deze toegelicht (II.1 tot II.10). Daarna volgt een opsomming en een korte situering van de nog lopende onderzoeken (II.11).

II.1. EEN AUDIT BIJ DE MILITAIRE INLICHTINGENDIENST

II.1.1. INLEIDING

De Belgische militaire inlichtingendienst kreeg van de wetgever vier taken toebedeeld:

- een inlichtingenopdracht met betrekking tot elke activiteit die onder meer de onschendbaarheid van het nationaal grondgebied, de militaire defensieplannen, het wetenschappelijk en economisch potentieel, de vervulling van de opdrachten van de strijdkrachten of de veiligheid van de Belgische onderdanen in het buitenland bedreigt of zou kunnen bedreigen;
- de zorg voor het behoud van de militaire veiligheid van het personeel en de militaire installaties;
- een beschermingsopdracht van de geheimen die verbonden zijn met onder andere militaire installaties en inlichtingen;
- en, ten slotte, het uitvoeren van veiligheidsonderzoeken (art. 11 W.I&V).

Uiteraard kunnen deze opdrachten slechts naar behoren worden vervuld indien de ADIV zijn middelen op een efficiënte en effectieve wijze inzet. Om uit te maken of dit zo is, besloot het Vast Comité I, daarin geruggensteund door de Senatoriële Begeleidingscommissie, om een audit uit te voeren.[9]

Het Comité verrichtte niet alleen een 'prestatie-audit'[10] die een zicht moest bieden op de toestand van de betrokken dienst; het wou tevens een dynamiek op gang brengen die, waar nodig, tot reële verandering en verbetering zou leiden. Met het oog op de totstandkoming van deze dynamiek, formuleerde het Comité een omstandig aantal aanbevelingen.[11] Om deze aanbevelingen te kaderen, worden in dit hoofdstuk onder meer de structuur van de geauditeerde dienst en het verloop en de resultaten van de audit kort toegelicht.

II.1.2. DE CENTRALE THEMA'S

Gezien het Comité zich een relatief kort tijdsbestek had vooropgesteld – zes maanden – werd een keuze gemaakt in de te onderzoeken domeinen. Deze keuze gebeurde aan de hand van criteria als toegevoegde waarde[12], materialiteit[13] en risico- en onzekerheidsgraden.[14]

De eerste twee geselecteerde onderzoeksdomeinen betroffen 'de personeelsmiddelen' en 'de informatiehuishouding'. Immers, binnen een inlichtingendienst zijn zowel de inzet van het personeel als het gebruik van de beschikbare informatie, cruciaal. Dit is niet enkel zo op vlak van investeringen[15], maar ook in strategisch opzicht, aangezien inlichtingenwerk staat of valt met de menselijke inzet en met het beschikken over de juiste informatie. Ook het zogenaamde 'organisatiebeheersingsysteem' (dit is de interne controle van de geauditeerde) werd bestudeerd. De basis van interne controle wordt gevormd door het risicobeheer binnen een organisatie; vandaar dat deze materie als derde onderzoeksdomein onder de loep werd genomen.

---

9 'A*udit met het oog op het vaststellen en de verificatie van de voorwaarden noodzakelijk voor een goede inzet van de middelen bij de Algemene Dienst inlichting en veiligheid (ADIV), met onder andere aandacht voor het beheer en de leiding van het personeel, de informatiestromen en het risicobeheer*'.

10 Zie in die zin ook de audit bij de Veiligheid van de Staat: VAST COMITÉ I, *Activiteitenverslag 2009*, 5-23.

11 Zie Hoofdstuk IX. Aanbevelingen (in het bijzonder IX.2.1). De in de audit geformuleerde consideransen werden bovendien door het Comité uitgedrukt in een '*roadmap*' voor een verbeterde inzet van de middelen bij de ADIV.

12 'Hoe minder over een domein bekend is, hoe groter de toegevoegde waarde van een audit naar dat domein'.

13 'Belangrijkheid van het domein in termen van investeringen, strategisch belang, publieke impact…'.

14 'Domeinen waarover weinig geweten is (bijvoorbeeld omdat ze nog nooit geauditeerd werden) of domeinen waarin in het verleden incidenten voorkwamen, vormen in principe risico- of onzekerheidsdomeinen'.

15 Het personeelsbudget vormt het grootste gedeelte van het budget van de ADIV.

II.1.3. FASERING EN METHODOLOGIE

Het Vast Comité I investeerde grondig in dit toezichtonderzoek, zowel naar mensen als naar middelen.

De eigenlijke audit werd evident voorafgegaan door de opmaak van een auditplan en de uitwerking van een gefundeerde methodologische onderbouw overeenkomstig internationaal geldende standaarden.

Er werd gefaseerd tewerk gegaan. De eerste fase betrof de beeldvorming aan de hand van de opgevraagde documentatie en verkennende gesprekken (december 2010).

In een tweede fase werden gegevens verzameld over kwesties die in alle lagen van de organisatie leefden (zoals bijvoorbeeld interne communicatie, vorming, samenwerking) die vervolgens in 'harde', cijfermatige informatie werden omgezet. Ook werd op zoek gegaan naar mogelijke pistes voor verbetering, onder meer door een beroep te doen op de ervaring en de suggesties van de personeelsleden van de dienst. Aan de hand van een schriftelijke vragenlijst kon het personeel zijn mening te kennen geven (januari – februari 2011).[16] In een persoonlijk en vertrouwelijk interview konden de respondenten eventueel bijkomende informatie kwijt. Ook alle (sub)divisies van de ADIV werden bezocht, waarbij zowel de verantwoordelijken als hun medewerkers hun werkzaamheden en werkomstandigheden konden toelichten.

De verzamelde informatie werd in een derde fase teruggekoppeld: aan de hand van gesprekken met verantwoordelijken en domeinexperten werden de geïdentificeerde kwesties afgetoetst en uitgediept. Ook werd getracht suggesties voor verbetering nader uit te werken. Hiertoe werden 'focusgroepen' opgericht, waarbij divisie-overschrijdend werd gewerkt (maart-mei 2011).

Een laatste fase omvatte de rapportering (juni 2011). De audit resulteerde in een lijvig verslag (198 p.) dat als 'GEHEIM' diende te worden geclassificeerd.

II.1.4. STRUCTUUR VAN DE MILITAIRE INLICHTINGENDIENST

De leiding van de ADIV wordt uitgeoefend door het Commando (ADIV/C), dat kan beschikken over een kleine staf en een secretariaat. De ADIV – waar zowel burgers als militairen tewerkgesteld zijn – is ingedeeld in vier divisies die voor het grootste gedeelte vanuit Brussel opereren.

In de Divisie A(*ppui*) zijn alle diensten verzameld die instaan voor de algemene ondersteuning van de ADIV, te weten personeels- en budgettair beheer, ICT, logistieke aspecten die binnen de ADIV worden beheerd…

[16] De bruto-responsratio van deze enquête bedroeg 71,5%; de netto-respons, dit wil zeggen zonder blanco's, lag op 67,3%. Deze resultaten zijn zeker representatief.

De Divisie C(*ounter*)I(*ntelligence*) volgt fenomenen op die de militaire veiligheid kunnen bedreigen en die zich voornamelijk op Belgisch grondgebied situeren. Deze divisie beschikt over een aantal provinciale detachementen die de verzamelde gegevens doorgeven aan de analisten binnen de sectie.

De Divisie I(*ntelligence*) vormt de grootste divisie binnen de ADIV en heeft evenzeer een collecte- en een analysetaak. Ze richt zich op fenomenen die zich in het buitenland voordoen en bedreigingen vormen die binnen de werkingssfeer van de ADIV vallen. De analysediensten van deze divisie zijn grotendeels per geografische regio georganiseerd, terwijl ook bureaus voor *Naval-, Air-* en *Land Intelligence* en transnationale aangelegenheden bestaan. De Afdeling I/Ops is actief in het buitenland, en dit ter ondersteuning van Belgische troepen. Zij verzamelt ter plaatse inlichtingen, zowel ten behoeve van de militairen op het terrein als ten behoeve van de ADIV in het algemeen.

De Divisie S(*ecurity*) heeft twee kerntaken. Enerzijds voert ze de veiligheidsonderzoeken uit ten aanzien van personen of firma's die een veiligheidsmachtiging of -attest aanvragen, noodzakelijk om binnen of voor defensie bepaalde taken of opdrachten te kunnen uitvoeren (S/Habilitations). Ook deze divisie kan een beroep doen op provinciale detachementen. Anderzijds waakt de divisie over de militaire veiligheid (domeinen, personen, ICT-systemen) in die zin dat ze richtlijnen formuleert die door de diverse entiteiten van Landsverdediging moeten worden gevolgd en dat ze in bepaalde gevallen inspecties kan uitvoeren (S/*Security*, MIS[17] en S/*Infosec*).

II.1.5. KRACHTLIJNEN VAN DE AUDIT

In wat volgt worden de resultaten van de audit per geselecteerd domein kort toegelicht.

II.1.5.1. Inzet, beheer en motivatie van het personeel

Inzake het personeelsbeheer[18] en -motivatie staat de ADIV nog voor heel wat uitdagingen.

Dé sterke punten van de dienst zijn ongetwijfeld de boeiende functie-inhoud en de mogelijkheid voor het personeel om, waar nuttig, eigen initiatieven te ontplooien. Dit zijn uiterst belangrijke elementen en vormen de basis voor motivatie en inzet.

Het personeel kan evenwel doeltreffender en doelmatiger worden ingezet. Vooral de wijze waarop de doelstellingen intern worden geformuleerd en naar de

17 *Military and Industrial Security.*

18 De *human ressources*-thema's als werving, beheer van de natuurlijke afvloeiing, loopbaan, verloning…

mensen op het terrein worden vertaald, kan beter. Uit de audit bleek overigens dat de medewerkers hiervoor zelf vragende partij waren.

De audit toonde verder aan dat de personeelsbeheer- en organisatiefunctie (P&O-functie) moest worden versterkt, opdat zou kunnen worden geïnvesteerd in functiebeschrijvingen, previsioneel personeelsbeheer, *coaching*… De organisatie-ontwikkelingscapaciteit, die elke organisatie nodig heeft om continu de eigen werking te onderzoeken, te verbeteren en te veranderen (leercapaciteit), diende eveneens te worden versterkt.

De medewerkers waren eerder matig tevreden over de loopbaanmogelijkheden en de verloning. Dit zijn echter aspecten waarvoor de ADIV niet (alleen) verantwoordelijk is. Voor dergelijke materies is de inlichtingendienst immers afhankelijk van de medewerking van andere entiteiten zoals de Algemene Directie *Human Resources* binnen Defensie. Maar ook daar blijken de middelen eerder schaars. Een actieve samenwerking en overleg tussen alle partners zowel binnen als buiten de ADIV blijft noodzakelijk.

Een ander heikel punt betrof de gelijke behandeling (inzake carrièremogelijkheden, systeem van toelagen…) van de diverse personeelsgroepen binnen de ADIV. Vooral de situatie van de burgers trok de aandacht. Het was niet duidelijk welke hun plaats is binnen de militaire structuren en wat ze van hun loopbaan binnen de ADIV mogen verwachten. Een aantal factoren hebben bewerkstelligd dat het evenwicht tussen burgers en militairen danig werd verstoord. Hoewel (statutaire) ongelijkheden een gegeven vormen dat de ADIV overstijgt, werden deze wel erg geproblematiseerd nu het aantal burgers in het geheel van het personeelsbestand van de ADIV verhoudingsgewijs relatief hoog blijkt. Bovendien speelt het burgerpersoneel in de inlichtingencyclus, en meer bepaald in de analysefase, een centrale rol. Het Vast Comité I meent evenwel dat deze problematiek voorzichtig moet worden benaderd. Immers, elke maatregel die ten voordele van één welbepaalde groep wordt genomen, kan door andere medewerkers terug als onbillijk worden beschouwd.

Uit de audit bleek echter dat ongelijkheden niet één enkele groep troffen, maar zich bij vele groepen voordeden, ongeacht of het burgers dan wel militairen betrof. Gezien het Comité van oordeel is dat de dienst ruimte moet bieden voor de ambities van álle medewerkers, was het de mening toegedaan dat de heersende 'groepslogica' plaats dient te maken voor een 'functionele' logica. Het is aangewezen om niet te denken in termen van 'personeelsgroepen' (militairen *versus* burgers, contractuelen *versus* statutairen, niveau X *versus* niveau Y…) maar eerder in termen van 'functies' (bijvoorbeeld de lijn-[19], analyse- of collectefunctie). Binnen deze functies kan er dan naar worden gestreefd om eenieder – ongeacht statuut of graad – op eenzelfde manier te behandelen.

Het Comité meende dat de analysefunctie, waar personeelsleden met diverse statuten worden tewerkgesteld, prioritaire aandacht verdiende. Dit betekent ech-

[19] Dit is een hiërarchische functie.

ter niet dat andere 'ongelijkheden' – onder andere in de collecte-diensten – daarom minder aandacht zouden verdienen.

Een ander probleem was dat de militaire personeelsleden van de ADIV vanuit andere entiteiten van de Krijgsmacht komen en soms slechts kort bij de ADIV worden ingezet. De relatief grote rotatie stelde problemen voor het onthaal, de opleiding en het kennisbeheer. Het Vast Comité I was de mening toegedaan dat hieraan zou kunnen worden verholpen door de creatie van een 'inlichtingentak' waarbinnen zich de loopbaanontwikkeling en de kennisopbouw kan afspelen. Het aantrekken van medewerkers, het opstellen van coherente functieprofielen, het uitbouwen van competentiebeheer, de organisatie van loopbanen en opleiding zou vanuit en binnen deze tak kunnen worden georganiseerd. Ook het burgerpersoneel zou binnen een dergelijke 'inlichtingentak' een meer duidelijke positie hebben en haar loopbaan beter kunnen uitbouwen.

II.1.5.2. Informatiehuishouding

Wat de informatiehuishouding betreft, kon het Vast Comité I vaststellen dat de personeelsleden van de ADIV met veel 'huisvlijt' maar met beperkte middelen, het steeds stijgende volume aan informatie en documentatie trachten te beheersen. Een *Request for Information*-systeem (RFI-systeem)[20], bedoeld om een antwoord te bieden op vaststellingen van een eerder toezichtonderzoek[21], werd in het najaar van 2011 geïmplementeerd.

Ondanks de verrichte inspanningen, moest het Comité vaststellen dat een geïntegreerd ICT-systeem, waarin de personeelsleden op een makkelijke en snelle manier gegevens kunnen invoeren en terugvinden, op korte termijn niet zal kunnen worden gerealiseerd. De noodzakelijke investeringen blijken steeds te worden uitgesteld. Een aantal vernieuwingen kon wel worden doorgevoerd, weze het vertraagd door de verschuiving van de geplande investeringen (op het ogenblik van de audit reeds tot in 2016). Het Comité diende te constateren dat de inlichtingenwerkzaamheden niet (meer) voldoende werden ondersteund door de ICT. Door het grote volume was bepaalde informatie moeilijk toegankelijk of verwerkbaar, of dreigde ze aan de ADIV voorbij te gaan. In die zin waren de voorwaarden voor een goed beheer van de informatie niet (langer) volledig vervuld.

Het Vast Comité I wees op de evidente risico's die dit met zich brengt. Er bestaat immers geen garantie dat informatie – die achteraf in een dossier cruciaal zou blijken – (tijdig) door de dienst wordt opgevangen, teruggevonden en/of verwerkt. Deze risico's moeten worden ingeperkt door investeringen in ICT.

---

20 Het *Request for Information-systeem* is geënt op een gestandaardiseerd document waarin wordt beschreven welke inlichtingen worden gevraagd.

21 'Toezichtonderzoek inzake de informatiehuishouding bij de militaire inlichtingendienst'. De initiële aanleiding voor de opening van dit toezichtonderzoek was de constatering dat er in een concreet geval een gebrek aan informatiedoorstroming was vastgesteld tussen de Divisies *Intelligence* en *Counter Intelligence*. Zie hierover VAST COMITÉ I, *Activiteitenverslag 2010*, 41-42.

Echter, net zoals dit het geval is voor het personeelsbeheer, hangt de ADIV voor de materiële en budgettaire behoeften af van andere entiteiten van Defensie. Dit deed het Comité besluiten dat de samenwerking tussen de ADIV en deze entiteiten van alle betrokken partijen een nieuwe vorm van openheid vergde, waarbij het vaak 'geheime' karakter van de werkzaamheden van de ADIV de communicatie niet mag belemmeren.

II.1.5.3. Organisatiebeheerssystemen en risicobeheer

Een laatste onderzoeksdomein betrof het organisatiebeheer en het daaraan gekoppelde risicobeheer. Het Vast Comité I wees er op dat bij de ADIV omwille van rotatie en uitstroom van het personeel een aantal risico's[22] inzake discontinuiteit en kennisverlies bestonden. Deze risico's moesten verder in kaart worden gebracht en beheerd. Ook hier blijkt een sterke P&O-functie, goede ICT-hulpmiddelen en een gedegen kennismanagement noodzakelijk om vooruitgang te kunnen boeken. Recent heeft de ADIV een risicobeheersinstrument geïmplementeerd. Het beheersen van risico's kan evenwel pas echt worden aangevat wanneer de doelstellingen van de ADIV goed omschreven zijn (*supra*) en de bedrijfsprocessen op punt zijn gesteld.

II.1.5.4. Andere vaststellingen

Tijdens de audit werden enkele vaststellingen gedaan die buiten de *scope* van het onderzoek vielen.

Zo stonden de fysieke beveiliging van de infrastructuur en de bewakingsmiddelen bij de ADIV niet overal op het niveau dat van een militaire inlichtingendienst mag worden verwacht.

Wat betreft personeelsbehoeften[23] stelde het Comité vast dat sommige analyse- en collectebureaus tot een minimumbezetting terugvielen. Ook dit hield risico's in voor de continuïteit van de dienstverlening.

Ten slotte moest ook worden vastgesteld dat de samenwerking tussen de ADIV en andere onderdelen van Defensie, in het bijzonder de directies *Human* en *Material Resources,* alsook de Interne Audit van Defensie, diende te worden versterkt.

---

22 Onder 'risico's' wordt verstaan de onzekerheid die op de doelstellingen van de organisatie weegt. Risico's zijn alle gebeurtenissen en omstandigheden die de realisatie van deze doelstellingen kunnen beïnvloeden.

23 De audit kon zich hierover verder niet uitspreken. De personeelsbehoeften kunnen enkel worden bepaald nadat de doelstellingen en *Service Levels* van de ADIV in detail zijn vastgelegd.

II.1.6. ALGEMENE EVALUATIE

Op de vraag of de voorwaarden voor een goed beheer wat betreft het personeel vervuld zijn, kon positief worden geantwoord, alhoewel uiteraard verbeteringen en veranderingen mogelijk en nodig zijn.

Wat betreft de toegang en de exploitatie van de aanwezige informatie (de eigenlijke inlichtingenwerkzaamheden), bleek het antwoord daarentegen eerder negatief. Het Vast Comité I kon vaststellen dat het de militaire inlichtingendienst – zeker op ICT-vlak – aan de nodige middelen ontbrak waardoor het risico bestaat dat bepaalde gegevens aan de ADIV voorbijgaan, ofwel niet geëxploiteerd worden.

Het organisatie- en risicobeheer ten slotte is een domein waar de ADIV pas sinds kort aandacht aan besteedt en waar nog veel werk moet worden verricht.

Dat de ADIV vooralsnog in staat bleek gedegen werk af te leveren, heeft veel te maken met de werkijver en beroepsernst van zijn personeelsleden. De inzet van veel medewerkers maakt dat de reële problemen en risico's waarmee de organisatie wordt geconfronteerd, minder zichtbaar zijn.

Het is voorspelbaar dat de precaire situatie waarin de ADIV zich op het ogenblik van de audit bevond, op termijn niet houdbaar zal zijn. Het Comité concludeerde dat ofwel het ambitieniveau moet worden bijgesteld, ofwel dat de middelen (én de organisatie) dienen te worden aangepast. Zoniet moeten de risico's die uit de situatie voortvloeiden, worden aanvaard. Een van die risico's is dat niet langer kan worden voldaan aan het (hoge) verwachtingspatroon bij de opdrachtgevers van de ADIV.

II.2. DE BESCHERMING VAN COMMUNICATIE-SYSTEMEN TEGEN MOGELIJKE BUITENLANDSE INTERCEPTIES EN CYBERAANVALLEN

In een informatiemaatschappij is de beveiliging van communicatiesystemen die beheerd worden via informaticatechnologieën cruciaal. Diverse grootmachten aanzien massale aanvallen op die systemen immers als één van de voornaamste bedreigingen voor de veiligheid, de militaire belangen en de economie van een land, maar ook voor de fundamentele rechten en vrijheden van burgers. De Begeleidingscommissie van de Senaat drukte dan ook de wens uit om door het Vast Comité I geïnformeerd te worden over wijze waarop de inlichtingendiensten deze materie opvolgen.[24]

Achtereenvolgens wordt een overzicht geboden van de federale instellingen die vandaag belast zijn met de beveiliging van de ICT-systemen en wordt de rol van de Veiligheid van de Staat en de ADIV toegelicht. Er wordt afgesloten met een aantal conclusies.

---

[24] De Commissie wenste ook een *update* van het Echelon-rapport dat het Vast Comité I in 2000 presenteerde (VAST COMITÉ I, *Activiteitenverslag 2000*, 27 e.v.).

II.2.1. FEDERALE INSTELLINGEN BELAST MET DE MATERIE

In tegenstelling tot zijn buurlanden[25], beschikt België niet over een orgaan dat specifiek belast is met de bescherming van informatiesystemen. De materie ligt verspreid over meerdere federale overheidsdiensten, die daarenboven niet steeds over voldoende middelen beschikken. Welke zijn nu deze diensten?

Vooreerst ressorteert het (inlichtingen)beleid inzake de bestrijding van de bedreigingen tegen informatiesystemen onder het Ministerieel Comité voor inlichting en veiligheid (MCIV). Het MCIV heeft *in casu* evenwel nog geen concrete richtlijn uitgewerkt.

Ook de FOD Informatie- en Communicatietechnologie (FEDICT) heeft de opdracht een beleid uit te werken en te voeren met het oog op het beveiligen van de informatiesystemen van de federale administraties. FEDICT is onder meer belast met het ontwikkelen van een structuur van *online*-diensten van de regering (*e-government*) en het bevorderen van de informatisering van de samenleving. Het kreeg ook de taak een inventaris op te stellen van de kritieke informaticainfrastructuur.

De Nationale Veiligheidsoverheid (NVO) werd aangewezen als homologatieoverheid voor de systemen en netwerken van de federale overheidsdiensten die nationale of internationale (EU, NAVO) geclassificeerde informatie verwerken, doorgeven of bewaren. De NVO heeft de opdracht te waken over de veiligheid van de informatiesystemen, en dit in drie fasen: de evaluatie, de certificatie en de eigenlijke homologatie. Omwille van een gebrek aan middelen, was de NVO echter niet ten volle in staat om deze taak uit te oefenen.

In 2000 werd BELNET[26] opgericht. Deze dienst werd onder meer belast met de ontwikkeling, invoering en beheer van het communicatienetwerk tussen de federale overheidsdiensten en het internet. Sommige verbindingen van dit zogenaamde FEDMAN-netwerk (*Federal Metropolitan Area Network*) zijn beveiligd. Een onderdeel van FEDMAN – BINII genaamd[27] – is voorbehouden voor de uitwisseling van geclassificeerde informatie. Deze functie wordt beheerd door de ADIV. Ook de oprichting van een *Computer Emergency Response Team* (CERT)[28]

---

25 Zie bijvoorbeeld het *Agence Nationale de la Sécurité des Systèmes d'Information* (Frankrijk), het *Bundesamt für Sicherheit in der Informationstechnik* (Duitsland) of het *Office of Cyber Security* (Verenigd Koninkrijk).

26 BELNET is een staatsdienst met afzonderlijk beheer binnen de FOD Wetenschapsbeleid.

27 Zie ook VAST COMITÉ I, *Activiteitenverslag 2007*, 50.

28 Gewoonlijk wordt een CERT met volgende taken belast:
- de gecentraliseerde signalisatie van incidenten (aanvallen) op de informatienetten en -systemen, en centralisatie van vragen om bijstand als gevolg van die veiligheidsincidenten (ontvangst van de aanvragen, analyse van de symptomen en eventuele correlatie van de incidenten);
- het verwerken van de waarschuwingen en reactie op computeraanvallen: technische analyse, uitwisseling van informatie met andere CERT's, bijdrage tot specifieke technische studies;

op federaal niveau, werd toevertrouwd aan BELNET.[29] Het betreft een waarschuwings- en reactiecentrum waarop overheidsinstanties en bedrijven een beroep kunnen doen wanneer ze het doelwit zijn van een elektronische aanval. De overheidsdienst CERT.be ging in september 2009 van start.[30]

Voordien werd reeds het Federaal Overlegplatform Informatieveiligheid opgericht, beter bekend als het *Belgian Network Information Security* (BELNIS). Naast de VSSE en de ADIV verenigt dit platform vertegenwoordigers van federale overheden zoals de NVO, het Crisiscentrum van de regering, de *Federal Computer Crime Unit*, het College van procureurs-generaal, de Privacycommissie… Het BELNIS-platform formuleerde onder meer voorstellen met betrekking tot de bescherming van kritieke ICT-infrastructuur en de homologatie van de systemen die geclassificeerde gegevens verwerken. In de loop van 2007 realiseerde BELNIS het Witboek *voor een nationaal beleid van de informatieveiligheid*. Hieruit kon worden afgeleid dat in België de problematiek slechts fragmentair wordt aangepakt. Het Witboek formuleerde een aantal voorstellen om de vastgestelde tekortkomingen weg te werken.[31] Onderstaande aanbevelingen waren voor het Vast Comité I essentieel[32]:

- de goedkeuring van een kaderwet die de algemene doelstellingen van ons land inzake informatieveiligheid vaststelt;
- de aanwijzing van de instellingen die met de verwezenlijking van die doelstellingen worden belast;
- de oprichting van een nationale overheid voor de certificatie en homologatie van de gevoelige systemen, die handelt in overleg met de NVO en de ADIV;
- de verbetering en coördinatie van de Belgische vertegenwoordiging in internationale werkgroepen[33];

  - het opmaken en bijhouden van een databank met kwetsbare plekken;
  - preventie door het verspreiden van informatie over de te nemen voorzorgsmaatregelen om het risico van incidenten of, in het slechtste geval, hun gevolgen te beperken;
  - eventuele coördinatie met de andere entiteiten (buiten het actiegebied): competentiecentra netwerken, operators en leveranciers van internettoegang, nationale en internationale CERT's.

29 BELNET deed dit in samenwerking met het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT).

30 Binnen Landsverdediging werd eveneens een CERT opgericht dat de opdracht heeft verdachte activiteiten te analyseren en veiligheidsincidenten te behandelen die voorkomen op de computers van zijn netwerken. Het team heette aanvankelijk *Computer Security Incident Response Capability* (CSIRC); zijn opdracht beperkte zich tot het verwerken van incidenten inzake informatieveiligheid.

31 Het Vast Comité I moest vaststellen dat het Witboek nergens gewag maakte van de rol die de VSSE ter zake kan vervullen.

32 Ondertussen werden een aantal aanbevelingen gerealiseerd: de oprichting van een nationaal CERT (met name CERT.be); de creatie van een systeem voor het inventariseren van kritieke ICT-infrastructuur; de aanwijzing van informatieveiligheidsconsulenten in de federale administraties…

33 Zo blijken het BIPT, de ADIV en een aantal individuele experts – vaak vrijwilligers – België te vertegenwoordigen in tal van internationale werkgroepen, zonder dat er evenwel sprake is van een reële coördinatie met de andere betrokken overheden.

– de opmaak van een inventaris van de – zowel publieke als private – kritieke ICT- infrastructuur in België.

II.2.2. DE VEILIGHEID VAN DE STAAT

II.2.2.1. Bevoegdheden en middelen

Binnen het geheel van beschreven overheidsdiensten (*supra*) speelt de VSSE slechts een beperkte rol. De wetgever gaf de dienst niet de wettelijke opdracht de ICT-netwerken te 'beschermen', noch beschikt de VSSE over de wettelijke en technische capaciteit om elektronische tegenmaatregelen te treffen.

Met de middelen waarover ze beschikt en rekening houdend met de initiatieven van de verschillende betrokken instanties en diensten, beperkt de VSSE zich tot zijn 'inlichtingenopdracht'. Deze bestaat erin informatie te verzamelen over (dreigende) aanvallen en intercepties van communicatie die onder meer uitgaan van *state* en *non-state actors*.

Wat betreft de vastgestelde (al dan niet geslaagde) aanvallen, zijn de enige relevante informatiebronnen de informaticaonderzoeken ('*computer forensics*'). Deze veronderstellen een wettelijke en technische capaciteit om bijvoorbeeld e-mailadressen en de houders van die adressen te identificeren. Tot voor de implementatie van de BIM-Wet beschikte de VSSE niet over die mogelijkheid. Ondertussen kan de dienst, bij wijze van specifieke methode, overgaan tot '*maatregelen tot identificatie van de abonnee of de gewone gebruiker van een dienst van elektronische communicatie of van het gebruikte elektronische communicatiemiddel*', en tot '*maatregelen van opsporing van de oproepgegevens van elektronische communicatiemiddelen en de lokalisatie van de afkomst of de bestemming van elektronische communicatie*.'[34]

II.2.2.2. De informaticasectie van de VSSE

Binnen de VSSE heeft een informaticasectie als taak operationele ICT-ondersteuning te bieden aan de buitendiensten alsook het informatiesysteem van de VSSE te beheren. Maar de opdracht van deze sectie bestaat er ook in de dreigingen tegen ICT-systemen te volgen, documentatie aan te leggen over de vastgestelde tendensen, bewustmakingsacties te voeren, veiligheidsadviezen uit te brengen alsook onderzoeken te voeren in reactie op vastgestelde feiten.[35]

---

34 Artikel 18/2 § 1, 4° en 5° W.I&V.

35 De leden van de sectie nemen ook deel aan de werkzaamheden van de '*Working Group on Electronic Attack*' (WGEA) van de Club van Bern. Deze werkgroep komt samen om informatie uit te wisselen over de tendensen en de vastgestelde feiten inzake cyberaanvallen tegen ICT-systemen en om, in voorkomend geval, gemeenschappelijke acties te kunnen coördineren.

Het Strategisch Plan van de VSSE voorzag in de aanstelling van een ICT-directeur en in de uitbreiding van het kader van deze sectie. De dienst kreeg hiervoor echter niet het fiat van de Stafdienst Personeel en Organisatie van de FOD Justitie en van de Inspecteur van Financiën. Het Vast Comité I oordeelde dat deze situatie erg problematisch was en deed de aanbeveling om alsnog het noodzakelijke gekwalificeerde personeel ter beschikking te stellen.

II.2.2.3. INFOSEC-materieel[36]

Informatie afkomstig van buitenlandse diensten kan slechts worden verwerkt wanneer internationaal geldende veiligheidsnormen worden nageleefd. De VSSE maakt dan ook alleen gebruik van gecertificeerd en gehomologeerd materieel. Door het gebrek aan (technische) middelen bij de NVO (*supra*), is de VSSE echter nog steeds verplicht om gebruik te maken van systemen en procedures die werden gecertificeerd door buitenlandse overheden. Het Vast Comité I vindt dit problematisch.

II.2.2.4. Beoordeling van de dreiging

Gelet op het aantal potentiële doelwitten (de Europese instellingen, de hoofdkwartieren van de NAVO en SHAPE, de Belgische publieke instellingen, de onderzoeksinstituten en *hightech*-bedrijven), meent de VSSE dat de dreiging van cyberaanvallen ernstig moet worden genomen. Cyberaanvallen die de Belgische belangen en veiligheid kunnen bedreigen, gaan uit van buitenlandse mogendheden, zelfstandige individuen en groepen, klassieke cyberpiraten alsook de georganiseerde misdaad. De VSSE vraagt de Belgische overheden dan ook om dringend werk te maken van beschermings- en opsporingsmaatregelen[37], waarbij kan worden gedacht aan bewustmakingscampagnes, preventiemaatregelen en een noodplan in geval van een grootschalige cyberaanval.

II.2.2.5. Bewustmakingsacties en gerichte interventies

De VSSE besteedt veel aandacht aan sensibilisering inzake algemene of concrete dreigingen. Zo waarschuwde de VSSE Belgische overheden dat de vertrouwelijkheid en integriteit van communicatie via een *BlackBerry* gevaar kan lopen. In

---

36 Met INFOSEC wordt de toepassing bedoeld van veiligheidsmaatregelen die tot doel hebben de informatie te beschermen die wordt verwerkt, opgeslagen of doorgestuurd door communicatie- en informatiesystemen of andere elektronische systemen tegen inbreuken op de vertrouwelijkheid, de integriteit of de beschikbaarheid van die informatie (ongeacht of het om accidentele of opzettelijke inbreuken gaat) alsook om inbreuken op de integriteit en de beschikbaarheid van de systemen zelf te voorkomen.

37 In november 2007 deinsde de VSSE er niet voor terug om de toenmalige houding van de overheid ter zake als 'bijna blindheid' te bestempelen.

diezelfde zin lichtte de dienst tal van overheden (bijvoorbeeld de minister van Justitie, het College voor inlichting en veiligheid, het Directiecomité van de FOD Justitie, de FOD Buitenlandse Zaken) in over bedreigingen van cyberaanvallen. Ook heeft de VSSE meegewerkt aan de organisatie van een bewustmakingscampagne voor Europese parlementsleden en werd een briefing georganiseerd voor Belgische parlementsleden en vertegenwoordigers van andere overheden.

De INFOSEC-activiteiten van de VSSE focussen zich vandaag op gerichte interventies bij incidenten waarover de dienst werd ingelicht door de slachtoffers zelf en waarbij die laatste spontaan samenwerkten met de dienst. De informaticadienst van de VSSE participeerde in die zin bijvoorbeeld aan een onderzoek van de veiligheidsofficieren van Buitenlandse Zaken. Het doel daarbij was tweeledig: een digitaal bewijs van een aanval vinden en nagaan of en in welke mate de cyberaanvallen de integriteit van de beoogde informatica-infrastructuur hadden beschadigd.

II.2.3. DE ALGEMENE DIENST INLICHTING EN VEILIGHEID

II.2.3.1. Dreigingen

De ADIV volgt het steeds stijgende aantal aanvallen tegen de informatienetwerken van de federale overheden (zoals Landsverdediging[38]) en verzamelt ook informatie uit open bronnen over cyberaanvallen die in het buitenland werden ontdekt. Die penetraties blijken steeds complexer en moeilijker opspoorbaar zodat de bron en de precieze redenen van die aanvallen vaak moeilijk te identificeren zijn.

Wat betreft de versterking van de Amerikaanse wetgeving met betrekking tot het onderscheppen van communicatie (cf. *Echelon*), kon het Comité vaststellen dat de acties van de Amerikaanse inlichtingendiensten niet voor komen in het Inlichtingenstuurplan. De ADIV rekent immers op de loyaliteit van de partnerdiensten binnen de NAVO aangezien de toepassing van de *Patriot Act* gericht is tegen de vijanden van de Verenigde Staten.[39] Toch erkent de ADIV dat het risico

[38] Eén van de aanvallen betrof het zogenaamde Conficker-virus en zijn varianten. De ADIV kon daarbij geen infecties vaststellen in de geclassificeerde informaticasystemen. Wel werden eind 2008 gevallen van infectie vastgesteld in het niet-geclassificeerd administratief netwerk van Landsverdediging.

[39] In 2000 verklaarde de ADIV aan het Vast Comité I dat de eventuele militaire spionage uitgaande van de aan België geallieerde landen voor hem geen prioritaire opdracht was (zie VAST COMITÉ I, *Activiteitenverslag 2000*, 57). De VSSE verklaarde hieromtrent dat indien de uitvoering van de *Patriot Act* een activiteit zou meebrengen die afbreuk doet aan een van de belangen die zij krachtens de wet moet beschermen, ze niet zou nalaten haar inlichtingen te bezorgen aan de bevoegde instanties.

van interceptie is toegenomen en schrijft daarom voor dat geclassificeerde informatie bij transmissie gecodeerd wordt.

II.2.3.2. De sectie INFOSEC

Binnen de Divisie S(*ecurity*) van de ADIV is de sectie INFOSEC actief op het vlak van elektronische beschermings- en opsporingsmaatregelen. De sectie is met andere woorden zowel actief op vlak van preventie en detectie, en recent ook reactie. (zie II.2.3.4). De afgelopen jaren voerde ze onderzoek naar verschillende incidenten. De ADIV analyseerde de *modi operandi*, evalueerde de geleden schade en informeerde de militaire overheden hieromtrent.

Deze sectie ondervond echter ernstige moeilijkheden om gekwalificeerd personeel te rekruteren en te behouden. Velen stapten over naar de privésector waar de lonen veel aantrekkelijker zijn. Het rekruteringsplan voor 2009 voorzag in bijkomende informatici bij de ADIV. Die werden in dienst genomen in 2010. Het toezichtonderzoek waarschuwde ervoor dat dit mogelijks niet zou volstaan om aan het chronisch personeelstekort te verhelpen.

II.2.3.3. Sensibilisering, ondersteuning en beheer

Op aangeven van de ADIV, trof het Ministerie van Landsverdediging diverse maatregelen om het hoofd te bieden aan informatica-aanvallen. Zo bijvoorbeeld wordt het personeel stelselmatig geïnformeerd over de bedreigingen en de toe te passen beveiligingsregels, werd een intern veiligheidsreglement opgesteld, worden veiligheidsaudits en -controles in de eenheden uitgevoerd en nieuwe technische middelen aangewend (verbeteren van de software, configuratie van het *Intrusion Prevention and Detection System*…).

Verder levert de ADIV ondersteuning aan andere federale diensten. Zo is de dienst onder meer actief binnen het platform BELNIS, wordt er samengewerkt met de VSSE bij de analyse van spionagesoftware, ondersteunt de dienst het CERT.be en sensibiliseert en adviseert hij FOD's bij het implementeren van beveiligde netwerken.

De ADIV beheert ten slotte ook een beveiligde intranetdienst op het FEDMAN-netwerk (zie II.2.1). Dit netwerk werd gecreëerd om geclassificeerde inlichtingen uit te wisselen tussen het OCAD en de inlichtingendiensten en de federale politie enerzijds en om geclassificeerde informatie te kunnen verspreiden vanuit OCAD naar de betrokken FOD's anderzijds. Het netwerk kan ook gebruikt worden voor het uitwisselen van geclassificeerde informatie tussen alle aangesloten federale administraties.

II.2.3.4. Een nieuwe opdracht voor de ADIV

Tot voor kort kon de ADIV geen elektronische tegenmaatregelen treffen in geval van een cyberaanval. Er bestond immers geen wetsbepaling die dat toeliet. In de loop van het toezichtonderzoek bracht de BIM-Wet hierin verandering: '*in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de Minister van Landsverdediging beheerst,* [heeft de ADIV als taak] *de aanval te neutraliseren en er de daders van te identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten*'.[40]

Het Vast Comité I drukte zijn tevredenheid uit over deze nieuwe opdracht. Wel vroeg het zich af waarom er niet werd voorzien in een dergelijke mogelijkheid in geval van aanvallen tegen het informaticasysteem van andere overheidsdiensten of van ICT-systemen die gerekend worden tot de nationale kritieke infrastructuur.

II.2.4. CONCLUSIES

Zowel de VSSE als de ADIV zijn zich bewust van de ernst van de bedreigingen die cyberaanvallen vormen voor de vitale (civiele en militaire) informatiesystemen van het land. De twee inlichtingendiensten hebben bijgevolg initiatieven genomen om hun 'klanten' te sensibiliseren voor de problematiek en wijzen voortdurend op de noodzaak om beschermende maatregelen te nemen.

In de mate waarin de beperkte middelen waarover ze beschikken het toelaten, voeren de diensten ook onderzoek naar specifieke aanvallen tegen de informatiesystemen. Het betreft een voornamelijk defensieve benadering op basis van detectie en evaluatie. Recent werd ook een reactieve benadering mogelijk voor de ADIV.

Ondanks alles moet worden vastgesteld dat het ontbreken van een globaal federaal beleid inzake informatieveiligheid ons land zeer kwetsbaar maakt voor aanvallen tegen zijn vitale informatiesystemen en -netwerken.[41]

Daarbij komt dat het ontbreekt aan één centrale dienst voor de beveiliging van ICT-systemen. Geen van de instellingen die vandaag een bevoegdheid heeft in dit domein, blijkt een volledig beeld te hebben van de problematiek. Gelet op deze grote versnippering, schaarde het Vast Comité I zich achter de besluiten van het *Witboek voor een nationaal beleid voor de informatieveiligheid*. Het Vast Comité I beval ook aan dat er ter zake een federale strategie zou worden uitgewerkt en dat

40 Artikel 11 W.I&V.

41 Het Vast Comité I vestigde al in 1995 de aandacht op het belang van de veiligheid van informatiesystemen en de noodzaak om hieromtrent een globaal veiligheidsbeleid te ontwikkelen (zie VAST COMITÉ I, *Activiteitenverslag 1995*, 114-118).

er snel één agentschap zou worden opgericht met als opdracht de activiteiten rond informatieveiligheid te coördineren.[42] De ervaring en *knowhow* waarover de Belgische inlichtingendiensten beschikken, kan worden aangewend binnen of ten voordele van dat agentschap.

Er kon worden vastgesteld dat de leden van de ADIV en de VSSE – zonder echte coördinatie met andere overheden – België vertegenwoordigen binnen bepaalde internationale werkgroepen. Het is noodzakelijk om duidelijk de rol te definiëren die aan de inlichtingendiensten wordt toegewezen op het vlak van de bescherming van de informatiesystemen. Het Vast Comité I beval aan dat het MCIV daartoe de nodige stappen zou ondernemen.

Ten slotte moet er over worden gewaakt dat de Belgische inlichtingendiensten over de vereiste (technische en personele) middelen kunnen beschikken om hun opdracht in deze materie te kunnen vervullen. Meer bepaald moeten ze de gekwalificeerde personeelsleden kunnen rekruteren en behouden.

II.3. DE INFORMATIEPOSITIE EN DE ACTIES VAN DE INLICHTINGENDIENSTEN MET BETREKKING TOT LORS DOUKAEV

Op 10 september 2010 deed zich een ontploffing voor in een hotel in de Deense hoofdstad Kopenhagen. Daarbij raakte een zekere Lors Doukaev licht gewond. De explosieven die hij bij zich had en die bestemd waren voor een aanslag op de Deense krant Jyllands Posten, gingen voortijdig af.[43]

Doukaev bezat de Belgische nationaliteit en daarom opende het Vast Comité I een onderzoek naar de informatiepositie en de eventuele acties van de Belgische inlichtingendiensten vóór de mislukte aanslag.

II.3.1. DE FEITEN

II.3.1.1. Wie was Lors Doukaev?

Doukaev werd in 1986 in Tsjetsjenië geboren. Op tienjarige leeftijd werd hij het slachtoffer van een granaatontploffing, waarbij zijn rechterbeen gedeeltelijk werd geamputeerd. In 2000 vluchtte hij met zijn moeder en zus naar België. Ze kregen het statuut van politiek vluchteling. Later, in maart 2006, verkreeg Doukaev de

42 Zie ook 'Hoofdstuk I.1.7. Strategie in verband met informatieveiligheid' en 'Hoofdstuk V.3. Voorstel van resolutie inzake de beveiliging van informatie- en communicatiesystemen'.

43 Doukaev werd voor deze feiten midden 2011 veroordeeld door een Deense rechter tot een gevangenisstraf van twaalf jaar.

Belgische nationaliteit. Zoals vereist, werd de VSSE gevraagd of er mogelijke tegenindicaties waren. De betrokkene was toen echter niet bekend bij de dienst.

II.3.1.2. De informatiepositie en de acties van de ADIV

In 2007 werd Doukaev toevallig opgemerkt door een agent van de buitendiensten van de ADIV. Hij had op straat een man met een baard en een geamputeerd been opgemerkt in het gezelschap van een gesluierde vrouw en wilde nagaan of de betrokkene mogelijks deel uitmaakte van een radicale beweging. Verificaties binnen zijn dienst, bij de federale politie en bij de Dienst Vreemdelingenzaken[44] leverden echter niets verdacht op. De inlichtingenagent maakte dan ook geen verslag op voor zijn dienst.[45] Wel hield hij de informatie bij in zijn eigen documentatie.

II.3.1.3. De informatiepositie en de acties van de VSSE

In een 'routinebericht' van een buitenlandse partnerdienst van eind januari 2010 werd aan de VSSE gemeld dat bij een wegcontrole in oktober 2009 deelnemers aan een bijeenkomst van een radicaal islamistische beweging waren geïdentificeerd. Lors Doukaev was een van hen. Tot vóór die datum had hij nooit de aandacht van de VSSE getrokken.

Binnen de VSSE werd het bericht van de partnerdienst zondermeer doorgestuurd naar de betrokken operationele afdelingen en naar de bevoegde analysedienst. Het bericht kreeg om drie redenen een 'routinebehandeling': tussen de vaststellingen (oktober 2009) en de doorzending van het bericht (januari 2010) was heel wat tijd verstreken, de partnerdienst had geen specifieke vraag gesteld en Doukaev kwam niet voor in de databank van de VSSE.

Een van de operationele afdelingen consulteerde daarop de elementen waarover de Dienst Vreemdelingenzaken beschikte en stuurde het bericht van de partnerdienst samen met de resultaten van zijn onderzoek door naar de bevoegde provinciepost. Het bericht en de onderzoeksresultaten werden 'ter informatie' verzonden; er werden geen specifieke vragen geformuleerd.

Nog dezelfde dag wees de postoverste de zaak 'voor onderzoek' toe aan de inlichtingenagent die belast is met de opvolging van het Tsjetsjeense milieu. Belangrijk was dus dat de initiële status van het bericht werd gewijzigd. De agent van de VSSE nam contact op met de politie-inspecteur van de wijk waar Doukaev verbleef en vernam dat betrokkene enkel bekend stond voor oude feiten van slagen en verwondingen en dat hij enkele maanden geleden vertrokken was, zonder

44 De VSSE werd dus niet geraadpleegd.

45 Er werd uiteraard ook geen informatie bezorgd aan andere diensten, zoals de VSSE of het OCAD.

verdere gegevens. Hij contacteerde ook zijn informanten, evenwel zonder resultaat. Wel nam hij geen contact op met de ADIV of met de federale politie.

De agent van de VSSE oordeelde het niet nuttig een verslag op te stellen of andere diensten in kennis te stellen. Hij vond dat hij hiervoor over te weinig elementen beschikte. De VSSE oordeelde naderhand dat dit allerminst professioneel was en nam maatregelen om herhaling te voorkomen (zie verder). Ook het Comité besloot dat het dossier een grotere aandacht verdiende gelet op het bericht van de partnerdienst, op Doukaev's 'verdwijning' en op zijn afkomst. Anderzijds benadrukte het Comité dat het initiële bericht vanuit de centrale diensten van de VSSE slechts 'ter informatie' was doorgestuurd.

II.3.1.4. Politionele informatie

In mei 2010 vroeg de politie van een buurland aan de federale gerechtelijk politie van Luik informatie over een zekere 'Lors'. De Luikse politie antwoordde dat het Lors Doukaev betrof, dat hij bekend stond om feiten van slagen en verwondingen maar ook dat tegen hem een bevel tot aanhouding was uitgevaardigd als gevolg van een correctionele veroordeling van februari 2010. Tot besluit vermeldde de politie dat Lors Doukaev '*destijds niet 'terro' gekend was en dat ze nooit over hem had horen spreken binnen de moslimgemeenschap in Luik'* (vrije vertaling).

Verder beschikte de federale politie ook over informatie die afkomstig was van een bron. Samengevat kwam het er op neer dat een fundamentalistische, islamistische organisatie Lors Doukaev zou hebben gerekruteerd. Hij zou zijn baard hebben laten groeien en zou op zoek geweest zijn naar wapens en explosieven. Het Vast Comité I kon evenwel niet uitmaken of die informatie dateerde van voor of na de mislukte aanslag.

II.3.2. CONCLUSIES

Het Comité benadrukte dat het voor veiligheidsdiensten moeilijk is om een zogenaamde '*lonesome wolf*' te identificeren, vooral indien het radicaliseringsproces snel verloopt zoals dat mogelijks het geval was bij Doukaev. Of de betrokkene al dan niet aan dit profiel beantwoordt, zal evenwel pas blijken na confrontatie met de informatie waarover de federale politie beschikte.

Los daarvan kwam het Comité tot de bevinding dat beide inlichtingendiensten los van elkaar beschikten over gedeeltelijke informatie met betrekking tot Doukaev.

Wat betreft de ADIV, stelde zich de vraag naar de relevantie van de informatie van de agent en naar het belang daarvan voor welke databank ook. Het opnemen van informatie in een bestand, louter op basis van elementen zoals kledij en fysieke eigenschappen, lijkt overdreven en zelfs strijdig met de privacywetgeving.

Wat betreft de VSSE, stelde het Comité vast dat informatie van een bevriende dienst niet werd benut. Het onderzoek van de provinciepost werd '*a minima*' gevoerd en werd niet gevolgd door een passend verslag. De VSSE trok evenwel lessen uit deze tekortkoming en nam structurele maatregelen om dergelijke fouten in de toekomst te vermijden.

Het Comité moest verder vaststellen dat er geen informatie werd uitgewisseld tussen de inlichtingendiensten onderling, noch tussen de inlichtingendiensten en de politiediensten. Het Comité wees in dit verband specifiek op de politionele informatie die voorhanden was. Het verzocht het Vast Comité P dan ook om een onderzoek te openen naar de inlichtingen waarover de politiediensten beschikten vóór Doukaev's arrestatie in Kopenhagen. Het verslag van het Vast Comité I zal desgevallend worden aangevuld en bijgewerkt op basis van de vaststellingen van dat toezichtonderzoek.

Het Comité benadrukte dat, mocht de partiële informatie gedeeld zijn geweest, het duidelijk was geworden dat de inlichtingen- en politiediensten bijzondere aandacht hadden moeten besteden aan betrokkene. Uiteraard mag hier niet uit worden afgeleid dat hierdoor de poging tot aanslag met zekerheid had kunnen voorkomen worden.

In het algemeen wees het Comité op het belang van het rechtstreeks uitwisselen van concrete informatie tussen de inlichtingendiensten en de politiediensten. Het benadrukte dat de informatie-uitwisseling niet beperkt mag blijven tot het uitwisselen van (algemene of specifieke) analyses op bijvoorbeeld het niveau van het OCAD. Immers, het gebrek aan een rechtstreekse doorstroming van gegevens kan ertoe leiden dat de diensten kansen ontlopen om personen te traceren die de samenleving en de burgers in gevaar kunnen brengen.

II.4. DE INFORMATIESTROMEN TUSSEN HET OCAD EN ZIJN ONDERSTEUNENDE DIENSTEN

De kerntaak van het OCAD bestaat erin op eigen initiatief of op verzoek van bepaalde overheden punctuele of strategische evaluaties te maken over dreigingen inzake terrorisme en extremisme.[46] Deze taak berust bij (extern gerekruteerde) analisten en bij (vanuit de zogenaamde 'ondersteunende diensten' gedetacheerde) experten. Deze ondersteunende diensten vormen voor het OCAD de belangrijkste informatiebronnen. Het zijn de VSSE, de ADIV, de geïntegreerde politie (zowel de federale politie als de lokale korpsen), de Administratie der Douane en Accijnzen van de FOD Financiën, de Dienst Vreemdelingenzaken van de FOD Binnen-

[46] Deze opdracht staat omschreven in de Wet van 10 juli 2006 houdende analyse van de dreiging (W.OCAD) en in het K.B. van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging (KB.OCAD).

landse Zaken, de FOD Mobiliteit en Vervoer en de FOD Buitenlandse Zaken.[47] Elk van die diensten moet in principe over een centraal contactpunt beschikken waarlangs de uitwisseling van informatie, inlichtingen en analyses van en naar het OCAD dient te verlopen.

Met dit gemeenschappelijk toezichtonderzoek wensten de Vaste Comités P en I een *status quaestionis* op te maken van de informatiestromen tussen het OCAD en de ondersteunende diensten en dit aan de hand van een uitgebreide bevraging. Daarenboven werd de informatie-uitwisseling in een concrete *testcase* bestudeerd. Het betrof de dreigingsanalyse naar aanleiding van een mogelijke ontsnappingspoging tijdens het terrorismeproces rond Malika El Aroud.[48] Hieronder worden de algemene bevindingen van beide facetten van het onderzoek kort toegelicht.

II.4.1. DE INFORMATIESTROMEN KWANTITATIEF BENADERD

De Comités wensten een globaal zicht te krijgen op het aantal onderling uitgewisselde inlichtingen, berichten en analyses. Dit was zo goed als onmogelijk omdat elke actor een eigen telwijze bleek te hanteren en omdat bepaalde centrale contactpunten niet op de hoogte waren van alle uitgewisselde inlichtingen en documenten. Dit laatste was onder meer het gevolg van het feit dat het OCAD vaak rechtstreeks communiceerde met bepaalde sleutelfiguren binnen de ondersteunende diensten. De Comités vonden dit op zich niet problematisch, mits die contacten echter 'traceerbaar' zijn en het centrale contactpunt er een zicht op heeft.

Andere frappante vaststelling bij dit luik van het onderzoek was dat de cijfers die het OCAD aan de Comités meedeelde, verschilden van deze die het nadien elders bekend maakte.

---

47 De wet laat toe het aantal ondersteunende diensten uit te breiden. Volgens het OCAD is hier momenteel geen nood aan. Dit betekent evenwel niet dat er geen contacten worden onderhouden met andere diensten. Zo zijn er bijvoorbeeld het Crisiscentrum van de regering (op vlak van dreigingsevaluaties bij bezoeken), het Directoraat-generaal preventie en veiligheid van de FOD Binnenlandse Zaken (op het vlak van de ondersteuning van sociale initiatieven met als aandachtspunt de radicalisering), het Federaal parket, de Cel voor Financiële Informatieverwerking (inzake verdachte transacties), de FOD Justitie (op het vlak van internationale samenwerking), de Dienst Strafrechtelijk Beleid en het Commissariaat-generaal voor de Vluchtelingen en de Staatlozen. Het OCAD beschouwt deze diensten als 'partners'. Ze vielen buiten de *scope* van dit toezichtonderzoek.

48 Deze *testcase* bleek achteraf niet representatief voor de vaststellingen uit het algemene deel van het onderzoek en dit om verschillende redenen: het betrof een lopend strafonderzoek onder embargoprocedure; de informatie werd aangeleverd op basis van een zeer gerichte vraag; de dreigingsevaluatie gebeurde voornamelijk op basis van elementen uit een ander strafrechtelijk dossier; de korte periode tussen de vraag om een evaluatie en de start van het proces; slechts een beperkt aantal ondersteunende diensten speelden een rol in deze dreigingsanalyse.

Niettegenstaande deze vaststellingen werd duidelijk dat de informatiestroom van en naar de VSSE, de ADIV, de politie en de FOD Buitenlandse Zaken substantieel[49] was én een stijgende tendens vertoonde. Hetzelfde gold echter niet voor de Administratie der Douane en Accijnzen, de Dienst Vreemdelingenzaken en de FOD Mobiliteit: de informatie die vanuit die diensten het OCAD bereikte, was op jaarbasis beperkt tot enkele (tientallen) berichten.

II.4.2. DE CENTRALE CONTACTPUNTEN

Elke ondersteunende dienst moet binnen haar schoot een centraal contactpunt organiseren waarlangs de informatie-uitwisseling met het OCAD verloopt (art. 11 KB.OCAD).

De contactpunten van de VSSE, de ADIV en de FOD Buitenlandse Zaken (met name de terrorismecoördinator), werden door het OCAD als zeer positief omschreven.

Bij de Administratie der Douane en Accijnzen[50], de Dienst Vreemdelingenzaken[51] en de FOD Mobiliteit[52] ontbrak echter een duidelijk aanwijsbaar en als dusdanig erkend contactpunt. Alhoewel deze lacune gedeeltelijk werd opgevangen door de gedetacheerde experts, waren de Comités van oordeel dat hieraan op korte termijn moet geremedieerd worden.

Ook over het 'contactpunt politie' was het OCAD niet onverdeeld positief. Zo is er nooit overgegaan tot het aanduiden van een centraal contactpunt voor de geïntegreerde politie als dusdanig. Er bestaat wel een contactpunt voor de federale politie: het Nationaal Invalspunt (NIP). Maar dit functioneert blijkbaar louter als doorgeefluik voor enerzijds de DGA (DAO)[53] wat betreft bestuurlijke informatie en anderzijds de DJP/TERRO[54] voor de gerechtelijke informatie.[55] Verder is er de beperkte betrokkenheid van de lokale politie. Gelet op de organisatie van de

---

49 Zie evenwel de bevindingen naar aanleiding van het toezichtonderzoek naar 'Een gepland werkbezoek in het buitenland door het OCAD' (Hoofdstuk II.5).

50 Het voor de Administratie der Douane en Accijnzen aangeduide contactpunt stelde tijdens de eerste bevraging dat hij niet op de hoogte was van zijn aanstelling.

51 De Dienst Vreemdelingenzaken had het Bureau Opsporingen binnen de Directie Inspectie aangeduid als centraal contactpunt. Het OCAD was echter in de overtuiging dat het contactpunt de administrateur-generaal van de dienst was.

52 Het contactpunt van de FOD Mobiliteit was totaal niet zichtbaar in de structuur van de organisatie. Ook het feit dat deze FOD is opgebouwd uit drie onafhankelijke pijlers (vervoer te land, over het water en in de lucht) bemoeilijkt het werk van dit contactpunt. Zijn bijdrage is dan ook zeer beperkt. Ook het OCAD erkent dit en richt zich doorgaans rechtstreeks tot bepaalde personen binnen de organisatie.

53 De directie operaties en informatiebeheer van het directoraat-generaal bestuurlijke politie van de federale politie.

54 De directie van de bestrijding van de criminaliteit tegen personen – Terrorisme.

55 Het OCAD pleitte er voor dat de DGA het hoofdkanaal zou worden. De Comités betwijfelen de haalbaarheid van deze piste gelet op de vertrouwelijkheid van sommige gerechtelijke informatie, waarvan moeilijk kan aangenomen worden dat de gerechtelijke overheden ermee zouden

informatiestromen binnen de geïntegreerde politie, zou in theorie alle relevante informatie moeten terechtkomen bij het DJP/TERRO en via die weg bij het OCAD. De directie van het OCAD betwijfelde echter of dit effectief gebeurt en wenste een grotere betrokkenheid van de lokale politie ter zake.[56]

II.4.3. DE NOTIES 'INLICHTINGEN' EN 'RELEVANT'

Ingevolge artikel 6 W.OCAD zijn de ondersteunende diensten verplicht alle 'inlichtingen' waarover zij in het kader van hun wettelijke opdrachten beschikken en die 'relevant' zijn voor de werking van het OCAD aan dit orgaan mee te delen. Met betrekking tot deze verplichting deden de Comités twee vaststellingen.

Enerzijds interpreteren de twee inlichtingendiensten in tegenstelling tot de politie deze regel in die zin dat zij in principe geen ruwe doch alleen verwerkte informatie doorzenden (zie ook II.4.10 en II.4.11).

Anderzijds bleek niet voor alle ondersteunende diensten steeds even duidelijk wanneer informatie 'relevant' is of niet. Deze vaststelling gold bijvoorbeeld voor de FOD Buitenlandse Zaken die hieraan trachtte te verhelpen via regelmatig overleg met het OCAD. Maar ook voor de geïntegreerde politie bleken er zich in het verleden enkele problemen te hebben voorgedaan, vooral dan met betrekking tot het luik 'extremisme'. Om dit probleem op te lossen, werd een werkgroep opgericht met leden van het OCAD, de federale gerechtelijke en bestuurlijke politie en de Vaste Commissie voor de Lokale Politie.

II.4.4. ONTVANGSTMELDINGEN EN DE OPVOLGING VAN DE ANTWOORDTERMIJNEN

Artikel 11 §§ 2 en 3 KB.OCAD schrijft voor dat iedere informatieaanvraag het voorwerp moet uitmaken van een automatische bevestiging of ontvangstbevestiging die de reglementaire antwoordtermijnen doet lopen. Die regeling blijkt in de praktijk echter niet te worden toegepast: het OCAD noch de ondersteunende diensten werken met een uitgebouwd opvolgsysteem. Er wordt van uitgegaan dat wie niet antwoordt op een verzoek, niet over relevante informatie beschikt.[57]

Verder bleek niet steeds duidelijk of berichten vanuit het OACD 'ter info' of 'voor actie' werden verzonden.

---

instemmen dat die zomaar via de informatiekanalen van bestuurlijke politie behandeld zou worden.

56 Gezien de structuur van de geïntegreerde politie heeft de federale politie geen zeggenschap over de lokale politie. Het OCAD verdedigde dan ook het feit dat het rechtstreekse banden moet onderhouden met de belangrijkste korpsen van de lokale politie. De Comités kunnen deze werkwijze onderschrijven mits het contactpunt voor de geïntegreerde politie een totaalbeeld behoudt van de informatiestroom van een naar de politie.

57 Ook in de *testcase* werd deze werkwijze gevolgd.

II.4.5. DE TWEE EMBARGOPROCEDURES

Om de ongecontroleerde verspreiding van bepaalde gevoelige informatie tegen te gaan heeft de W.OCAD twee zogenaamde 'embargoprocedures' ingevoerd: één ten aanzien van gerechtelijke inlichtingen afkomstig van de politiediensten (art. 11 W.OCAD) en één ten aanzien van inlichtingen van de VSSE, de ADIV, de Administratie der Douane en Accijnzen en de FOD Buitenlandse Zaken (art. 12 W.OCAD). Beide procedures moeten het mogelijk maken dat dergelijke inlichtingen *as such* niet in analyses worden opgenomen of dat niet alle overheden de analyses ontvangen waarin melding wordt gemaakt van die informatie.

In beide gevallen deelt de aanleverende dienst de inlichtingen in principe uitsluitend mee aan de directeur van het OCAD. In de praktijk interpreteert de directie van het OCAD deze regeling echter zo dat niet alleen de directeur persoonlijk, maar ook de personeelsleden die werken rond de betrokken materie, kennis krijgen van de gevoelige gegevens.[58]

De laatste jaren werd er geen gebruik meer gemaakt van de embargoprocedure *ex* artikel 12 W.OCAD. Embargodossiers onder artikel 11 W.OCAD waren er wel. Hun toepassing leverde geen problemen op.

Naast de artikelen 11 en 12 W.OCAD staat ook een embargoprocedure omschreven in de artikelen 44/1 en volgende van de Wet op het Politieambt. De Comités merkten evenwel op dat de term 'embargo' vaak gebruikt wordt zonder dat het duidelijk is naar welke procedure wordt verwezen. Dergelijke begripsverwarring zou moeten vermeden worden.

II.4.6. DE REGEL VAN DE DERDE DIENST OF DE REGEL VAN HET DERDE LAND

Het OCAD was van oordeel dat de 'regel van de derde dienst' in de (internationale) praktijk evolueert naar een 'regel van het derde land'. Dit blijkt uit het feit dat informatie vanuit het buitenland wordt doorgestuurd met de vermelding '*for Belgian eyes only*'. Dit deed het OCAD vermoeden dat het oorspronkelijke wantrouwen ten aanzien van het Coördinatieorgaan op dit vlak stilaan aan het verdwijnen zou zijn.

Ook voor de VSSE en de ADIV stelde de regel van de derde dienst in de praktijk geen problemen. Doordat het OCAD beter bekend raakt in het buitenland, blijken de meeste landen nu inderdaad informatie over te zenden '*for Belgian eyes only*', waarbij het gebruik niet meer beperkt is tot een bepaalde dienst.

---

58 Zie hierover ook VAST COMITÉ I, *Activiteitenverslag 2008*, 112-113.

II.4.7. EEN BEVEILIGD COMMUNICATIE- EN INFORMATIEPLATFORM

De meeste ondersteunende diensten benadrukten dat het bestaande communicatie- en informatiesysteem zeer duur en weinig performant is. Verder bleken heel wat noodzakelijke aansluitingen nog niet gebeurd te zijn. Hiermee werd niet alleen verwezen naar sommige ondersteunende diensten (zoals bijvoorbeeld de FOD Mobiliteit) maar ook naar andere bestemmelingen van de analyses van het OCAD zoals de leden van Ministerieel Comité voor inlichting en veiligheid en de verschillende 'partners'. Ten slotte voorzagen niet alle ondersteunende diensten in een permanente monitoring van het systeem en werden bepaalde documenten via andere kanalen (bijvoorbeeld per fax of per drager) verzonden.

II.4.8. OMGAAN MET GECLASSIFICEERDE INFORMATIE

Alhoewel alle ondersteunende diensten over een veiligheidsofficier beschikten, kon niet elke dienst garanderen dat alle bepalingen van de classificatiewetgeving gerespecteerd worden. In die diensten valt een veiligheidsincident met geclassificeerde informatie dan ook niet uit te sluiten.

Wat het gebruik van geclassificeerde informatie betreft, stelden zich slechts uitzonderlijk problemen: indien nodig, wordt informatie (gedeeltelijk) gedeclassificeerd en kan ze verspreid worden binnen de ondersteunende dienst. Indien de informatie niet mag gedeclassificeerd worden, ligt dit uiteraard anders. In dit kader merkte de politie op dat het soms moeilijk is om met dergelijke gegevens optimaal te werken, daar geen enkel ICT-systeem binnen de politie (zoals bijvoorbeeld de Algemene Nationale Gegevensbank) voldoet aan de reglementaire normen ter zake en men dus aangewezen is op een papieren verspreiding.

II.4.9. ENKELE SPECIFIEKE BEDENKINGEN DOOR EN OVER HET OCAD

Algemeen stelde de directie van het OCAD dat zijn werking op kruissnelheid is gekomen. Bij de informatie-uitwisseling deden zich geen noemenswaardige problemen meer voor en het OCAD was ervan overtuigd dat het alle relevante informatie aangeleverd krijgt[59] en dat deze informatiestroom blijft groeien. Het Coördinatieorgaan ervoer dan ook een verbeterde werkrelatie met de ondersteunende diensten. Daar waar sommige diensten het OCAD in de beginjaren eerder zagen als een concurrent, zouden zij zich vandaag bewust zijn van zijn meerwaarde en

[59] Ook met betrekking tot de *testcase* was het OCAD van oordeel dat het destijds alle relevante informatie ontvangen had.

dit dankzij de analyses die een meer globaal beeld verschaffen van bepaalde dreigingen.

Het kader van het OCAD was ten tijde van het onderzoek *quasi* volledig ingevuld[60]: tien van de twaalf analisten en negen van de elf experten waren operationeel. Wat betreft de experten, blijken alle ondersteunende diensten het principe te hebben aanvaard dat zij een medewerker moeten detacheren. Wel kennen zij hieraan geen echte prioriteit toe: wanneer een nieuwe expert moet afgevaardigd worden, kan dat vrij lang duren. Zo ontbrak er geruime tijd een expert van de VSSE en van de FOD Buitenlandse Zaken. Het OCAD bleek wel zeer tevreden over het niveau van de ter beschikking gestelde mensen, niettegenstaande het voor sommige diensten moeilijk is om een persoon aan te duiden die vertrouwd is met alle aspecten van zijn administratie. Dit is bijvoorbeeld het geval met de FOD Mobiliteit die opgebouwd is uit drie totaal verschillende entiteiten[61] en met de Administratie der Douane en Accijnzen die bestaat uit veertien apart functionerende divisies. Wat de politie betreft, blijkt het dan weer moeilijk om 'de geïntegreerde politie' te vertegenwoordigen omdat die niet enkel de federale politie omvat, maar ook elke lokale politiezone.

Ten slotte waren de Vaste Comités P en I van oordeel dat de toekomstobjectieven die het OCAD voor zichzelf formuleerde zeer algemeen en weinig meetbaar bleken terwijl niet duidelijk was of deze doelstellingen overeenstemden met de verwachtingen van de diverse betrokken overheden.

II.4.10. ENKELE SPECIFIEKE BEDENKINGEN DOOR EN OVER DE VSSE

Over het algemeen omschreef de VSSE de relatie met het OCAD als positief.

De informatiestroom van en naar de VSSE[62] vertoont niet alleen een stijging in absolute cijfers; ook de inhoud zou merkelijk verbeterd zijn. Wel catalogeert de VSSE de kwaliteit van de inlichtingen als zeer variabel. De dienst is daarenboven vragende partij voor een verfijning van het niveau van de dreigingsanalyse en voor een betere bronvermelding. Zo is bijvoorbeeld niet steeds duidelijk vanwaar bepaalde informatie afkomstig is. Dit kan ertoe leiden dat de VSSE in een analyse van het OCAD een bevestiging leest van haar eigen bevindingen, terwijl het werk van het OCAD uitsluitend gebaseerd is op informatie van de VSSE zelf. Of soms is de informatie waarop het OCAD zich baseert, louter afkomstig van open bronnen, terwijl dit niet expliciet wordt vermeld.

---

60 Ondanks die bezetting kan het OCAD nog geen permanentie organiseren. Buiten de diensturen is er enkel een systeem van terugroepbaarheid voorzien.

61 Vervoer te land, ter zee en via de lucht.

62 De VSSE maakt enkel analyses en inlichtingen over aan het OCAD. Alleen bij imminent gevaar wordt ook de ruwe informatie aangeleverd.

Een ander heikel punt vormen de contacten die het OCAD op basis van artikel 8, 3° W.OCAD onderhoudt met homologe buitenlandse diensten. Wanneer die diensten zelf deel uitmaken van een operationele inlichtingendienst[63], wordt dit door de VSSE als problematisch ervaren. Ze beschouwt zusterdiensten immers als haar natuurlijke correspondenten en vreest dat de contacten van het OCAD zich in die gevallen niet beperken tot de afdeling die belast is met dreigingsanalyses.

II.4.11. ENKELE SPECIFIEKE BEDENKINGEN DOOR EN OVER DE ADIV

Het OCAD en de ADIV omschrijven hun onderlinge verhouding als positief. Er zouden zich nog geen ernstige problemen hebben voorgedaan.

Net zoals de VSSE gaat de ADIV er van uit dat het OCAD vooral nood heeft aan gecontextualiseerde gegevens, waardoor er dus hoofdzakelijk afgewerkte producten (analyses) doorgestuurd worden. Uitzonderlijk (bij imminent gevaar) maakt de ADIV ruwe informatie over. Deze werkwijze werd in akkoord met het OCAD uitgewerkt en is in voege sinds 2007.

De ADIV maakte reeds een aantal maal gebruik van de mogelijkheid om aan het OCAD een analyse te vragen over een bepaalde dreiging. Een van de redenen hiervoor was dat de ADIV zelf met een tekort aan analysecapaciteit kampte als gevolg van het feit dat een aantal van haar analisten een functie hadden verkregen binnen het OCAD.

Een gevoelig punt voor de ADIV blijft de rol die het OCAD speelt met betrekking tot analyses over bedreigingen inzake de Belgische belangen in het buitenland. Vooral de Divisie I van de ADIV is er niet van overtuigd dat het OCAD bevoegd is om analyses te maken over dreigingen in het buitenland. Daarenboven stelt deze divisie zich heel wat vragen bij de kwaliteit van de opgestelde analyses.

De ADIV is vragende partij voor meer globale en prospectieve dreigingsanalyses. Nu zouden de evaluaties te veel focussen op het aspect 'openbare orde'.

Anders dan de VSSE was de ADIV van oordeel dat het OCAD in zijn analyses wel voldoende aan bronvermelding deed.

II.4.12. ALGEMEEN BESLUIT

De twee Comités konden vaststellen dat de informatiestromen zowel kwantitatief als kwalitatief een stijgende tendens vertoonden. Wel hadden een aantal onder-

63 Zie voor dergelijke voorbeelden: VAST COMITÉ I (ed.), *Fusion Centres Throughout Europe. All-source Threat Assessments in the Fight Against Terrorism*, Antwerpen, Intersentia, 2009, 220 p.

steunende diensten nog een ernstige inhaalbeweging uit te voeren om op niveau te functioneren.

Algemeen zijn de ondersteunende diensten positief over de werking van het OCAD[64] en wordt dit Coördinatieorgaan als een meerwaarde ervaren. Toch waren de Comités van oordeel dat er nog mogelijkheden ter verbetering zijn en dit door een antwoord te bieden op de specifieke noden van bepaalde ondersteunende diensten.

II.5. EEN GEPLAND WERKBEZOEK IN HET BUITENLAND DOOR HET OCAD

Begin 2009 plande het Coördinatieorgaan voor de dreigingsanalyse (OCAD) een korte missie naar de Democratische Republiek Congo (DRC). Deze werd echter in allerlaatste instantie afgeblazen.

Met deze missie wou het OCAD onder meer een beter zicht krijgen op de veiligheidssituatie in de DRC en op de eventuele aanwezigheid van radicale, extremistische of terroristische groeperingen. Er werden ontmoetingen met heel wat publieke en private instanties en personen in het vooruitzicht gesteld.

Een van de achterliggende redenen voor de dienstreis was volgens het OCAD dat de FOD Buitenlandse Zaken reeds geruime tijd in gebreke bleef om inlichtingen over Centraal-Afrika door te geven en dit ondanks de verplichting daartoe én spijts concrete initiatieven vanwege het OCAD. Wanneer zich onverwachts de gelegenheid aandient om naar de DRC af te reizen en zo ter plaatste zijn kennis over de regio te vergroten, greep het OCAD die kans: er was plaats aan boord van een militaire vlucht die binnen de week zou vertrekken. De voorbereidingstijd van de missie was derhalve zeer kort.

De directie van het OCAD duidde in haar midden een analist en een expert aan om deze zending uit te voeren en nam contact op met de FOD Buitenlandse Zaken en met het ministerie en het kabinet van Defensie.[65]

Alhoewel deze betrokkenen aanvankelijk hun medewerking verleenden, meldde het kabinet van de minister van Buitenlandse Zaken plots dat de zending op dat ogenblik niet kon plaatsvinden, wegens te delicaat. Toch was de directeur van het OCAD van oordeel dat de ware reden elders lag: een ondersteunende dienst zou niet opgezet zijn geweest met het initiatief waarbij het OCAD zelfstandig wenste te opereren.

Ook al werd de buitenlandse missie afgelast, toch openden de Vaste Comités P en I een gemeenschappelijk toezichtonderzoek. Ze wensten na te gaan of het

64 Bij alle respondenten noteerden de Comités een heel positief tot een eerder gematigd positief verhaal met betrekking tot de evolutie van de informatiestromen. Dit neemt uiteraard niet weg dat soms melding werd gemaakt van bepaalde losstaande incidenten.

65 Het OCAD zou ook het hoofd van de ADIV over deze zending hebben ingelicht.

ondernemen van dergelijke missies in het algemeen kadert in of voortvloeit uit het takenpakket door of krachtens de wet aan het OCAD toevertrouwd. Specifiek wat de afgelaste zending betrof, was er vanuit doeltreffendheidsoogpunt ook de vraag of het OCAD alle nodige voorbereidingen en voorzorgsmaatregelen had getroffen. In de marge van dit onderzoek kwam ten slotte nog een derde aspect aan bod. Het wordt hieronder als eerste toegelicht.

II.5.1. GEBREK AAN INFORMATIE INZAKE CENTRAAL-AFRIKA

De dienstreis werd georganiseerd – aldus het OCAD – omdat het Coördinatieorgaan sedert 2008 verstoken was gebleven van inlichtingen vanwege de FOD Buitenlandse Zaken. Vanaf midden 2009 leverde deze ondersteunende dienst wel aanzienlijk meer inlichtingen aan, maar niet met betrekking tot de toestand in Centraal-Afrika, en dit ondanks gerichte vragen. Het OCAD wenste met de dienstreis dan ook zijn kennis van de regio te vergroten teneinde accurate analyses te kunnen aanleveren. Volgens de directeur heeft het feit dat de missie niet kon uitgevoerd worden, toen verhinderd dat het OCAD zijn informatiepositie met betrekking tot de DRC verbeterde.

De Comités moesten echter vaststellen dat de missie louter *getriggerd* was door een opportuniteit (met name de nakende militaire zending naar de DRC). Het beweerde onontbeerlijke karakter van de voorgenomen missie kwam in het licht hiervan dan ook weinig overtuigend over.

Los daarvan oordeelden de Comités evenwel dat de houding van de FOD Buitenlandse Zaken onduldbaar was. De minister van Buitenlandse Zaken is naar aanleiding van dit toezichtonderzoek overigens tussengekomen teneinde aan de situatie te verhelpen. In overleg met het OCAD werd beslist om regelmatige informatievergaderingen over Centraal-Afrika te houden. Tevens ging de minister over tot de verplichte detachering van een expert van de FOD Buitenlandse Zaken naar het OCAD.

Verder bekritiseerden de Comités dat zij eerder toevallig en op indirecte wijze kennis hadden gekregen van de malaise tussen het OCAD en een van zijn ondersteunende diensten. Nochtans beweerde het OCAD dat zijn werking omtrent Centraal-Afrika gedurende meer dan een jaar gehypothekeerd was door de gebrekkige instroom van informatie over die regio vanwege de FOD Buitenlandse Zaken. Niettegenstaande dit op een structurele disfunctie kon wijzen, werden de Comités – die nu net als taak hebben desgevallend aanbevelingen te formuleren om de efficiëntie te verhogen – niet spontaan ingelicht.

II.5.2. VOORBEREIDING VAN DE DIENSTREIS

De Vaste Comités P en I merkten ook op dat de planning van de missie eerder mager oogde. De voorbereiding bestond uit een beperkte correspondentie en een algemene situering van de desiderata. Er was geen inhoudelijk uitgewerkt programma, geen veiligheidsbriefing, en de ministers van Justitie en Binnenlandse Zaken werden niet voorafgaandelijk in kennis gesteld.

De Comités oordeelden dat het delicate karakter van officiële bezoeken in de Centraal-Afrikaanse regio maximale diplomatie en voorzichtigheid gebiedt, zeker voor een orgaan als het OCAD.

Bij de voorbereiding van deze missie was dus ruimte voor verbetering, zowel op inhoudelijk, communicatief als organisatorisch vlak. Naast een gedetailleerde planning, had ook aandacht moeten worden besteed aan gepaste en specifieke voorzorgsmaatregelen. Verder was overleg met de inlichtingendiensten aangewezen. Ten slotte dienden de politiek verantwoordelijke voogdijministers vooraf te worden ingelicht.

II.5.3. DE VERSCHILLENDE ASPECTEN VAN DE MISSIE EN HET WETTELIJK EN REGLEMENTAIR KADER

Het OCAD is belast met het opstellen van punctuele en strategische evaluaties omtrent potentiële extremistische en terroristische dreigingen tegen de veiligheid van de Staat maar ook tegen '*Belgische belangen en de veiligheid van de Belgische onderdanen in het buitenland*' (artt. 3 en 8, 1° en 2° W.OCAD). Daarnaast heeft het OCAD als opdracht '*met gelijkaardige buitenlandse of internationale diensten specifieke internationale contacten te verzekeren overeenkomstig de richtlijnen van het Ministerieel Comité'* (artikel 8, 3° W.OCAD).

Andere opdrachten heeft het OCAD in de Wet van 10 juli 2006 houdende analyse van de dreiging niet meegekregen. Een dienstreis kan dan ook nooit gezien worden als een opdracht doch slechts als een mogelijke meerwaarde voor de realisatie van de taken opgesomd in artikel 8 W.OCAD.

Past het voorgenomen werkbezoek binnen dit wettelijk en reglementair kader? De missie had een drieledige finaliteit. Elk aspect wordt hieronder apart behandeld.

II.5.3.1. Een studiereis

Eén gedeelte van de zending kon zeker beschouwd worden als studiereis. Voor zover dergelijke reizen ertoe strekken de experten en analisten toe te laten op binnen- en buitenlandse fora hun professionele relaties uit te bouwen en hun expertise verder te ontwikkelen, moet de betrachting van de directeur van het OCAD

om dit maximaal te stimuleren, toegejuicht worden. Dit kan de kwaliteit van de analyses slechts ten goede komen.

II.5.3.2. Specifieke contacten met homologe diensten

Het geplande werkbezoek omvatte ook een ontmoeting met de Congolese afgevaardigde van het *Centre Africain d'Etude et de Recherche sur Ie Terrorisme* (CAERT). Gelet op de missie van het CAERT, beschouwt het OCAD dit centrum als een buitenlandse homologe dienst in de zin van artikel 8, 3° W.OCAD.

Alhoewel de in dit artikel omschreven opdracht nog steeds nadere invulling behoeft vanwege het Ministerieel Comité voor inlichting en veiligheid, heeft het OCAD terecht niet gewacht met het opnemen van deze taak. Wel zou dergelijke richtlijn snel moeten worden uitgevaardigd. Dit moet toelaten een beter zicht te krijgen op de noties 'specifieke contacten' en 'gelijkaardige diensten'. De Comités wezen er in dit verband op dat de wetgever met deze opdracht alleszins geen eigen informatiegaring op het terrein door het OCAD, boven en naast de ondersteunende diensten, heeft gewenst (zie ook II.5.3.3): '*Indien zou blijken dat [het OCAD] via deze contacten kennis zou krijgen van informatie of van gegevens, is voorzien dat het die meedeelt aan de bevoegde Belgische diensten of autoriteiten, teneinde deze informatie of gegevens krachtens hun wettelijke opdrachten te behandelen.*'[66]

II.5.3.3. Inlichtingen verzamelen op het terrein

De Comités moesten vaststellen dat de zending vooral tot doel had om een beter zicht te krijgen op en meer inlichtingen te bekomen over de juiste toestand in de DRC. Beide Comités benadrukten echter dat het OCAD bevoegd noch verantwoordelijk is om gebeurlijke lacunes in de aangeleverde inlichtingen zelf *in situ* te gaan aanvullen.[67] De wetgever heeft dit duidelijk zo gewild. De parlementaire werkzaamheden bij de Wet van 10 juli 2006 laten hierover geen twijfel bestaan: het OCAD '*is geen nieuwe inlichtingen- of politiedienst, het verzamelt geen eerstelijnsinformatie, maar evalueert de dreiging op basis van de inlichtingen die geproduceerd of aangeleverd worden door de deelnemende diensten.*'[68] Dit maakt dat het OCAD in het Belgische veiligheidslandschap een bijzondere positie bekleedt. Zijn evaluaties zijn in wezen het verwerkte product van de door de ondersteunende diensten aangeleverde inlichtingen en informaties. Die producten moeten zelf als 'inlichtingen' worden beschouwd. Toch maakt dit van het OCAD nog geen inlichtingendienst. Het Coördinatieorgaan dient er dan ook zorgvuldig over te waken dat er geen foutieve perceptie ontstaat over zijn opdracht en statuut om zo span-

66 *Parl. St.* Kamer, 2005-06, nr. 51 2032/001, 20.

67 Overigens beschikt het OCAD ook niet over de nodige *knowhow* of middelen om zich op het terrein te begeven.

68 *Parl. St.* Kamer, 2005-06, nr. 51 2032/001, 4. Zie in dezelfde zin *Parl. St.* Senaat, 2005-06, 3-1611/3, 3 en 12.

ningen met de inlichtingendiensten of diplomatieke incidenten te vermijden. Indien het OCAD van oordeel is dat bepaalde ondersteunende diensten hun verplichtingen niet volledig nakomen, is het aangewezen dat het zich wendt tot bijvoorbeeld de Vaste Comités P en I.

II.6. DE VEILIGHEID VAN DE STAAT, DE STRIJD TEGEN DE PROLIFERATIE EN DE BESCHERMING VAN HET WEP

II.6.1. OPVOLGINGSONDERZOEK AAN DE HAND VAN EEN CONCRETE *CASUS*

Het Vast Comité I deed reeds meermaals onderzoek naar de problematiek van de strijd tegen proliferatie[69] en naar de bescherming van het wetenschappelijk en economisch potentieel (WEP)[70] door de inlichtingendiensten. De VSSE[71] heeft in beide materies een belangrijke rol te spelen. De inlichtingen die de dienst doorgeeft aan diverse overheidsdiensten en de wijze waarop deze de gegevens vervolgens gebruiken, kunnen voor de betrokken bedrijven soms verstrekkende (nadelige) gevolgen hebben. Daarenboven lopen de belangen die enerzijds gelden in de strijd tegen de proliferatie en anderzijds bij de bescherming van het WEP, niet steeds samen.

Bij eerdere toezichtonderzoeken kwam aan het licht dat de aanpak van deze materie door de VSSE soms met een zekere nonchalance gepaard ging. Zo werden bijvoorbeeld de bevoegde overheden en de voogdijminister niet (steeds) correct geïnformeerd. Om die reden wenste het Comité onder meer een nauwere samenwerking tussen de inlichtingendiensten en de andere betrokken overheden.

Met onderhavig onderzoek wou het Vast Comité I aan de hand van een concrete *casus* nagaan hoe de VSSE de afgelopen jaren (2006-2011) tewerk was gegaan bij de opvolging van een Belgisch bedrijf, gespecialiseerd in de vervaardiging van hoogtechnologisch materiaal. Tevens werd nagegaan of de VSSE rekening had gehouden met de vorige aanbevelingen in het kader van de strijd tegen proliferatie en de bescherming van het WEP. Het toezichtonderzoek liet alvast niet toe te besluiten dat er op betekenisvolle wijze werd geremedieerd aan de lacunes die voorheen werden vastgesteld.

---

69 Zie bijvoorbeeld VAST COMITÉ I, *Activiteitenverslag 2005*, 8-27 en *Activiteitenverslag 2008*, 42-57.

70 Zie bijvoorbeeld VAST COMITÉ I, *Activiteitenverslag 2005*, 67 en 98-145 en *Activiteitenverslag 2008*, 60-66.

71 Recent breidde de BIM-Wet ook de inlichtingenopdracht van de ADIV uit tot *'het wetenschappelijk en economisch potentieel met betrekking tot de actoren, zowel de natuurlijke als de rechtspersonen, die actief zijn in de economische en industriële sectoren die verbonden zijn met defensie'* (art. 11 W.I&V).

II.6.2. ONDERZOEKSVASTSTELLINGEN

II.6.2.1. Benadering van de thematiek door de VSSE

II.6.2.1.1. Reactief *versus* proactief optreden inzake proliferatie

De VSSE meent dat haar rol op vlak van proliferatie beperkt[72] is gezien de regionalisering van de bevoegdheid om vergunningen voor wapenuitvoer toe te kennen. Voor de VSSE zijn het de diensten die instaan voor het verlenen van de licenties, die de eerste verificaties moeten verrichten en zelf moeten uitmaken welke vergunningsaanvragen aan de VSSE worden voorgelegd. Daarenboven is de VSSE van mening dat zij niet bevoegd is om adviezen te verlenen aan overheden, doch slechts inlichtingen. Het Comité deelde deze mening niet.

Het Comité kon wel vaststellen dat recent – met name in haar *Actieplan 2011* – de VSSE onder meer de (tussen-)handel in grondstoffen, *tools* en technologieën die kunnen bijdragen tot de proliferatie van massavernietigingswapens, een 'actieve prioritaire opvolging' toekende. Voor de studie van sommige 'risicolanden', voor de gerichte bewustmaking van de wetenschappelijke, industriële en academische wereld en voor het opstellen van een profiel van potentiële doelwitten voorzag de VSSE in een 'actieve opvolging'.

Het Comité benadrukte evenwel dat de VSSE[73] nog steeds niet beschikt over de materiële en personele middelen die moeten toelaten het hoofd te bieden aan de toename en de dringendheid van het werk in de strijd tegen proliferatie.

Bijkomend was de VSSE van oordeel dat een akkoord met de Administratie der Douane en Accijnzen absoluut noodzakelijk is om tot een globale strategische analyse van de proliferatie in België te kunnen komen. In een dergelijk akkoord moeten duidelijke en praktische procedures vastgelegd worden voor de informatie-uitwisseling tussen beide administraties.[74]

II.6.2.1.2. Economische *versus* veiligheidsbelangen

De VSSE is zich terdege bewust van het feit dat de strijd *tegen* proliferatie en dus *voor* de veiligheid ook een keerzijde heeft: er zijn eveneens economische belangen

---

72 De VSSE is zeker niet bevoegd om gevoelige exportverrichtingen *materialiter* te controleren en te verhinderen, zoals sommige buitenlandse diensten dit soms aan de VSSE vragen. Deze bevoegdheid komt alleen toe aan de Administratie der Douane en Accijnzen.

73 Wat betreft de ADIV betreurde het Vast Comité I reeds in zijn *Activiteitenverslag 2008* (p. 51) dat er binnen de dienst slechts één analist was toegewezen aan de sectie '*proliferatie van massavernietigingswapens en hun dragers*'. Deze situatie bleek in geen geval in gunstige zin te zijn geëvolueerd.

74 Een vergadering die in februari 2010 in die zin plaatsvond en tot doel had de 'Werkgroep Proliferatie' (met vertegenwoordigers van beide instanties) nieuw leven in te blazen, miste haar doel. De Douanediensten zouden niet meer geneigd zijn om een protocol af te sluiten met de VSSE nu ze een akkoord hebben gesloten met de Gewesten.

mee gemoeid, bijvoorbeeld in die zin dat de concurrentiepositie van een bedrijf niet uit het oog mag worden verloren.[75] In dit kader wees de VSSE op de risico's die de regionalisering van de toekenning van uitvoerlicenties met zich heeft gebracht: de verschillende bevoegde overheden hanteren uiteenlopende criteria bij de beoordeling van de aanvragen. Daarbij hebben de gewestelijke administraties soms de neiging om voorrang te geven aan commerciële belangen, terwijl het CANVEK de nadruk legt op het veiligheidsbelang.

Het standpunt van de VSSE ter zake is alvast duidelijk: veiligheid moet in dergelijke dossiers steeds voorrang krijgen, ook al is het economisch belang van een onderneming meer concreet en meer direct. Het Vast Comité I deelde deze zienswijze.

Wel merkte het Comité op dat er reeds geruime tijd een voorstel circuleerde om beide, tegengestelde belangen beter te verzoenen: binnen de CANVEK zou een procedure van '*voorafgaand advies*' kunnen ingevoerd worden. Hierdoor zou de commerciële schade die een onderneming kan oplopen als gevolg van negatieve adviezen die pas na lange tijd worden uitgebracht (en soms nadat de materialen reeds vervaardigd zijn), beperkt kunnen worden. Deze piste werd onderzocht maar de discussie werd (nog) niet afgerond.

II.6.2.1.3. Strijd tegen proliferatie *versus* bescherming van het WEP tegen inmenging

Het Comité heeft kunnen vaststellen dat de VSSE oog had voor mogelijke pogingen tot 'inmenging in beslissingsprocessen' door vreemde mogendheden in het kader van de strijd tegen proliferatie. Dergelijke inmenging kan een bedreiging vormen voor het WEP.

Om deze dreiging behoorlijk te kunnen inschatten, is een goede informatiepositie uitermate belangrijk. Nochtans blijkt de VSSE (nog steeds) te veel afhankelijk van de (geclassificeerde) informatie die ze van buitenlandse diensten ontvangt, zelfs met betrekking tot verdachte transacties die in België plaatsvinden.

Een ander belangrijk element in dit verband is de noodzakelijke 'koppeling' tussen beide materies. Eerder werd door het Comité voorgesteld om de analisten en operationele agenten die actief zijn op de beide domeinen, samen te brengen. Ze zouden een gemeenschappelijke methodologie moeten vastleggen met de bedoeling om namens de VSSE een eenduidig standpunt in te kunnen nemen ten aanzien van de bevoegde politieke instanties. Bij gebrek aan voldoende middelen bleef dit voorstel zonder gevolg.

---

[75] De VSSE stelde bijvoorbeeld vast dat de versterkte controlemaatregelen en de internationale sancties tegen een bepaald proliferatieland geleid hebben tot een afname van het aantal (gevoelige) exportverrichtingen van de onderneming die als *casus* diende van het toezichtonderzoek.

II.6.2.1.4. Samenwerking binnen de CANVEK

Er bestaat nog steeds geen interne richtlijn over het mandaat van de vertegenwoordiger van de VSSE bij de CANVEK. Bijgevolg wordt de inhoud van de informatie die aan deze commissie wordt bezorgd en de wijze van communicatie ervan (schriftelijk of mondeling), overgelaten aan de vrije beoordeling van de betrokkene.

Daarenboven ontbreekt er een samenwerkingsprotocol waarin de voorwaarden worden vastgelegd voor de communicatie en bescherming van geclassificeerde informatie die aan deze commissie wordt bezorgd.

II.6.2.2. De opvolging van de betrokken firma

Het Comité kon vaststellen dat de VSSE een aantal transacties van de firma met één of meer zogenaamde 'proliferatielanden' tot midden 2008 aandachtig had opgevolgd.

Pas na een onderbreking van bijna twee jaar, wekte het bedrijf opnieuw de belangstelling. Dit omdat buitenlandse inlichtingendiensten de VSSE op de hoogte brachten van nieuwe plannen voor transacties met 'gevoelige landen'. Tijdens de intense bilaterale samenwerking die daarop volgde, werd druk uitgeoefend op de VSSE om gebruik te maken van alle middelen om zich te verzetten tegen de uitvoer van bepaald materieel. De transacties werden evenwel alleen opgevolgd in functie van de informatie die de buitenlandse inlichtingendiensten spontaan hadden verstrekt. Daarvan werden de ministers en de betrokken federale[76] en gewestelijke diensten door de VSSE op volledige en regelmatige wijze in kennis gesteld. Dit werd soms wel bemoeilijkt door de toepassing van de 'regel van de derde dienst'.

Het Comité moest vaststellen dat de opvolging van de betrokken onderneming voornamelijk 'reactief' en *ad hoc* was. Wellicht was het gebrek aan middelen hiervoor de voornaamste reden.

Het duurde tot eind 2010 voor de VSSE eindelijk op meer algemene wijze aandacht toonde voor de onderneming zelf, haar productie en haar klanten en daarmee een eerste 'proactieve' zoektocht naar inlichtingen aanvatte.

---

[76] '*En vue d'améliorer l'efficacité de notre travail (…), nous avons renforcé les échanges d'informations avec les Administrations belges compétentes dans le domaine de la contre-prolifération, et avons informé de façon systématique le ministre de la Justice quant aux faits pertinents dont nous avions connaissance*', aldus de AG van de VSSE. Ook bracht de VSSE-vertegenwoordiger bij de CANVEK meermaals transacties van het bedrijf met sommige 'gevoelige' landen ter sprake. Informatie over verdachte bestellingen werd aan de commissie bezorgd.

II.7. KLACHT VAN EEN LID VAN DE VSSE EN ZIJN ECHTGENOTE

Midden 2010 ontving het Vast Comité I een klacht van een lid van de VSSE en van zijn echtgenote. De klacht omvatte vier verschillende aspecten.

De klager had eerder een 'schriftelijke verwittiging' gekregen omdat hij aan een derde zijn hoedanigheid van lid van de VSSE zou hebben onthuld. Hij aanvaardde niet dat deze nota in zijn personeelsdossier werd bewaard.

Een ander aspect betrof het feit dat de dienst Veiligheidsonderzoeken van de VSSE op de hoogte bleek van verklaringen die de klager zou hebben afgelegd tijdens een vertrouwelijk gesprek met een psycholoog van de VSSE.

Tijdens datzelfde veiligheidsonderzoek zouden tevens oude feiten, waarvan zijn echtgenote het slachtoffer was geweest, op een lasterlijke en eerrovende manier in twijfel zijn getrokken.

Ten slotte beweerde de klager dat er een klimaat van antisemitisme zou heersen binnen de afdeling waar hij werkzaam was. Symptomatisch hiervoor waren – volgens de klager – en krantenknipsel en een *flyer* die waren opgehangen in een dienstlokaal van de VSSE.

Het Comité onderzocht elk aspect van de klacht[77] maar waakte er tevens over niet buiten zijn wettelijk mandaat te treden. Bepaalde onderdelen van de klacht behoorden immers niet tot zijn bevoegdheid. Zo bestempelden de klagers de woorden van de onderzoekers van de VSSE als 'lasterlijk en eerrovend'. Dit is een strafrechtelijke kwalificatie waarover alleen een rechtbank kan oordelen. Het Vast Comité I is echter steeds bevoegd om de materialiteit van feiten vast te stellen en die te beoordelen in het licht van zijn eigen bevoegdheden. Hetzelfde gold voor de schriftelijke verwittiging in zijn personeelsdossier: hoewel het Comité geen beroepsorgaan in tuchtzaken is, mag het onderzoeken of de VSSE geen afbreuk doet aan de rechten die de Grondwet en de wet verlenen aan haar personeelsleden en of een bepaalde praktijk een impact kan hebben op de efficiëntie van de dienst. Vanuit diezelfde twee invalshoeken kan het Comité ook het verloop van veiligheidsonderzoeken analyseren, zonder zich daarbij in de plaats te stellen van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen.

II.7.1. DE 'SCHRIFTELIJKE VERWITTIGING' IN HET PERSONEELSDOSSIER

Ondanks het feit dat de klager betwiste dat hij zijn hoedanigheid van lid van de VSSE aan een derde kenbaar zou hebben gemaakt zonder dat daarvoor een pro-

[77] Overeenkomstig artikel 3, derde lid van de Classificatiewet van 11 december 1998 werd het onderzoek wel tijdelijk opgeschort ingevolge het beroep dat het betrokken personeelslid aantekende tegen de intrekking van zijn veiligheidsmachtiging.

fessionele reden was en ondanks de stopzetting van de tuchtprocedure, besliste de VSSE hem een 'schriftelijke verwittiging' te geven. Deze werd opgenomen in het persoonlijke dossier van de klager.

Het Comité was van mening dat dergelijke werkwijze in de huidige stand van de regelgeving niet toelaatbaar was. Deze mogelijkheid is immers niet voorzien in het personeelsstatuut van 13 december 2006. Het zonder enige beperking in de tijd bewaren van nota's met ongunstige elementen, kan overigens ernstige schade toebrengen aan de verdere carrière van personen.

II.7.2. HET BEROEPSGEHEIM EN HET VEILIGHEIDS-ONDERZOEK

In het bijzijn van zijn dienstoverste legt de klager bepaalde verklaringen af tegenover een psycholoog van de VSSE.[78] Later worden die gegevens – die betrekking hadden op een ernstig functioneringsprobleem binnen zijn dienst – in een veiligheidsonderzoek in hoofde van de klager gebruikt. De dienstoverste had er immers zijn hiërarchie van in kennis gesteld. Het Comité benadrukte dat de psycholoog weliswaar gebonden is door het beroepsgeheim[79], maar dat dit niet geldt voor het betrokken diensthoofd. Hij mocht dan ook de verklaringen doorgeven aan zijn hiërarchie en op die manier het algemeen belang van zijn dienst boven het specifieke belang van zijn medewerker plaatsen.

II.7.3. HET INTERVIEW NAAR AANLEIDING VAN HET VEILIGHEIDSONDERZOEK

Om de betrouwbaarheid van de klager na te gaan, gingen de veiligheidsonderzoekers dieper in op de oude feiten van agressie ten aanzien van zijn echtgenote. Wanneer de klager hierbij de indruk kreeg dat de onderzoekers deze feiten minimaliseerden, weigerde hij zijn verdere medewerking aan het interview.

Het Vast Comité I benadrukte dat het voornaamste doel van het veiligheidsonderzoek erin bestond de echtheid van de verklaringen van de klager te toetsen. Hierbij moesten de onderzoekers noodgedwongen verifiëren of en waarvoor de

---

78 Deze psycholoog maakte deel uit van het psychologisch en sociaal begeleidingsteam van de VSSE. Rekening houdend met de impact van de verantwoordelijkheden en de psychologische en sociale lasten die de ambtenaren van de VSSE op zich nemen, heeft het K.B. van 13 december 2006 een dergelijk team opgericht.

79 Artikel 143 van het K.B. van 13 december 2006 luidt als volgt: '*Het begeleidingsteam komt tussen ofwel op vraag van het personeelslid zelf, ofwel op vraag van de hiërarchische chef of een collega en in dat geval, met akkoord van het betrokken personeelslid. De leden van het begeleidingsteam zijn gebonden door het beroepsgeheim. Zij werken buiten elk personeelsdossier om en garanderen de anonimiteit. Behalve mits schriftelijke toestemming van het betrokken personeelslid, delen zij in geen geval de inhoud van hun gesprekken mee aan de hiërarchie.*'

vrouw destijds klacht had neergelegd. Wel hadden zij daarbij niet dieper hoeven in te gaan op de strafrechtelijke kwalificatie die het slachtoffer zelf meende te moeten geven van de feiten.

II.7.4. DE GEWRAAKTE DOCUMENTEN

In een dienstlokaal waren een krantenknipsel en een *flyer* opgehangen die een standpunt weergaven in het Israëlisch-Palestijns conflict. Dit gebeurde buiten het medeweten van het diensthoofd.

Het Comité was van oordeel dat de documenten niet indicatief waren voor het beweerde antisemitische klimaat. Wel meende het Comité dat ze niet thuishoorden in een lokaal van de VSSE, dit gelet op de plicht tot discretie en neutraliteit die de ambtenaren van deze dienst in acht moeten nemen.

In principe genieten ambtenaren van de buitendiensten van de VSSE de vrijheid van meningsuiting. Ze moeten er zich echter in alle omstandigheden van onthouden in het openbaar uiting te geven aan hun politieke overtuigingen en zich in het openbaar in te laten met politieke activiteiten.[80] De betrokken ambtenaren worden regelmatig herinnerd aan deze principes. Ze werden opgenomen in een ontwerp van administratief vademecum/deontologische code dat op het ogenblik van het afsluiten van dit toezichtonderzoek nog in voorbereiding was.

II.8. DE BELGISCHE VERTEGENWOORDIGING BIJ INTERNATIONALE VERGADERINGEN INZAKE TERRORISME

De Vaste Comités P en I stelden vast dat de Belgische politie- en inlichtingendiensten en het OCAD geregeld samen deelnamen aan internationale vergaderingen inzake de strijd tegen het terrorisme. De vraag rees dan ook of er tussen die diensten enige coördinatie plaatsvond en of, met andere woorden, de eisen van doeltreffendheid en efficiëntie werden nageleefd. Uiteraard werden het OCAD, de federale politie, de VSSE en de ADIV, als voornaamste actoren in de strijd tegen het terrorisme en het extremisme, bij het onderzoek betrokken. Maar ook de andere ondersteunende diensten van het OCAD werden bevraagd: de korpsen van de lokale politie, de Administratie der Douane en Accijnzen van de FOD Financiën, de Dienst Vreemdelingenzaken van de FOD Binnenlandse Zaken, de FOD Mobiliteit en Vervoer en de FOD Buitenlandse Zaken.[81] Ook het federaal

80 Artikel 12 K.B. van 13 december 2006.

81 Sommige diensten en ministers antwoordden pas na verschillende herinneringsbrieven. De Comités bleven zelfs zonder antwoord vanwege de ministers van Financiën en van Binnenlandse Zaken.

parket en het Crisiscentrum van de regering zijn regelmatig vertegenwoordigd op internationale meetings. Zij waren echter niet het voorwerp van onderzoek aangezien de Comités geen controlebevoegdheid hebben ten aanzien van deze instanties.

Het onderzoek peilde naar het onderwerp van internationale (strategische of operationele) vergaderingen, bijeenkomsten of werkgroepen in het kader van de strijd tegen terrorisme en extremisme en naar wie daaraan langs Belgische zijde deelnam. Tevens werd onderzocht of er tussen de Belgische actoren voorafgaand overleg plaatsvond omtrent de agenda en de standpunten die namens België zouden of moesten ingenomen worden. Verder werd de wijze bestudeerd waarop de resultaten, verslagen, afspraken of standpunten van de vergadering werden verspreid tussen deelnemende en/of niet-deelnemende diensten. Ten slotte kregen de betrokken actoren de gelegenheid hun visie omtrent de samenstelling van de delegatie aan welbepaalde fora uiteen te zetten.

Het onderzoek bevestigde dat de Belgische politie- en inlichtingendiensten en het OCAD, maar ook de FOD Buitenlandse Zaken, deelnemen aan vele internationale vergaderingen inzake de strijd tegen het terrorisme en/of het extremisme. Uit de informatie kwam ook een enigszins caleidoscopisch beeld naar voor van wie waar aanwezig is. Binnen eenzelfde forum of vergadering zijn soms verschillende diensten tegelijk vertegenwoordigd.[82] Ook is niet steeds duidelijk of de aanwezige dienst(en) België dan wel zichzelf vertegenwoordigt of vertegenwoordigen. Ten slotte bleek dat geen enkele dienst een volledig zicht had op de bestaande internationale fora.

Hoewel alle instanties ter voorbereiding van internationale bijeenkomsten een of andere vorm van voorafgaand overleg hanteerden – ook met diensten die zelf niet aan de vergaderingen deelnamen – kon worden vastgesteld dat er geen duidelijk omschreven werkwijze voorhanden was om de vergaderingen voor te bereiden en om te bepalen welk standpunt België desgevallend moest innemen.[83] De Comités stelden vast dat de werking informeel en niet gestructureerd verliep,

---

82 Er zijn natuurlijk fora die voorbehouden zijn voor één actor. Zo stelt de VSSE dat er twee soorten vergaderingen bestaan: vergaderingen van inlichtingendiensten die worden beheerst door de basisregels van de inlichtingenwereld (met name de '*need to know*' en de 'regel van de derde dienst') en gemengde vergaderingen met zowel inlichtingendiensten als andere inzake terrorisme en extremisme bevoegde diensten. Deze laatste vinden voornamelijk plaats in het kader van de Europese Unie.

83 De federale politie stelde hierover dat er weinig of geen specifieke structurele mechanismen bestaan om de deelname aan vergaderingen en de standpunten, te bespreken. Veelal wordt punctueel afstemming gezocht indien dit noodzakelijk lijkt. Wel vindt in vele gevallen een zekere afstemming plaats binnen de schoot van nationale fora, zoals bijvoorbeeld het College voor inlichtingen en veiligheid.
De VSSE verklaarde dat de Belgische deelnemers maar ook de diensten die niet deelnemen elkaar voorafgaand aan die vergaderingen ontmoeten en hun standpunten uitwisselen. Zo bijvoorbeeld werd het programma inzake de strijd tegen het terrorisme en het extremisme met het oog op het Belgische voorzitterschap Justitie en Binnenlandse Zaken van de Europese Unie (JBZ), opgesteld in overleg met alle betrokken instanties.

zodat er geen zekerheid bestond omtrent het feit of alle betrokken diensten hun standpunt voorafgaand hadden uiteengezet en dat er op de vergaderingen een gezamenlijk 'Belgische standpunt' werd ingenomen.

Hetzelfde gold voor de verspreiding van de resultaten van de vergaderingen: dit gebeurde eveneens informeel en niet-gestructureerd zodat het niet zeker was dat alle betrokken diensten de noodzakelijke *feedback* ontvingen.

II.9. KLACHT INZAKE DE MEDEDELING VAN INFORMATIE DOOR DE ADIV AAN DE FEDERALE POLITIE

Wanneer een kandidaat-beroepsvrijwilliger bij de Krijgsmacht niet slaagt voor zijn basisopleiding, uit hij tegenover zijn collega's concrete bedreigingen ten aanzien van het Belgische leger. Zijn hiërarchie stelt de ADIV hiervan in kennis. De militaire inlichtingendienst voert daarop een onderzoek en komt tot het besluit dat er effectief sprake is van een potentiële bedreiging. Dienvolgens wordt deze informatie meegedeeld aan de politie.

Wanneer de betrokkene zich later kandidaat stelt voor een functie bij de federale politie, slaagt hij niet voor zijn persoonlijkheidstest. Volgens hem is dat te wijten aan de informatie die de ADIV aan de politie heeft bezorgd. Hij beweert in dat kader het slachtoffer te zijn geweest van discriminatie omwille van zijn etnische afkomst.

Het Vast Comité I kwam echter tot de conclusie dat de ADIV handelde conform zijn wettelijke opdracht (artikel 11 W.I&V) en dat de politie, gelet op haar bevoegdheden, gerechtigd was kennis te krijgen van die informatie (artikel 19 W.I&V en 44/1 van de Wet op het Politieambt). Daarbij was duidelijk dat de inlichtingen niet waren doorgegeven met de bedoeling de politie in het kader van een selectieprocedure een beoordelingselement aan te reiken omtrent de persoonlijkheid van de klager. De ADIV deed dan ook geen afbreuk aan de rechten van de betrokkene en er werd door het Vast Comité I geen enkele discriminerende behandeling vastgesteld.

Voor vergaderingen op het niveau van de Verenigde Naties en op het niveau van de Europese Unie zijn er binnen de FOD Buitenlandse Zaken voorafgaande vergaderingen, waarin voortdurend de positie van België wordt besproken. Aan deze vergaderingen nemen de FOD Justitie, de FOD Binnenlandse Zaken, de federale politie, de VSSE, de ADIV en het OCAD deel.

II.10. DE MOGELIJKHEID OM PRIVATE PLAATSEN TE BETREDEN BIJ BESCHERMINGS-OPDRACHTEN

Om een bepaalde evacuatieweg te verkennen betraden de beschermingsofficieren van de VSSE de privétuin van een appartementsgebouw. Deze tuin grensde aan een locatie waar zij instonden voor de bescherming van een hoogwaardigheidsbekleder. De controle gebeurde in aanwezigheid van medewerkers van de private veiligheidsdienst van de betrokken locatie, maar zonder dat de eigenaars van het appartement daarvan op de hoogte waren gesteld. Twee bewoners vroegen zich af of beschermingsofficieren het recht hebben om te allen tijde hun privéterrein te betreden.[84]

De Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst bepaalt dat de agenten van de VSSE slechts onder bepaalde voorwaarden private plaatsen mogen betreden '*buiten medeweten en zonder de instemming van de eigenaar*'.[85] Die specifieke of uitzonderlijke bevoegdheid geldt echter alleen in de uitoefening van hun inlichtingenopdrachten. In het kader van beschermingsopdrachten kan van deze mogelijkheid geen gebruik worden gemaakt. De beschermingsofficieren van de VSSE beschikken weliswaar over bepaalde bevoegdheden van bestuurlijke politie die vergelijkbaar zijn met die van de politiediensten: ze zijn gewapend en mogen gebruik maken van geweld wanneer het leven of de fysieke integriteit van de beschermde persoon in gevaar is. Maar ze mogen – tenzij het een verlaten domein betreft[86] – niet zonder toestemming private plaatsen betreden.

Als gevolg van het voorval zijn de betrokken private veiligheidsdienst en de vertegenwoordiger van het appartementsbewoners tot een consensus gekomen in die zin dat deze laatste voorafgaand op de hoogte zal worden gebracht van elke inspectie door de VSSE.

---

84 De tuin van het appartementsgebouw was bezwaard met een erfdienstbaarheid van doorgang bij hoogdringendheid en bij evacuatie van het naburige gebouw. Deze erfdienstbaarheid had evenwel geen betrekking op eventuele voorafgaandelijke controles van de vluchtweg.

85 Zie art. 18/2, 18/4 en 18/5 W.I&V.

86 Art. 24 W.I&V.

II.11. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2011 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2011 WERDEN OPGESTART

Dit onderdeel bevat een opsomming en een korte situering van alle in 2011 opgestarte onderzoeken en van die onderzoeken waaraan tijdens het werkingsjaar 2011 werd verder gewerkt maar die nog niet konden worden afgerond.

II.11.1. ONDERZOEK MET BETREKKING TOT DE ACTIVITEITEN VAN DE ADIV IN AFGHANISTAN

De Belgische troepen maken in Afghanistan deel uit van de internationale vredesmacht ISAF. Het grootste gedeelte van het Belgische contingent bevindt zich in de Afghaanse hoofdstad Kaboel en bestaat uit een beschermingscompagnie voor de internationale luchthaven. In Kunduz steunt België de werking van de provinciale reconstructieteams en levert ons land *Operational Mentoring and Liaison Teams*. In Kandahar ten slotte draagt België bij met F-16's.[87]

Uit een briefing van de ADIV over de situatie ter plaatse, bleek dat de dienst heel wat inlichtingenmethoden (HUMINT, OSINT, IMINT, SIGINT…) inschakelde en er nauw samenwerkte met inlichtingendiensten van andere landen. Met het oog op het krijgen van een totaalbeeld (en mogelijks de uitwerking van een referentiekader) besliste het Comité over te gaan tot de opening van een toezichtonderzoek '*naar de rol van de ADIV bij de opvolging van de situatie in Afghanistan*'. Daarbij zijn topics als het ingezette personeel, de gehanteerde inlichtingenmethoden, de samenwerking met buitenlandse inlichtingendiensten en de transmissie van inlichtingen aan de orde.

Het Vast Comité I heeft de intentie dit toezichtonderzoek in het najaar van 2012 af te sluiten.

II.11.2. OPVOLGING VAN EEN VEROORDEELD TERRORIST TIJDENS EN NA DIENS DETENTIE IN BELGIË

Volgens een persartikel uit de Britse krant *The Independent*[88] zou een in België veroordeelde terrorist die zijn straf uitzat in de gevangenis van Vorst, onder druk zijn gezet door een agent van een Britse geheime dienst om voor hen te werken. Deze berichtgeving werd uitvoerig overgenomen in de Belgische pers. De man

87 De Belgische regering besliste eind 2011 om vanaf 2012 aan te vatten met de terugtrekking van de Belgische soldaten. In 2014 zouden de laatste militairen moeten vertrokken zijn.

88 *The Independent*, 23 juli 2010.

zou illegaal zijn overgebracht naar het Verenigd Koninkrijk en 'opgesloten' in een geheime basis. Daar zou hij zijn ondervraagd en gedwongen om zijn medewerking te verlenen.

Volgens zijn advocaat kon deze operatie niet plaatsvinden zonder goedkeuren of medeweten van onder meer de Belgische inlichtingendiensten.

Daarop besloot het Vast Comité I een toezichtonderzoek te openen naar '*de mogelijke opvolging van een persoon (M.J.) door de VSSE en de ADIV tijdens en na zijn hechtenis in België*'. De resultaten van dit toezichtonderzoek werden in het voorjaar van 2012 bezorgd aan de Senatoriële Begeleidingscommissie en de bevoegde ministers.

II.11.3. PUNCTUELE ANALYSES DOOR HET OCAD IN HET KADER VAN BEZOEKEN VAN BUITENLANDSE PERSONALITEITEN

In oktober 2010 opende het Vast Comité I, samen met het Vast Comité P, een onderzoek naar '*de evaluatie van de dreiging die door het OCAD wordt uitgevoerd betreffende buitenlandse personaliteiten op bezoek in België*'. De cijfers die door het OCAD in zijn jaarlijkse verslaggeving werden aangehaald, lieten immers veronderstellen dat dergelijke punctuele analyses een enorme investering naar tijd en middelen betekenen voor het Coördinatieorgaan.

De eindrapportage was voorzien in 2011. Het laattijdige antwoord van het OCAD maakte echter dat de onderzoeksverrichtingen niet konden worden gefinaliseerd. De resultaten van het toezichtonderzoek worden in 2012 verwacht.

II.11.4. ADVIEZEN DIE DE VSSE VERSTREKT IN HET KADER VAN NATURALISATIEAANVRAGEN

Eén van de vragen die aan bod kwamen in de zogenaamde zaak-Belliraj[89] was op welke wijze de Veiligheid van de Staat zou zijn tussengekomen in de naturalisatie van deze persoon. Een *item* waarop ook de leden van de Senatoriële Begeleidingscommissie bij de bespreking van het toezichtonderzoek in november 2010 uitvoerig terug kwamen.

In het verlengde hiervan, verzocht de toenmalige Voorzitter van de Senaat het Vast Comité I over te gaan tot het openen van een toezichtonderzoek '*naar de wijze waarop en de omstandigheden waarin de VSSE de vragen tot inlichtingen met betrekking tot de procedures tot het verkrijgen van de Belgische nationaliteit, onderzoekt en behandelt*'. De resultaten van dit onderzoek, dat een juridisch, een des-

[89] VAST COMITÉ I, *Activiteitenverslag 2009*, 30-40.

criptief en een kwantitatief luik omvat, werden in het voorjaar van 2012 bezorgd bij de Begeleidingscommissie.

II.11.5. OPVOLGING VAN BEPAALDE BUITENLANDSE INLICHTINGENDIENSTEN TEN AANZIEN VAN HUN DIASPORA IN BELGIË

België blijkt een grote aantrekkingskracht te hebben op buitenlandse inlichtingendiensten. De aanwezigheid van de Europese instellingen en de NAVO op het grondgebied is daar niet vreemd aan. Buitenlandse inlichtingendiensten vertonen bovendien veel interesse voor het Belgisch hoogtechnologisch onderzoek in ruimtevaartprogramma's, de wapenindustrie en de energiepolitiek. Maar sommige buitenlandse inlichtingendiensten volgen ook nauwgezet de activiteiten van hun eigen migrantengemeenschappen – hun diaspora – in België op.

Op verzoek van de toenmalige Voorzitter van de Senaat werd in juli 2011 een toezichtonderzoek geopend *'naar de wijze waarop de Belgische inlichtingendiensten de gebeurlijke activiteiten opvolgen die inlichtingendiensten uit belangrijke immigratielanden van buiten de Europese Unie ontplooien op het Belgisch grondgebied'*.

In de loop van 2011 werden aan de VSSE en de ADIV diverse vragen gesteld. De resultaten van het toezichtonderzoek worden verwacht in de loop van 2012.

II.11.6. HET RECHT OP SYNDICALE BIJSTAND IN HET KADER VAN VEILIGHEIDSONDERZOEKEN

In oktober 2011 ontving het Vast Comité I de vraag of een vakbondsafgevaardigde het recht heeft een militair bij te staan tijdens een interview in het kader van een veiligheidsonderzoek. Het Vast Comité I opende hierop een toezichtonderzoek.

De betrokken militair tekende evenwel in december 2011 beroep aan bij het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen. Met toepassing van artikel 3 W.Beroepsorgaan schorste het Vast Comité I het toezichtonderzoek op. Begin 2012 volgde de uitspraak van het Beroepsorgaan en kon het onderzoek worden hernomen.

HOOFDSTUK III.
CONTROLE OP DE BIJZONDERE INLICHTINGENMETHODEN

Artikel 35 § 1, 1° W.Toezicht bepaalt dat het Comité in zijn jaarlijks activiteitenverslag '*specifiek aandacht [moet besteden] aan de specifieke en de uitzonderlijke methoden voor het verzamelen van gegevens, zoals bedoeld in artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten [en] aan de toepassing van hoofdstuk IV/2 van dezelfde wet*'.[90] Voorliggend hoofdstuk behandelt dan ook de inzet van bijzondere inlichtingenmethoden door de beide inlichtingendiensten en de wijze waarop het Vast Comité I zijn jurisdictionele rol in deze waarneemt. Het vormt de verkorte weergave van de twee zesmaandelijkse verslagen die het Comité ten behoeve van de Begeleidingscommissie van de Senaat opstelde.[91]

III.1. ENKELE SPECIFIEKE AANDACHTSPUNTEN

III.1.1. INFORMELE OVERLEGMOMENTEN MET DE BETROKKEN ACTOREN

Het Vast Comité I pleegde op regelmatige basis overleg over de toepassing van de BIM-Wet en dit met de VSSE, de ADIV en de BIM-commissie.

Met de BIM-commissie werden onder meer volgende items besproken:

- de doorstroming van informatie en documenten van de BIM-commissie naar het Vast Comité I;
- de permanentie van de BIM-commissie tijdens verlofperiodes, mede gelet op de afwezigheid van plaatsvervangers;

---

90 Zie voor een bespreking van de bijzondere inlichtingenmethoden en de controle hierop: VAST COMITÉ I, *Activiteitenverslag 2010*, 51-63 en W. VAN LAETHEM, D. VAN DAELE en B. VANGEEBERGEN (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, 299 p.

91 Art. 35 § 2 en 66*bis* § 2, derde lid, W.Toezicht. De twee verslagen werden respectievelijk midden september 2011 en begin februari 2012 aan de Begeleidingscommissie overgezonden.

– de vertraging in de toezending van toelatingen tot aanwending van specifieke methoden aan het Comité in die gevallen waarin de BIM-commissie bijkomende informatie opvraagt bij de inlichtingendiensten;
– de problematiek van de inzet van specifieke methoden ter identificatie van gebruikers van communicatiemiddelen, in het licht van de subsidiariteitseis (zie ook III.2.2.1 en III.3.2.6);
– de wijze van in kennisstelling van de commissieleden in geval van een methode die gemachtigd wordt na eensluidend advies van de voorzitter van de BIM-commissie die bij hoogdringendheid werd gevat.

Onderstaande punten werden aangekaart met de inlichtingendiensten:
– de voorwaarden waaronder de Dienst Enquêtes van het Vast Comité I op informele wijze bijkomende informatie kan verkrijgen van de inlichtingendiensten vóór de eventuele ambtshalve vatting door het Comité;
– de eventuele gevolgen voor de werking van de twee diensten of hun reactie wanneer het Comité vaststelt dat de VSSE en de ADIV onafhankelijk van elkaar (een) bijzondere methode(n) inzetten op eenzelfde *target*.

III.1.2. VIA BIJZONDERE METHODEN 'BEHAALDE RESULTATEN'

Artikel 35 § 2 W.Toezicht bepaalt dat '*in voorkomend geval, de behaalde resultaten*' moeten worden opgenomen in het zesmaandelijks verslag dat het Comité dient te richten aan de Begeleidingscommissie. Gelet op de complexiteit en de sensibiliteit van dergelijke rapportage in een inlichtingencontext, werkt het Comité momenteel een methodologie uit om steekproefsgewijs de appreciatie die de inlichtingendiensten geven van de door hen behaalde resultaten, te evalueren. Dit instrument moet toelaten nuttig (dit is in functie van aanbevelingen omtrent de doelmatigheid en rechtmatigheid van het optreden van de diensten) te kunnen rapporteren over de inzet van bijzondere methoden.

III.1.3. ARREST VAN HET GRONDWETTELIJK HOF

Het Grondwettelijk Hof heeft zich op 22 september 2011 uitgesproken over de twee verzoeken tot vernietiging van diverse bepalingen van de BIM-Wet.[92] Daarbij werd slechts één wetsartikel vernietigd: artikel 2 § 3 W.I&V, dat een passieve notificatieverplichting in het leven roept, moet op twee punten aangepast worden.

[92] Door de Orde van Vlaamse balies (*BS* 16 augustus 2010) en door de Liga voor Mensenrechten (*BS* 27 oktober 2010). Een uittreksel uit het arrest werd gepubliceerd in het Belgisch Staatsblad van 12 december 2011.

Enerzijds moeten ook rechtspersonen in kennis kunnen worden gesteld wanneer zij het voorwerp uitmaakten van een bijzondere methode. Anderzijds moet voorzien worden dat de betrokken inlichtingdienst een (rechts)persoon op eigen initiatief in kennis stelt van zodra de BIM-commissie dit mogelijk acht.

III.2. CIJFERS MET BETREKKING TOT DE SPECIFIEKE EN UITZONDERLIJKE METHODEN

In 2011 werden voor beide inlichtingendiensten samen 831 toelatingen of machtigingen (verder steeds aangeduid als 'toelating'[93]) verleend tot het aanwenden van bijzondere inlichtingenmethoden: 764 voor de VSSE (waarvan 731 specifieke en 33 uitzonderlijke) en 67 voor de ADIV (waarvan 60 specifieke en 7 uitzonderlijke). Bij de interpretatie van deze cijfers dienen twee zaken voor ogen te worden gehouden:

– in principe wordt per 'toelating' slechts één soort bijzondere methode gemachtigd (een observatie *of* een doorzoeking, niet beide). Hiervan wordt in één geval afgeweken: in één en dezelfde toelating kan een inlichtingendienst gemachtigd worden om oproep- of lokalisatiegegevens te bekomen en nadien tot de identificatie over te gaan van de aldus bekomen informatie (zie verder III.2.2.1);
– per toegelaten methode kunnen wel meerdere *targets* (zoals personen, organisaties, plaatsen, voorwerpen, communicatiemiddelen…) worden geviseerd. Naar impact op de werklast van de inlichtingendiensten en de privacy van burgers kan de ene toelating dan ook veel ingrijpender zijn dan de andere.

De cijfers voor de twee diensten worden hieronder apart weergegeven. Beide diensten beschikken weliswaar over dezelfde bevoegdheden, maar hun opdrachten zijn dermate verschillend dat uit een cijfermatige vergelijking van de twee diensten, weinig lessen kunnen getrokken worden.

Per dienst worden drie grote rubrieken onderscheiden: cijfers over de specifieke methoden, cijfers over de uitzonderlijke methoden en cijfers inzake de dreigingen en te verdedigen belangen die door de verschillende methoden beoogd worden.

93 In de wet worden de termen 'toelating', 'machtiging' en 'beslissing' veelal door elkaar gebruikt. Omwille van de leesbaarheid van dit verslag wordt de eerste term voorbehouden voor alle door het diensthoofd of de minister toegelaten bijzondere methoden, terwijl de term 'beslissing' wordt gereserveerd in het kader van de jurisdictionele controle door het Vast Comité I.

III.2.1. TOELATINGEN MET BETREKKING TOT DE ADIV

III.2.1.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	7
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	0
Kennisnemen van identificatiegegevens van elektronisch communicatie-verkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	23
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	17
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator	13
TOTAAL	60[94]

III.2.1.2. De uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	0
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	0
Oprichten en gebruiken van een fictieve rechtspersoon	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	0
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	5
Binnendringen in een informaticasysteem	0
Afluisteren, kennisnemen en opnemen van communicaties	2
TOTAAL	7

[94] In drie gevallen had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

III.2.1.3. De belangen en dreigingen die de inzet van de bijzondere methoden rechtvaardigen

De ADIV mag de specifieke en de uitzonderlijke methoden aanwenden in het kader van drie van zijn opdrachten die elk op zich specifieke te vrijwaren belangen behelzen:

- de inlichtingenopdracht die gericht is op dreigingen tegen onder meer de onschendbaarheid van het nationaal grondgebied, de militaire defensieplannen en het wetenschappelijk en economisch potentieel op vlak van defensie (art. 11, 1° W.I&V);
- de opdracht inzake de militaire veiligheid die bijvoorbeeld gericht is op het behoud van de militaire veiligheid van het defensiepersoneel, van de militaire installaties en de militaire informatica- en verbindingssystemen (art. 11, 2° W.I&V);
- de bescherming van militaire geheimen (art. 11, 3° W.I&V).

AARD BELANG	AANTAL
Inlichtingenopdracht	38
Militaire veiligheid	8
Bescherming geheimen	19

Anders dan voor de VSSE, staan de dreigingen waaraan de ADIV aandacht mag of moet besteden, niet in de wet omschreven. Toch vermeldt deze dienst in zijn toelatingen systematisch welke bedreiging wordt geviseerd. Dergelijke transparantie verdient inderdaad aanbeveling. De cijfers tonen aan dat, wat betreft de inzet van bijzondere methoden, de strijd tegen spionage de eerste prioriteit is van de militaire inlichtingendienst.

AARD DREIGING	AANTAL
Spionage	54
Terrorisme	10
Extremisme	3

III.2.2. TOELATINGEN MET BETREKKING TOT DE VSSE

III.2.2.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	89
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	4
Kennisnemen van identificatiegegevens van elektronisch communicatie-verkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	355
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	237
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator	46
TOTAAL	731[95]

Bovenstaande tabel maakt duidelijk dat het overgrote deel van de methoden die door de VSSE worden ingezet, betrekking heeft op de (weinig intrusieve) identificatie van de abonnee of de gebruiker van een telefoon- of GSM-nummer. Het betreft 355 toelatingen tot identificaties waarbij in één toelating doorgaans meerdere nummers zijn opgenomen. *In casu* hadden de 355 toelatingen betrekking op 1892 nummers. Toch ligt het aantal werkelijk uitgevoerde identificaties nog hoger. Het Vast Comité I heeft zich immers in samenspraak met de BIM-commissie akkoord verklaard met de werkwijze waarbij het diensthoofd van een inlichtingendienst in éénzelfde toelating zowel de opsporing alsook de identificatie van oproepgegevens machtigt. Hierdoor wordt vermeden dat het diensthoofd twee opeenvolgende *quasi* identieke toelatingen moet verlenen in eenzelfde dossier. Beide methoden zijn immers sterk verknocht: oproepgegevens zijn slechts nuttig indien ze kunnen toegeschreven worden aan een welbepaalde persoon of organisatie. Deze werkwijze heeft weliswaar tot gevolg dat het Comité geen automatisch zicht heeft op het aantal verrichte identificaties.

Het Comité eist echter dat de inlichtingendienst alleen die nummers via een operator zou laten identificeren die niet via een gewone methode kunnen worden geïdentificeerd én die noodzakelijk zijn in het kader van het inlichtingenonderzoek. Op die manier is voldaan aan het proportionaliteits- en subsidiariteitsbeginsel. De diensten hebben hun toelatingen waarin zij achtereenvolgens kennis

[95] In negen gevallen had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

willen nemen van oproep- én identificatiegegevens in die zin aangepast. Het Comité heeft steekproefsgewijs gecontroleerd hoe de diensten deze afspraak invullen.

III.2.2.2. De uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	2
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	3
Oprichten en gebruiken van een fictieve rechtspersoon	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	4
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	10
Binnendringen in een informaticasysteem	3
Afluisteren, kennisnemen en opnemen van communicaties	11
TOTAAL	33

Deze tabel toont aan dat de VSSE, vergeleken met de ADIV, intenser gebruik maakt van de mogelijkheid om bijzondere inlichtingenmethoden aan te wenden.

III.2.2.3. De belangen en dreigingen die de inzet van de bijzondere methoden rechtvaardigen

De VSSE mag slechts optreden ter vrijwaring van volgende belangen:
- de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde;
- de uitwendige veiligheid van de Staat en de internationale betrekkingen;
- de vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

AARD BELANG	AANTAL[96]
De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde	694
De uitwendige veiligheid van de Staat en de internationale betrekkingen	571
De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel	24

[96] Per toelating kunnen meerdere belangen aan de orde zijn.

Volgende tabel geeft een beeld van de (potentiële) dreigingen die de VSSE viseerde bij de inzet van specifieke en uitzonderlijke methoden. Uiteraard kan één methode gericht zijn tegen meerdere dreigingen. De VSSE kan de specifieke methoden aanwenden in het kader van alle dreigingen die tot haar bevoegdheid behoren (art. 8 W.I&V). Uitzonderlijke methoden mogen niet ingezet worden in het kader van het extremisme en de inmenging. Zij zijn wel toegelaten in het kader van het aan het terrorisme voorafgaande radicaliseringsproces (art. 3, 15° W.I&V).

AARD DREIGING	AANTAL[97]
Spionage	193
Terrorisme (en radicaliseringsproces)	371
Extremisme	319
Proliferatie	17
Schadelijke sektarische organisaties	4
Inmenging	3
Criminele organisaties	3

Inzake de inzet van bijzondere methoden zijn het terrorisme en extremisme duidelijk topprioriteiten voor de VSSE. Verder is opvallend dat – net zoals voor de ADIV – spionage als dreiging een aanzienlijk aandeel heeft in de inzet van specifieke en uitzonderlijke methoden.

III.3. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS JURISDICTIONEEL ORGAAN

III.3.1. DE CIJFERS

Het Vast Comité I kan op vijf manieren worden gevat om zich uit te spreken over de wettelijkheid van bijzondere inlichtingenmethoden (art. 43/4 W.I&V):
- op eigen initiatief;
- op verzoek van de Commissie voor de bescherming van de persoonlijke levenssfeer;
- op klacht van een burger;
- van rechtswege als de BIM-commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden;
- van rechtswege als de bevoegde minister een toelating heeft verleend op basis van artikel 18/10 § 3 W.I&V.

97 Per toelating kunnen verschillende dreigingen aan de orde zijn.

Daarnaast kan het Comité ook gevat worden in zijn hoedanigheid van 'prejudicieel adviesverlener' (art. 131*bis*, 189*quater* en 279*bis* Sv.). Desgevraagd geeft het Comité een advies over de al dan niet rechtmatigheid van aan de hand van specifieke of uitzonderlijke methoden ingewonnen inlichtingen die in een strafzaak worden gebruikt. De beslissing om een advies te vragen, berust bij de onderzoeksgerechten of de strafrechters. Strikt genomen treedt het Comité alsdan niet op als jurisdictioneel orgaan.[98]

WIJZE VAN VATTING	AANTAL
Op eigen initiatief	28
Privacycommissie	0
Klacht	0
Schorsing door BIM-commissie	9[98]
Toelating minister	0
Prejudicieel adviesverlener	0
TOTAAL	37

Op een totaal van 831 toelatingen tot het aanwenden van bijzondere methoden, werd het Comité 37 maal gevat.[99] Eens gevat, kan het Comité verschillende soorten (tussen)beslissingen nemen. In de twee eerste gevallen wordt evenwel een beslissing genomen vóór de eigenlijke vatting.

- nietigheid van de klacht wegens vormgebrek of afwezigheid van een persoonlijk en rechtmatig belang (art. 43/4, eerste lid, W.I&V);
- beslissing om geen gevolg te geven aan een klacht die kennelijk niet gegrond is (art. 43/4, eerste lid, W.I&V);
- schorsing van de betwiste methode in afwachting van een definitieve beslissing (art. 43/4, laatste lid, W.I&V);
- vordering tot bijkomende informatie ten aanzien van de BIM-commissie (art. 43/5 § 1, eerste tot derde lid, W.I&V);
- vordering tot bijkomende informatie ten aanzien van de betrokken inlichtingendienst (art. 43/5 § 1, derde lid, W.I&V);
- onderzoeksopdracht voor de Dienst Enquêtes I (art. 43/5 § 2 W.I&V). In deze rubriek wordt niet verwezen naar de veelvuldige bijkomende informatie die door de Dienst Enquêtes I wordt ingewonnen vóór de eigenlijke vatting en dus op eerder informele wijze;
- horen van de BIM-commissieleden (art. 43/5 § 4, eerste lid, W.I&V);

98 In twee dossier schorste de BIM-commissie een toelating nadat het Vast Comité I zich reeds had gevat. Deze schorsingen worden hier niet meegerekend.

99 De 'vatting' heeft steeds betrekking op de toelating door het hoofd van de inlichtingendienst.

- horen van het diensthoofd of de leden van de betrokken inlichtingendienst (art. 43/5 § 4, eerste lid, W.I&V);
- beslissing over geheimen die betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek waarvan de leden van de inlichtingendiensten drager zijn, na overleg met de bevoegde magistraat (art. 43/5 § 4, tweede lid, W.I&V);
- uitspraak door de voorzitter van het Vast Comité I, na het diensthoofd te hebben gehoord, indien het lid van de inlichtingendienst meent het geheim waarvan hij drager is te moeten bewaren omdat de onthulling ervan nadelig is voor de bescherming van de bronnen, de bescherming van de persoonlijke levenssfeer van derden of de vervulling van de opdrachten van de inlichtingendienst (art. 43/5 § 4, derde lid, W.I&V);
- stopzetting van een methode indien ze nog steeds in uitvoering is of indien zij werd geschorst door de BIM-commissie en bevel dat de gegevens die met deze methode werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd (art. 43/6 § 1, eerste lid, W.I&V);
- gedeeltelijke stopzetting van een toegelaten methode.[100] Hier wordt de situatie bedoeld waarbij bijvoorbeeld één methode in tijd wordt beperkt, niet de situatie waarbij in één toelating van een diensthoofd meerdere methoden worden gemachtigd en het Comité slechts één ervan stopzet.
- gehele of gedeeltelijke opheffing van de schorsing en het verbod die door de BIM-commissie was uitgesproken (art. 43/6 § 1, eerste lid, W.I&V). Dit houdt in dat de door het diensthoofd toegelaten methode door het Comité wel (gedeeltelijk) wettelijk, proportioneel en subsidiair werd bevonden;
- onbevoegdheid van het Vast Comité I;
- ongegrondheid van de aanhangige zaak en geen stopzetting van de methode;
- advies als prejudicieel adviesverlener (artt. 131*bis*, 189*quater* en 279*bis* Sv.).

AARD VAN DE BESLISSING	AANTAL	AANTAL EIND-BESLISSINGEN
Nietige klacht	0	
Kennelijk ongegronde klacht	1	
Schorsing methode	3	
Bijkomende informatie van BIM-commissie	4	
Bijkomende informatie van inlichtingendienst	9	
Onderzoeksopdracht Dienst Enquêtes	17	
Horen BIM-commissieleden	0	
Horen leden inlichtingendiensten	1	

[100] Deze beslissing, die niet als dusdanig omschreven staat in de wet, kan vergeleken worden met een 'gedeeltelijke stopzetting'.

AARD VAN DE BESLISSING	AANTAL	AANTAL EIND-BESLISSINGEN
Beslissing m.b.t. geheim van onderzoek	0	
Gevoelige informatie tijdens verhoor	0	
Stopzetting methode	12	39
Gedeeltelijke stopzetting methode	7	
(Gedeeltelijke) opheffing verbod van BIM-commissie	5[101]	
Onbevoegd	0	
Wettige toelating / Geen stopzetting methode / Ongegrond	15	
Prejudicieel advies	0	

In 2011 nam het Comité 39 eindbeslissingen.[102, 103] Er mag niet uit het oog worden verloren dat die beslissingen slechts het sluitstuk vormen van de BIM-activiteiten van het Comité en in die zin slechts een fractie van de reële inspanning uitmaken. Immers, *elke* BIM-toelating van de VSSE en van de ADIV wordt aan een inhoudelijke controle onderworpen en dit op basis van een gestandaardiseerde procedure en een gedetailleerde *checklist*. Desgevallend worden ook bijkomende vragen gesteld aan de inlichtingendiensten vooraleer tot een vatting wordt overgegaan. De controle op de BIM-toelatingen vertegenwoordigt dan ook een aanzienlijk aandeel in het tijdsbudget van het Comité.

Vijf van de negen door de BIM-commissie uitgesproken schorsingen werden geheel of gedeeltelijk opgeheven. Daarenboven zette het Comité dertien toelatingen geheel of gedeeltelijk stop zonder dat die vooraf door de BIM-commissie waren geschorst.

Van de negentien gehele of gedeeltelijke stopzettingen hadden er vijf betrekking op dossiers van de ADIV en veertien op dossiers van de VSSE.

---

101 In deze telling zitten twee beslissingen van het Comité vervat die ook opgenomen werden onder de rubriek 'Gedeeltelijke vernietiging van toelating' omdat het de BIM-commissie na de vatting van het Comité de toelatingen volledig had geschorst terwijl die schorsing gedeeltelijk moest opgeheven worden.

102 Het aantal vattingen en het aantal eindbeslissingen komt niet noodzakelijk overeen. Dit kan bijvoorbeeld omdat de eindbeslissing niet in de referteperiode van de vatting valt of omdat een vatting kan aanleiding geven tot meerdere eindbeslissingen. *In casu* was dit laatste het geval (zie vorige voetnoot).

103 Het Vast Comité I moet binnen een termijn van een maand volgend op de dag waarop het werd geadieerd een definitieve uitspraak doen (art. 43/4 W.I&V). In alle dossiers werd die termijn gerespecteerd.

III.3.2. DE RECHTSPRAAK

Hieronder wordt de essentie weergegeven van de 39 eindbeslissingen die het Vast Comité I in 2011 nam. De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk worden opgenomen.

De beslissingen worden gegroepeerd in zes rubrieken:
- wettelijke (vorm)vereisten voorafgaand aan de uitvoering van een methode;
- motivering van de toelating;
- wettelijke (vorm)vereisten bij de uitvoering van een methode;
- wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging;
- de proportionaliteitseis;
- de subsidiariteitseis.

Indien relevant werden sommige beslissingen onder meerdere rubrieken opgenomen.

III.3.2.1. Wettelijke (vorm)vereisten voorafgaand aan de uitvoering van een methode

Geen bijzondere methode mag aangewend worden zonder voorafgaande schriftelijke toelating van het diensthoofd. In geval van een uitzonderlijke methode dient er daarenboven een ontwerp van machtiging en een eensluidend advies van de BIM-commissie voor te liggen. Indien methoden worden ingezet zonder dergelijke schriftelijke toelating of desgevallend eensluidend advies, moet het Comité uiteraard optreden.

III.3.2.1.1. Geen schriftelijke toelating

Het Comité stelde vast dat een inlichtingendienst was overgegaan tot de kennisname van de oproepgegevens van een mobiel én een vast telefoonnummer, terwijl de verleende toelating alleen betrekking had op het mobiele nummer (dossier 2011/501a). De 'observatie' van de vaste lijn werd dan ook vernietigd wegens onwettelijk aangezien er dienaangaande geen enkele schriftelijke toelating vanwege het diensthoofd voorlag.

In een ander dossier verleende een diensthoofd de toelating om de oproepgegevens van een GSM-nummer op te sporen gedurende zes maanden (dossier 2011/748). In uitvoering van deze toelating vorderde de inlichtingendienst één telecomoperator om de bedoelde oproepgegevens te verstrekken én alle telecomoperatoren om de titularissen te identificeren van de aldus bekomen nummers. Dergelijke identificatie maakt echter een aparte methode uit. Daarvoor was geen toelating verleend: '*Dat derhalve voormelde vordering, voor zover ze strekt tot de*

identificatie van de abonnee of de gewone gebruiker van de opgespoorde nummers (oproepgegevens) niet gedekt wordt door een (rechtsgeldige) beslissing en dienvolgens onwettig is.'

Dezelfde problematiek diende zich ook aan in een derde dossier. Het diensthoofd van de inlichtingendienst had de toelating verleend om over te gaan tot de identificatie van '*alle telefoonnummers waarvan X titularis is*' (dossier 2011/830). Uit de daaropvolgende vordering aan de operatoren bleek echter dat niet alleen werd verzocht om identificatie van de telefoonnummers op naam van X, maar ook om identificatie van de communicatiemiddelen van diverse andere abonnees. De aangewende methode was dus niet integraal gedekt door een schriftelijke en met reden omklede beslissing en dit op straffe van onwettelijkheid van dat gedeelte van de methode dat de beslissing gebeurlijk te buiten gaat. '*Dat dienvolgens targets (personen, plaatsen, …) die ten gene dele voorzien zijn in een beslissing, niet op legale wijze het voorwerp van een vordering kunnen uitmaken.*' Bovendien bleek dat, waar de toelating slechts gewag maakte van de identificatie van alle telefoonnummers van X., in de vordering aan de operatoren ook gevraagd werd om over te gaan tot de identificatie van *al* diens elektronische communicatiediensten: '*Dat ook hier geen overeenstemming is tussen de beslissing (gelimiteerd tot telefoniediensten) en de uiteindelijke vordering.*'

III.3.2.1.2. Toelating van de plaatsvervanger van het diensthoofd

Het Vast Comité I vatte zich in een dossier (2011/406) waarbij een specifieke methode werd gemachtigd '*Voor de Administrateur-generaal, afwezig, [naam], Adviseur*'. De betrokken adviseur nam op dat ogenblik de algemene directie van de dienst waar.

De vraag was of op deze wijze was tegemoet gekomen aan artikel 18/3 § 1, tweede lid, W.I&V dat onder meer bepaalt dat een specifieke methode slechts kan worden aangewend na een schriftelijke en met redenen omklede toelating van het diensthoofd, zijnde '*de administrateur-generaal van de Veiligheid van de Staat of, bij verhindering, de dienstdoende administrateur-generaal*'. Met deze bepaling wou de wetgever garanderen dat de directie van de inlichtingendiensten zelf steeds op de hoogte is van de aanwending van een specifieke methode en de uitvoering ervan. Alhoewel de betrokken adviseur formeel verkeerdelijk tekende '*voor de Administrateur-generaal*', nu hij op dat ogenblik zelf dienstdoende administrateur-generaal was, werd er in wezen wel degelijk tegemoetgekomen aan de finaliteit van de wet. Daarenboven bleek duidelijk dat de administrateur-generaal afwezig was zodat hij in het kader van de BIM-werking terecht tot delegatie kon overgaan. Daarnaast stelde het Comité vast dat in het K.B. van 14 januari 1994 houdende het statuut van de administrateur-generaal en de adjunct-administrateur-generaal van de Veiligheid van de Staat, noch in het K.B. van 5 december 2006 betreffende het algemeen bestuur en de ondersteuningscel van de Veiligheid

van de Staat dwingende regels zijn vermeld in verband met de vervanging van het diensthoofd. Er werd dan ook geen onwettigheid vastgesteld.

III.3.2.1.3. Voorafgaandelijke kennisgeving BIM-commissie in geval van een specifieke methode

Een inlichtingendienst had de toelating om gedurende een afgebakende periode de toegang van een private plaats te bewaken met een camera. Aangezien hij de maatregel wou 'verlengen'[104] stelde het diensthoofd een nieuwe toelating op voor een periode die onmiddellijk aansloot op de vorige termijn (dossier 2011/667). Bijzonder aan deze zaak was echter dat de BIM-commissie pas in de loop van de ochtend van de eerste dag van de nieuwe termijn kennis kreeg van de 'verlenging'. Nu bepaalt artikel 18/3 § 1 W.I&V dat een specifieke methode pas kan worden aangewend na kennisgeving van de toelating aan de BIM-commissie. Gevolg was dat de eventuele observatie vanaf middernacht (op dat ogenblik verliep de oorspronkelijke toelating om te observeren) tot aan de kennisgeving van de nieuwe toelating niet gedekt was door een geldig mandaat. De mogelijks in die korte tussenperiode genomen beelden dienden dan ook te worden vernietigd.

III.3.2.1.4. Afwezigheid van een eensluidend advies

Een inlichtingendienst wenste communicatie af te luisteren (art. 18/17 § 1 W.I&V) en een private plaats te betreden om er afluisterapparatuur te plaatsen (art. 18/17 § 2 W.I&V) (dossier 2011/300). Aangezien het een uitzonderlijke methode betrof, was het eensluidend advies van de BIM-commissie vereist. Dit advies sloeg naar oordeel van het Vast Comité I evenwel alleen op de bevoegdheid omschreven in artikel 18/17 § 2 W.I&V (en dus niet op het eigenlijke afluisteren). Ook uit de periode waarin de uitzonderlijke methode volgens de BIM-commissie kon worden toegepast, bleek voor het Comité dat het advies alleen betrekking had op het plaatsen en verwijderen van het afluisterdispositief; niet op het afluisteren zelf.

Het Vast Comité I besliste daarom tot de onwettigheid van de '*gebeurlijke beslissing tot uitvoering van de methode zoals bedoeld in art. 8/17 § 1 W.I&V*'.

III.3.2.1.5. (G)een eensluidend advies in geval van een vermeend journalist?

De betrokken inlichtingendienst wenste de identiteit te achterhalen van een anonieme *blogger* die op zijn website onder meer extremistische opinies verspreidde (dossier 2011/204). Hij stelde zich daarbij voor als journalist. De vraag was of de inlichtingendienst het eensluidend advies van de BIM-commissie moest beko-

[104] Anders dan voor uitzonderlijke methoden, voorziet de wet strikt genomen niet in de mogelijkheid om een specifieke maatregel te 'verlengen'. Is hij afgelopen, dan moet een nieuwe methode worden gemachtigd.

men voor deze methode zonder dat ze meer gegevens had over de beweerde hoedanigheid van de *blogger*. Immers, artikel 18/3 § 1, derde lid W.I&V bepaalt het volgende: '*De specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen- en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële bedreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op voorstel van het diensthoofd*.'

Net zoals de BIM-commissie, oordeelde het Comité dat de specifieke methode hier zonder voorafgaandelijk advies kon ingezet worden om zo de identiteit van de *blogger* na te gaan en vervolgens te controleren of het werkelijk een journalist betrof in de zin van de wet. Indien door deze verificatie zijn hoedanigheid van journalist zou worden bevestigd, moeten de bepalingen opgenomen in de artikelen 18/2 § 3 en 18/3 § 1, derde lid, W.I&V worden nageleefd.

Eenzelfde vraag was aan de orde in een ander dossier. Een inlichtingendienst wenste de identiteit te achterhalen van de titularissen van GSM-nummers die verdacht werden van inlichtingenactiviteiten maar die mogelijks onder de *cover* van journalist opereerden (dossier 2011/264). Opnieuw oordeelde het Comité dat de specifieke methode zonder meer kon worden ingezet om de identiteit en de eventuele hoedanigheid van journalist van de gebruiker na te gaan.

III.3.2.1.6. Eensluidend advies en de draagwijdte van het begrip 'informaticasysteem'

Een diensthoofd wenste over te laten gaan tot de identificatie van de PUK-codes van bepaalde SIM-kaartnummers die in het bezit waren van een persoon die de aandacht van zijn dienst genoot (dossier 2011/721). Hij beschouwde dit als een specifieke methode, met name '*de identificatie van de abonnee of de gewone gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel*' zoals omschreven in artikel 18/7 W.I&V. Onder dekking van dezelfde machtiging zou middels de bekomen PUK-codes een nieuwe PIN-code worden gecreëerd zodat nadien, '*via bijkomende BIM-methoden, de kaarten dan (kunnen) worden uitgelezen*'.

Het Vast Comité I schorste de betrokken methode en onderzocht de wettelijkheid. Het stelde vast dat de methode in realiteit niet strekte tot identificatie van de abonnee of de gebruiker van de bedoelde SIM-kaarten; deze was immers reeds gekend. Met de methode werd immers finaal het wijzigen van de PIN-code beoogd met behulp van de (te achterhalen) de PUK-code of unieke deblokkagecode van de SIM-chip.

In een SIM-kaart is een *S(ubscriber) I(dentity of identification) M(odule)* aangebracht, die een geïntegreerd circuit is, waarop onder meer data geïnformatiseerd en beveiligd worden opgeslagen. Dergelijke SIM-chip moet gezien worden als een 'informaticasysteem' in de zin van artikel 18/16 W.I&V. De wetgever heeft aan deze term immers dezelfde betekenis willen geven als in de Wet van 28 november 2000 inzake informaticacriminaliteit.[105] En bij de totstandkoming van de Wet van 28 november 2000 werden informaticasystemen omschreven als '*alle systemen voor de opslag, verwerking of overdracht van data. Hierbij wordt vooral gedacht aan computers, chipkaarten en dergelijke, maar ook aan netwerken en delen daarvan, evenals aan telecommunicatiesystemen of onderdelen daarvan die een beroep doen op IT.*'[106] Het verwerven én aanwenden van de PUK-code om de PIN-code te wijzigen en deze in te voeren, maakt dan ook de uitzonderlijke methode uit zoals bedoeld in artikel 18/16 § 1, 1° en 2° W.I&V ('*al dan niet met behulp van technische middelen, valse signalen, valse sleutels of valse hoedanigheden 1° toegang te krijgen tot een informaticasysteem; 2° er elke beveiliging van op te heffen;*'). Nu de wettelijke vereisten inzake de machtiging van een uitzonderlijke methode niet werden nageleefd, zette het Comité de methode stop.

III.3.2.1.7. Eensluidend advies in geval van hoogdringendheid

In het kader van een lopende operatie machtigde het diensthoofd van de betrokken inlichtingendienst een doorzoeking van een private plaats (dossier 2011/331). Er werd gebruik gemaakt van de procedure bij hoogdringendheid zoals omschreven in artikel 18/10 § 4 W.I&V. Deze bepaling laat het diensthoofd toe de uitzonderlijke methode schriftelijk te machtigen nadat hij het eensluidend advies van de voorzitter van de BIM-commissie (en dus niet van de gehele commissie) heeft verkregen. De kwestie draaide rond dit eensluidend advies. De schriftelijke machtiging van het diensthoofd vermeldde alleen dat dit advies bekomen was; het betrof evenwel een mondeling advies. Ook was geen schriftelijk ontwerp van machtiging, noch enig(e) geschreven (bevestiging van de concrete inhoud van het mondelinge) advies voorhanden.

Overeenkomstig artikel 18/10 § 1 W.I&V houdt het onderwerpen van een machtiging aan het eensluidend advies van de BIM-commissie een onderzoek in van de naleving van de wettelijke bepalingen voor het aanwenden van de uitzonderlijke methoden, van de principes van proportionaliteit en subsidiariteit, alsook een controle van de door artikel 18/10 § 2 W.I&V voorgeschreven vermeldingen. Van dergelijk onderzoek en van de klaarblijkelijke conformiteitsbevinding lag geen enkel verifieerbaar schriftelijk gegeven voor, op de loutere vermelding na van de aanwezigheid van een eensluidend advies in de machtiging. Het Comité oordeelde dat dit laatste onvoldoende was. Dergelijke handelwijze laat het Vast

105 *Parl. St.* Senaat 2008-2009, 4-1053/1, 54.
106 *Parl. St.* Kamer 1999-2000, 50-213/1 en 50-214/1, 12.

Comité I immers niet toe de legaliteitstoets in al zijn aspecten uit te voeren (met name *in casu* het nazicht van de overeenstemming tussen (het ontwerp van) de machtiging enerzijds en het verstrekte eensluidend advies anderzijds). Alleen al omdat zo de controletaak van het Vast Comité I wordt uitgehold, kon deze werkwijze niet als wettig worden aangezien.

Daarenboven merkte het Comité op dat de vigerende wettelijke en reglementaire bepalingen expliciet noch impliciet gewagen van enig mondeling ontwerp van machtiging vanwege het diensthoofd of van enig mondeling eensluidend advies vanwege de BIM-commissie. Bovendien bepaalt artikel 43/3 W.I&V dat *alle* beslissingen, adviezen en machtigingen onverwijld ter kennis moeten worden gebracht van het Vast Comité I en dit *ter fine* van zijn wettigheidscontrole. Dit betekent dat deze beslissingen, adviezen en machtigingen de vorm van een document moeten aannemen.

Het Comité puurde nog een bijkomend argument uit het feit dat de wetgever op het schriftelijke karakter slechts een zeer restrictieve uitzondering heeft toegestaan, met name inzake de vordering door de inlichtingenofficier bij uiterst dringende noodzaak in de gevallen van de specifieke methoden bedoeld in de artikelen 18/6 § 2, 18/7 § 2 en 18/8 § 2 W.I&V. Maar zelfs dergelijke vordering moet volgens de wet zo snel mogelijk schriftelijk worden bevestigd. Het Comité was dan ook van mening dat redelijkerwijze niet mocht worden aangenomen dat de wetgever inzake de meer intrusieve uitzonderlijke methoden op een impliciete wijze zou hebben willen afwijken van het schriftelijke karakter van een beslissing in één of meer van de onderscheiden stadia.

Daarom besloot het Vast Comité I dat het mondelinge karakter van de initiële aanvraag en van het eensluidend advies niet strookte met de letter en de geest van de wet.

III.3.2.2. Motivering van de toelating

III.3.2.2.1. Geen draagkrachtige motivering

In zes dossiers was door de BIM-commissie een schorsing uitgesproken omdat de toelating van het diensthoofd onvoldoende gemotiveerd was om een beoordeling van de wettelijkheid, de proportionaliteit en de subsidiariteit toe te laten. In de vijf eerste gevallen schaarde het Vast Comité I – dat ambtshalve gevat is wanneer de BIM-commissie een methode schorst – zich achter dit oordeel en beval het de stopzetting van de methode. In het zesde geval werd de schorsing opgeheven omdat de betrokken inlichtingendienst na de (terechte) beslissing van de BIM-commissie bijkomende informatie had aangeleverd. In een zevende dossier waarin de motivering van de toelating ter discussie stond, had het Comité zichzelf gevat.

In het eerste dossier (dossier 2011/84) werd een toelating om over te gaan tot de identificatie van de abonnee of gebruiker van een GSM-nummer door de BIM-

commissie geschorst omdat de toelating van het diensthoofd '*ne contient qu'une description succincte des éléments de faits justifiant la décision et par conséquent, ne permettant pas, en son état, à la Commission BIM, de procéder à la vérification des principes de subsidiarité et de proportionnalité*'.[107] Ook het Comité moest vaststellen dat de toelating geen enkel verband deed blijken tussen het geviseerde GSM-nummer en de dreiging: '*La décision ne démontre dès lors aucunement sa légalité, à quoi s'ajoute qu'un tel libellé ne permet nullement d'évaluer le respect les principes de subsidiarité et de proportionnalité.*'[108]

Toen een GSM-toestel toebehorend aan een Belgisch parlementslid in het buitenland spoorloos raakte, wou een inlichtingendienst het toestel lokaliseren via een specifieke methode (dossier 2011/192). Als potentiële dreiging wordt verwezen naar 'inmenging'. Ditmaal schorste de BIM-commissie de methode omdat '*le libellé de la décision ne contient aucune description, même succincte des éléments de faits justifiant la décision.*'[109] Het Comité kwam tot dezelfde vaststelling: de toelating '*ne définit pas concrètement en quoi consisterait la menace potentielle d'ingérence, en ne contient aucune description, même succincte des éléments de faits justifiant la décision.*'[110]

Een derde toelating werd geschorst omdat ze '*onvoldoende toelaat te achterhalen of de regels van de subsidiariteit in concreto gerespecteerd zijn en het daarin opgeworpen verband met de inwendige veiligheid van de staat niet overtuigt.*' (dossier 2011/307) Het Comité voegde daar volgende motivering aan toe: '*Waar een toelating, zoals in casu, geen daadwerkelijk of minstens redelijkerwijs aanneembaar verband tussen een target van een methode en een potentiële bedreiging zoals bedoeld in art. 18/1 W.I&V aangeeft, doch zich stoelt op allusies, zij gebrekkig gemotiveerd is en derhalve uit legaliteitsoogpunt niet genoegzaam met redenen is omkleed. Overwegende dat een en ander evenmin een adequate toetsing toelaat van de principes van proportionaliteit en subsidiariteit.*'

In een vierde dossier (2011/355) wenste de inlichtingendienst op verzoek van een buitenlandse correspondent over te gaan tot de identificatie van de gebruiker van een Belgisch telefoonnummer dat was opgedoken in een terrorismedossier. De toelating werd geschorst omdat ze op bepaalde punten onvoldoende gepreciseerd was: '*l'intérêt à protéger est insuffisamment précisé; l'identité du service étranger est insuffisamment précisée également; aucune information n'est donnée*

---

107 'bevat slechts een summiere beschrijving van de feitelijke elementen die de beslissing rechtvaardigen en daarom de BIM-commissie dan ook niet toelaat over te gaan tot een verificatie van de principes van subsidiariteit en proportionaliteit.' (vrije vertaling).

108 'De toelating toont dan ook op geen enkele wijze aan dat ze wettelijk is. Daarbij komt dat dergelijke bewoordingen op geen enkele wijze toelaten te evalueren of de principes van de proportionaliteit en de subsidiariteit werden nageleefd.' (vrije vertaling).

109 'de toelating geen enkele zelfs summiere beschrijving bevat van de feitelijke elementen die de toelating rechtvaardigen' (vrije vertaling).

110 'motiveert niet in concreto waaruit de potentiële dreiging van inmenging zou bestaan en bevat geen enkele zelfs summiere beschrijving van de feitelijke elementen die de toelating rechtvaardigen.' (vrije vertaling).

sur l'enquête en matière de terrorisme en cours; la proportionnalité et la subsidiarité sont insuffisamment motivées.'[111] Ook het Comité vond in de toelating te weinig elementen om de wettelijkheid, de proportionaliteit en de subsidiariteit *in concreto* te kunnen beoordelen.

In een vijfde dossier (2011/442) – waarin de inlichtingendienst de gebruikers van twee GSM-nummers wenste te identificeren – vond de BIM-commissie alweer '*aucune description, même succincte, des éléments de fait qui la justifiaient*'.[112] Het Comité kwam tot hetzelfde oordeel: de proportionaliteit en de subsidiariteit konden niet geverifieerd worden.

In het laatste dossier dat door de BIM-commissie geschorst was, wenste het diensthoofd een observatie met een technisch middel uit te laten voeren (dossier 2011/724). De commissie oordeelde echter dat '*telle qu'elle est libellée et, particulièrement, en ce que le degré de gravité de la menace potentielle qu'elle décrit n'est pas suffisamment précisé et justifié.*'[113] Het Vast Comité I kon de beweegredenen van de BIM-commissie, op het ogenblik van haar beslissing, slechts bijtreden. Echter, uit bijkomende mondelinge en schriftelijke informatie bleek dat '*van de target, op basis van gedocumenteerde elementen, onmiskenbaar een potentiële dreiging uitgaat tegen een van de belangen vermeld in art. 7 W.I&V.*' en dat '*de methode, waartoe is beslist, in verhouding staat tot de ernst van voormelde dreiging én voldoet aan de proportionaliteits- en subsidiariteitseis*'. Het Comité stelde wel dat '*het evenwel aangewezen ware geweest dat ab initio, in de beslissing zelf, meer omstandig gewag zou zijn gemaakt van de – overigens voorhanden zijnde – elementen die redelijkerwijze noodzakelijk waren om de inschatting van de dreiging, van de proportionaliteit en van de subsidiariteit op een adekwate manier te kunnen bewerkstelligen. Dat een beslissing tot aanwending van een methode op dit vlak voldoende zelfdragend moet zijn, op straffe van niet te voldoen aan de motiveringsverplichting en derhalve tijd en middelen te laten verloren gaan.*'

Ten slotte wenste de inlichtingendienst de oproepgegevens te bekomen van de GSM-nummers van drie onderscheiden personen, alsook van e-mailadressen van één van hen (dossier 2011/522). De beslissing was afdoende gemotiveerd wat betreft één GSM-nummer en de eraan gelinkte e-mailadressen. Maar dat was niet het geval met betrekking tot de GSM-nummers van de twee andere personen. De beslissing was onduidelijk met betrekking tot de bedreiging die de methode moest wettigen in die mate zelfs dat ze de vraag naar de bevoegdheid van de

111 'het te verdedigen belang is onvoldoende gepreciseerd; ook de identiteit van de buitenlandse dienst is onvoldoende gepreciseerd; er wordt geen enkele informatie gegeven over het lopende terrorismeonderzoek; de proportionaliteit en de subsidiariteit zijn onvoldoende gemotiveerd.' (vrije vertaling).

112 'geen enkele omschrijving, zelfs beknopt, van de feitelijke elementen die haar rechtvaardigden' (vrije vertaling).

113 'zoals zij werd opgesteld, en in het bijzonder waar de graad van de ernst van de potentiële dreiging die zij beschrijft niet genoegzaam gepreciseerd en gerechtvaardigd wordt' (vrije vertaling).

betrokken inlichtingendienst deed rijzen. Er werd evenmin een verband gelegd tussen de gebruiker van het éne GSM-nummer en de gebruikers van de twee andere. Op basis van de initiële informatie kon het Vast Comité I geen controle van de wettigheid verrichten. De betrokken inlichtingendienst maakte echter bijkomende documentatie over die aantoonde dat wel degelijk aan de wettelijke bevoegdheids- en dreigingsvoorwaarden was voldaan. Het Comité besloot dan ook tot de wettelijkheid van de methode maar merkte opnieuw op dat '*het evenwel aangewezen ware geweest dat ab initio, in de beslissing zelf, gewag zou zijn gemaakt van die elementen die* in concreto *de bevoegdheid en de bedreiging aantonen inzake elk van de onder methode geplaatste elektronische communicatiemiddelen*'.

III.3.2.2.2. Tegenstrijdigheid in de motivering

Luidens de schriftelijke toelating van het diensthoofd wenste de betrokken inlichtingendienst over te gaan tot de identificatie van de gebruiker van een telefoonnummer (dossier 2011/72). Deze methode staat omschreven in artikel 18/7 § 1, 1° W.I&V ('*de identificatie van de abonnee of de gewone gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel*'). Uit diezelfde toelating bleek echter dat het de bedoeling was om de titularis van een anoniem telefoonnummer te identificeren aan de hand van de communicaties verricht via dit nummer. In werkelijkheid wenste de dienst dus over te gaan tot '*het opsporen van de oproepgegevens van elektronische communicatiemiddelen van waaruit of waarnaar oproepen worden of werden gericht*' (art. 18/8 § 1, 1° W. I&V).

Het Comité oordeelde dat de beweegredenen aangehaald in de toelating van het diensthoofd de inzet van de gekozen methode moeten schragen. Gelet op de interne tegenstrijdigheid in de toelating, was zij niet behoorlijk gemotiveerd en werd de stopzetting van de methode bevolen.

III.3.2.3. Wettelijke (vorm)vereisten bij de uitvoering van een methode

Eens een methode geldig gemachtigd is en desgevallend ter kennis gebracht van de BIM-commissie, kan zij uitgevoerd worden. Maar ook bij deze uitvoering moet soms rekening worden gehouden met bijzondere regels.

III.3.2.3.1. Hoogdringendheidsprocedure bij de vordering van een operator

Artikel 18/8 § 2 W.I&V bepaalt dat in geval van uiterst dringende, met redenen omklede noodzakelijkheid de inlichtingenofficier bij mondelinge beslissing ogenblikkelijk oproepgegevens kan vorderen bij een operator mits voorafgaand mondeling akkoord van het diensthoofd (dossier 2011/227). Zoals vereist, bevestigde het diensthoofd nadien op schriftelijke wijze zijn voorafgaand mondeling akkoord. Deze bevestiging maakte echter niet duidelijk wie de effectief vorde-

rende inlichtingenofficier was, gaf geen indicatie van de datum en het tijdstip waarop de operator werd gevorderd en wees niet uit op welk ogenblik de mondelinge toestemming van het diensthoofd was gegeven. Deze gegevens bleken ook niet uit enig ander stuk waarover het Comité initieel beschikte zodat het onmogelijk was de wettigheid van de vordering te controleren.

In de loop van de procedure verstrekte de betrokken inlichtingendienst echter bijkomende documenten die aantoonden dat aan alle wettelijke voorwaarden was voldaan. Het Vast Comité I stelde dan ook vast dat de methode in overeenstemming was met de bepalingen van de wet. Toch onderlijnde het Comité dat het aangewezen is dat de elementen die *in concreto* aantonen dat de wettelijk vereiste formaliteiten vervuld zijn, *ab initio* in de schriftelijke toelating zelf zouden opgenomen worden.

III.3.2.3.2. Voorafgaandelijke verwittiging van de voorzitter van de Vereniging van Beroepsjournalisten

Omdat de betrokken dienst de oproepgegevens van een communicatiemiddel van een beroepsjournalist wenste te achterhalen, vroeg en bekwam hij het eensluidend advies van de BIM-commissie (dossier 2011/193). Artikel 18/2 § 3 W.I&V bepaalt echter dat '*deze methode niet [mag] uitgevoerd worden zonder dat […] de voorzitter […] van de Vereniging van Beroepsjournalisten hiervan vooraf op de hoogte is gebracht door de voorzitter van de commissie.*' Uit het advies van de BIM-commissie kon echter niet worden opgemaakt of deze formaliteit vervuld was. Navraag leerde dat de BIM-commissie de voorzitter niet had in kennis gesteld. Dit gebeurde pas later, na de opmerking ter zake van het Comité.

Aangezien artikel 18/2 § 3 W.I&V niet preciseert welke vorm deze verwittiging moet aannemen, noch wat moet begrepen worden onder '*de nodige inlichtingen*', oordeelde het Comité dat '*l'affirmation du Président de la Commission BIM que l'avertissement préalable a eu lieu, avec en plus, la précision du jour et de l'heure de cet avertissement préalable et que les "informations nécessaires" ont été données au Président de l'association des journalistes professionnels suffit au regard des exigences légales*'.[114]

De verwittiging van de betrokken voorzitter vormt een substantiële vormvereiste. Daarom oordeelde het Comité dat de eventuele uitvoering van de methode vóór die in kennisstelling onwettig was. De eventueel reeds ingewonnen gegevens moesten dan ook vernietigd worden; de gegevens verkregen vanaf de verwittiging mochten wel geëxploiteerd worden.

---

114 'de bevestiging van de Voorzitter van de BIM-commissie dat de voorafgaandelijke verwittiging heeft plaatsgevonden, met daarbij de precisering van de dag en het uur van deze voorafgaande verwittiging en de melding dat de "nodige inlichtingen" aan de Voorzitter van de Beroepsvereniging van Beroepsjournalisten werden gegeven, volstaat in het licht van de wettelijke vereisten' (vrije vertaling).

Ook in een tweede, vrijwel gelijkaardige zaak (dossier 2011/257) bleek niet uit het eensluidend advies van de BIM-commissie dat de voorzitter van de Vereniging van Beroepsjournalisten was verwittigd. Daarom vroeg het Vast Comité I de BIM-commissie om nadere uitleg. Aangezien de BIM-commissie meldde dat de voorzitter op een gegeven ogenblik '*de nodige inlichtingen*' had verkregen, besloot het Comité tot de wettelijkheid van de uitvoering van de specifieke methode vanaf dat ogenblik.

De problematiek van de kennisgeving kwam in nog twee zaken aan bod (dossiers 2011/761 en 2011/762): een diensthoofd had de toelating verleend om de GSM van buitenlandse maar in België als dusdanig erkende beroepsjournalisten te observeren. De BIM-commissie expliciteerde in haar eensluidende adviezen dat deze specifieke methoden slechts konden uitgevoerd worden nadat zij hiervan kennis had gegeven aan de voorzitter van de Vereniging van Beroepsjournalisten. Deze kennisgevingen gebeurden echter niet onmiddellijk. Het Vast Comité I controleerde een en ander en kwam tot het volgende besluit: '*Attendu qu'il échet de constater que le [service de renseignement] a mis en œuvre une méthode spécifique à l'égard d'un journaliste professionnel avant que le Président de la Commission BIM n'ait informé le Président de l'Association professionnelle des journalistes*'.[115] De gegevens die vóór de kennisgevingen waren verzameld, dienden dan ook te worden vernietigd.

III.3.2.4. Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van de dreiging

De inlichtingendiensten kunnen uiteraard niet zomaar elke methode of techniek inzetten: deze moeten voorzien zijn in de wet, zijn soms gebonden aan tijdslimieten, kunnen niet steeds voor elke dreiging worden ingezet, mogen niet buiten België worden aangewend, enz. In enkele beslissingen verduidelijkte het Vast Comité I deze grenzen.

III.3.2.4.1. Het retroactief opvragen van bankgegevens

De betrokken inlichtingendienst wenste diverse bank-gerelateerde data in te winnen, enerzijds over de afgelopen zes maanden en anderzijds voor de komende zes maanden (dossier 2011/304).

Deze uitzonderlijke methode was gebaseerd op artikel 18/15 W.I&V dat de inlichtingendiensten toelaat bankverrichtingen '*die in een bepaald tijdvak zijn*

[115] 'Overwegende dat het vaststaat dat de [inlichtingendienst] een specifieke methode in uitvoering heeft gebracht ten aanzien van een beroepsjournalist vooraleer de Voorzitter van de BIM-commissie de Voorzitter van de Vereniging van Beroepsjournalisten in kennis had gesteld' (vrije vertaling).

uitgevoerd' op te vorderen zonder dat de wet hierbij een maximumtermijn bepaalt. Artikel 18/10 § 1, tweede lid, W.I&V stelt echter dat '*de periode tijdens welke de uitzonderlijke methode voor het verzamelen van gegevens aangewend mag worden niet langer [mag] duren dan twee maanden*'.

Het Vast Comité I onderzocht de draagwijdte van deze twee bepalingen.

Wat betreft het in *real time* opvragen van (toekomstige) bankgegevens, stelde het Comité dat dit slechts kan voor een periode van maximaal twee maanden vanaf de machtiging. De BIM-Wet laat wel toe dat deze termijn mits een evaluatie verlengd wordt.

Wat betreft het retroactief opvragen van bankgegevens, kwam het Comité tot het besluit dat noch in de wet, noch in de voorbereidende werken een tijdslimiet is vermeld en '*dat de periode alsdan (enkel) wordt beperkt door het beginsel van de proportionaliteit.*' (zie verder III.3.2.5.1)

Deze principsbeslissing werd nadien nog enkele malen bevestigd (dossiers 2011/378, 2011/435 en 2011/436).

III.3.2.4.2. Geen aanduiding van de duur van een methode

Een inlichtingendienst wenste in twee onderscheiden dossiers via een telecomoperator over te gaan tot de kennisname van oproepgegevens van een bepaalde persoon (dossiers 2011/493 en 2011/494). De toelatingen vermeldden wel binnen welke termijn de vordering aan de operator moest worden gericht, maar niet de periode waarvoor de oproepgegevens werden aangevraagd. Na onderzoek door het Vast Comité I bleek echter de wettelijkheid van de methode gegarandeerd.

III.3.2.4.3. Kadert de toelating binnen de wettelijke dreigingen?

Een inlichtingendienst wenste retroactief en voor een korte periode na te gaan welke nummers gebeld hadden naar een bepaald GSM-toestel om vervolgens de verschillende abonnees en titularissen te identificeren (dossier 2011/609). Bijzonder aan deze toelating was dat het GSM-toestel toebehoorde aan een inlichtingenagent van de betrokken dienst zelf en dat hij hiervoor zijn toestemming had verleend. De agent was het slachtoffer van een incident en men wou definitief uitsluitsel over het eventuele maar weinig waarschijnlijke verband tussen dat feit en de dossiers die de agent behandelde. Immers, '*On ne peut toutefois exclure que l'agent et le service soient victimes d'un acte d'intimidation de la part d'une organisation suivie par l'agent dans le cadre des missions qui lui ont été affectées*'[116], aldus de betrokken dienst. Het Vast Comité onderzocht of de finaliteit van de methode effectief kaderde binnen de wettelijke opdracht van de dienst zoals

116 'Men kan evenwel niet uitsluiten dat de agent en de dienst slachtoffer zouden zijn van een daad van intimidatie vanwege een organisatie die door de agent wordt opgevolgd in het kader van de opdrachten die hem zijn toevertrouwd' (vrije vertaling).

omschreven in de wet van 30 november 1998. Het Comité maakte volgende redenering: '*Attendu qu'il en ressort que la finalité de la méthode spécifique envisagée est surtout de vérifier que la sécurité d'un agent de [renseignement] n'a pas été compromise dans l'exercice d'une de ses missions; Qu'une telle finalité de sécurité n'est pas, en soi, l'une des missions visées [par] la Loi R&S; Attendu toutefois qu'en voulant vérifier si son agent a été victime ou non d'un acte d'intimidation, [le service] cherche aussi la trace d'une activité éventuelle qui pourrait menacer la sûreté intérieure de l'Etat* '.[117]

III.3.2.4.4. De draagwijdte van het begrip 'post'

Een inlichtingendienst wenste gedurende twee maanden over te gaan tot kennisname van post- en postbusidentificatiegegevens van afzender(s) en bestemmeling(en) van al dan niet aan postoperators toevertrouwde postpakketten (dossier 2011/659). Artikel 3, 13° W.I&V omschrijft '*post*' als '*de postzending zoals gedefinieerd in artikel 131, 6°, 7° en 11°, van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven*'. Dit artikel 131 van de Wet van 21 maart 1991 werd echter gewijzigd na de inwerkingtreding van de BIM-Wet van 4 februari 2010. Bij artikel 5 van de Wet van 13 december 2010 (*BS* 31 december 2010) ondergingen zowel de volgorde als de definitie van diverse begrippen wijzigingen. Het Vast Comité I oordeelde echter dat die wijzigingen niet gelden ten aanzien van de inhoud die het begrip 'post' gekregen heeft in de BIM-Wet van 4 februari 2010. Hiervoor gelden nog steeds de definities uit artikel 131, 6°, 7° en 11°, van de Wet van 21 maart 1991 zoals die golden ten tijde van de inwerkingtreding van de BIM-Wet van 4 februari 2010.

III.3.2.4.5. Identificatie van onwettelijk verkregen oproepgegevens

Zoals hoger uiteengezet (zie III.3.2.1.1) stelde het Comité vast dat een inlichtingendienst was overgegaan tot de kennisname van de oproepgegevens van een mobiel én een vast telefoonnummer, terwijl de toelating alleen betrekking had op het mobiele nummer. De 'observatie' van de vaste lijn werd dan ook vernietigd en er volgde een verbod om de verkregen gegevens te gebruiken. Het betrokken diensthoofd had derhalve nadien evenmin toelating mogen verlenen om over te gaan tot de identificatie van de oproepgegevens van de vaste lijn. De identificatie van de oproepgegevens van de mobiele lijn was wel toegestaan (dossier 2011/501b).

117 'Overwegende dat hieruit blijkt dat de finaliteit van de bedoelde specifieke methode er in de eerste plaats in bestaat om te verifiëren of de veiligheid van een inlichtingenagent niet werd gecompromitteerd in de uitoefening van een van zijn opdrachten; Dat een dergelijke veiligheidsfinaliteit op zichzelf niet kadert binnen een van de opdrachten bedoeld in de W.I&V; Overwegende evenwel dat door te willen controleren of zijn agent ja dan neen slachtoffer was van een intimidatie, de dienst ook onderzoek doet naar een spoor van een eventuele activiteit die de interne veiligheid van het land zou kunnen bedreigen.' (vrije vertaling).

III.3.2.5. De proportionaliteitseis

Het Comité sprak zich verschillende malen uit over de vraag of een toegelaten methode in verhouding stond met de ernst van de dreiging.

III.3.2.5.1. Het retroactief opvragen van bankgegevens

Zoals hiervoor gesteld, aanvaardde het Comité het retroactief opvragen van bankgegevens voor een periode van meer dan twee maanden, onder de voorwaarde dat de periode proportioneel is met de ernst van de dreiging. In vier onderscheiden dossiers – die allen betrekking hadden op 'spionage' – heeft het Comité zich uitgesproken over deze problematiek. In het algemeen stelde het Comité dat '*la vérification du respect des principes de proportionnalité et de subsidiarité exige néanmoins que la durée de la période du passé visée par la collecte de données bancaires soit motivée par le service de renseignement de manière telle qu'elle permette au Comité permanent R d'en apprécier la justification en fonction de la gravité de la menace potentielle; cette appréciation doit être effectuée dans chaque cas en fonction des circonstances particulières justifiant la mise en œuvre de la méthode exceptionnelle*'.[118]

Er werden respectievelijk gegevens opgevraagd voor een periode van zes maanden (dossier 2011/403), acht maanden (dossier 2011/378), meer dan vijf jaar (dossier 2011/436) en meer dan vijftien jaar (dossier 2011/435). Daarbij kon het Comité vaststellen dat de motivering van de inlichtingendienst uitgebreider en meer nauwkeurig werd, naarmate de duur van de aangevraagde periode langer was. Alleen in het eerste geval was de keuze voor de periode niet gemotiveerd. Hier oordeelde het Comité evenwel dat het nuttig in kaart brengen van de financiële transacties en contacten van de geviseerde rekeningenhouders met het oog op het blootleggen van hun netwerk, een voldoende lang volgehouden inspanning vergde. *In casu* kwam de periode van een half jaar dan ook aanvaardbaar voor.

III.3.2.5.2. Afluisteren van nog niet gekende nummers

De betrokken dienst wenste alle gekende telefoontoestellen van een *target* af te luisteren (dossier 2011/322). Daarenboven wilde ze die toelating ook verlenen voor '*numéros non encore connus et a fortiori non encore identifiés qui apparaîtrai-*

118 'het nazicht van de naleving van de principes van proportionaliteit en subsidiariteit vereist echter dat de duur van de afgelopen periode waarop de inzameling van bankgegevens betrekking heeft, dermate wordt gemotiveerd door de inlichtingendienst dat het Vast Comité I bij machte is te beoordelen of deze periode gerechtvaardigd is in het licht van de ernst van de dreiging; deze beoordeling moet in elk dossier gebeuren in functie van de bijzondere omstandigheden die de uitvoering van de uitzonderlijke methode rechtvaardigen' (vrije vertaling).

ent dans le cadre de l'exécution d'une autre méthode spécifique'[119], maar die gebruikt werden door dezelfde *target*.

Het Comité bekeek de toelating voor de nog niet gekende nummers vanuit het oogpunt van de proportionaliteit. Het kon vaststellen dat de inlichtingendienst zeer precies had geformuleerd waarom zij deze methode wenste aan te wenden. Daaruit bleek dat zelfs de in de wet voorziene urgentieprocedure in dit uitzonderlijke geval geen soelaas zou kunnen bieden. Om die reden besloot het Comité tot de wettelijkheid van de methode.

III.3.2.5.3. De duur van de observatie van een private plaats

De inlichtingendienst wenste gedurende twee maanden een private plaats te observeren (dossier 2011/434). Daar zou een bijeenkomst plaatsvinden van een groepering die zijn interesse wegdroeg. Maar de duur van die bijeenkomst was uiteraard beperkt in de tijd: '*Considérant dès lors qu'une durée d'observation de deux mois excède la période au cours de laquelle l'événement à observer doit se dérouler*'[120] was de maatregel niet proportioneel zodat de methode gedeeltelijk vernietigd werd.

III.3.2.5.4. Kennisname van oproepgegevens van een niet-gekend nummer

De BIM-commissie had de kennisname van oproepgegevens van een GSM en de navolgende identificatie van de betrokken titularissen geschorst (dossier 2011/474). Reden was dat op het ogenblik dat de specifieke methode werd toegelaten wel de titularis van het GSM-toestel gekend was, maar niet diens nummer. Dat nummer kon pas gekend zijn na analyse van de resultaten van twee andere specifieke methoden. De BIM-commissie was van oordeel dat de toelating van de betrokken inlichtingendienst op die wijze niet toeliet om na te gaan of de proportionaliteit en meer in het bijzonder de subsidiariteit waren nageleefd. Het Vast Comité I oordeelde echter dat het in deze zaak niet nodig was om vooraf het nummer van de GSM te kennen om de proportionaliteit te beoordelen '*puisque l'on connait l'identité de son titulaire (à savoir la cible) et les circonstances qui motivent le recours à cette méthode*'.[121]

III.3.2.6. De subsidiariteitseis

Vier beslissingen betroffen de vraag of het door een methode beoogde doel ook op een minder ingrijpende manier kon bereikt worden.

---

119 'nummers die nog niet gekend en a fortiori nog niet geïdentificeerd zijn en die aan het licht zouden komen in het kader van de uitvoering van een andere specifieke methode' (vrije vertaling).

120 'Overwegende daarom dat een observatieduur van twee maanden de periode overstijgt gedurende dewelke het te observeren evenement zal plaatsvinden' (vrije vertaling).

121 'omdat men de identiteit kent van de titularis (te weten de *target*) en de omstandigheden die het beroep op deze methode motiveren' (vrije vertaling).

Zoals hoger reeds vermeld, wenste een inlichtingendienst een specifieke methode in te zetten om de verloren GSM van een Belgisch parlementslid te traceren. De toelating was naar het oordeel van het Comité niet alleen onvoldoende gemotiveerd (zie III.3.2.2.1.), ook was niet voldaan aan de subsidiariteitseis: het doel, met name de gegevens die op de GSM staan beschermen, kon immers ook bereikt worden door een eenvoudige tussenkomst van de operator en dus zonder de inzet van een specifieke methode.

In de tweede zaak, die hierboven ook reeds aan bod kwam (zie III.3.2.5.1), wilde de betrokken inlichtingendienst bankgegevens controleren die betrekking hadden op een zeer lange periode (meer dan 15 jaar). De *targets* werden verdacht van spionage in binnen- en buitenland. Aangezien *in casu* de enige mogelijkheid om het netwerk en de *modus operandi* van deze personen te kennen, erin bestond hun bankrekeningen te bestuderen vanaf hun verblijf in België, was *in casu* voldaan aan de subsidiariteitseis.

In de derde zaak wou de betrokken inlichtingendienst overgaan tot de kennisname van oproepgegevens van en naar een faxtoestel dat werd gebruikt door een onderzoekscentrum (dossier 2011/484). De bedoeling was na te gaan of dit centrum een uitnodiging had gekregen om deel te nemen aan een internationale conferentie over spitstechnologie in een land dat opgevolgd wordt in het kader van de strijd tegen proliferatie. De inlichtingendienst stelde dat het onmogelijk was om via gewone methoden op korte termijn bevestiging te krijgen van het feit dat het centrum effectief een uitnodiging had ontvangen. Bijgevolg oordeelde het diensthoofd dat de aanwending van deze specifieke methode onontbeerlijk was. Alhoewel het Vast Comité I vaststelde dat de inlichtingendienst niet buiten zijn wettelijk mandaat trad (*in casu* betrof het immers de strijd tegen proliferatie), concludeerde het toch dat de inzet van een gewone methode '*ne paraît pas insurmontable en l'occurrence*'.[122] Dit bleek nadien ook uit de feiten: aangezien de specifieke methode geen uitsluitsel gaf, wendde de inlichtingendienst zich met zijn vraag rechtstreeks tot het betrokken centrum. Mede gelet op het feit dat het onderzoekscentrum geen *target* is van de inlichtingendienst maar eerder een mogelijk slachtoffer van benaderingen door bepaalde landen, stelde het Comité dat het subsidiariteitsprincipe niet was nageleefd.

In een laatste dossier had het diensthoofd van de inlichtingendienst de toelating verleend om, naast het opsporen van communicatiegegevens, onmiddellijk over te gaan de identificatie van bepaalde telefoonnummers (dossier 2011/830 – zie ook III.3.2.1.1). De BIM-commissie had echter vastgesteld dat zijzelf via het nummer 1207 een deel van de nummers kon identificeren (met name bepaalde vaste telefoonnummers). Er was dus niet voldaan aan de subsidiariteitsvoorwaarde. Het Vast Comité I onderschreef het oordeel van de BIM-commissie maar preciseerde dat het subsidiariteitsgebrek van de beslissing enkel de vaste telefoonnummers behelsde en niet de mobiele nummers.

122 'lijkt niet onoverkomelijk in dit geval' (vrije vertaling).

III.4. CONCLUSIES

Wat betreft het eerste werkjaar waarin de BIM-Wet volledig in uitvoering was, formuleerde het Vast Comité I volgende algemene conclusies:

- de nieuwe controletaak die het Comité kreeg toebedeeld, vergt een aanzienlijke investering van tijd en middelen maar ze levert op twee vlakken een duidelijke meerwaarde. Vooreerst draagt het Comité bij tot de rechtmatigheid van het optreden van de VSSE en van de ADIV en, op die manier, tot de bescherming van de fundamentele rechten en vrijheden. Anderzijds laat de BIM-controle toe een meer volledig beeld te krijgen van de werking van de inlichtingendiensten hetgeen de reguliere controleopdracht van het Comité zeker ten goede komt;
- de VSSE lijkt de nieuwe mogelijkheden om bijzondere inlichtingenmethoden in te zetten op een evenwichtige manier te benutten. Haar gebruik van uitzonderlijke methoden, die zeer intrusief zijn, geschiedt conform de wet slechts 'bij uitzondering'. De dienst besteedt ook de nodige zorg aan de redactie van de toelatingen en machtigingen (goede motivering en contextualisering), ook al betekent dit een aanzienlijke administratieve werklast;
- voor de ADIV kunnen nog niet dezelfde conclusies worden getrokken. Ondanks het geringe aantal toelatingen is de redactie ervan niet steeds even accuraat al levert de dienst inspanningen om hieraan te verhelpen. Het Vast Comité I zal in de toekomst specifieke aandacht besteden aan deze vaststelling;
- momenteel is het nog niet mogelijk om nuttig te rapporteren omtrent de via bijzondere methoden 'behaalde resultaten';
- de wet biedt geen duidelijk, uniform en werkbaar kader voor de inzet van bijzondere methoden in hoogdringende situaties (zie III.1.1, III.2.1.1, III.3.2.1.7 en III.3.2.3.1).

HOOFDSTUK IV.
HET TOEZICHT OP DE INTERCEPTIE VAN COMMUNICATIE UITGEZONDEN IN HET BUITENLAND

Sinds begin 2011 kunnen zowel de VSSE als de ADIV onder zeer strikte voorwaarden communicaties afluisteren, er kennis van nemen en ze registreren (art. 18/17 § 1 W.I&V). Dergelijke 'veiligheidsintercepties' behoeven principieel een voorafgaand aval van de BIM-commissie en zijn steeds onderworpen aan het jurisdictionele toezicht van het Vast Comité I.[123] Ze kunnen overigens alleen gemachtigd worden voor methoden die worden ingezet '*op het grondgebied van het Rijk*' (art. 18/1 W.I8&V).

De 'BIM-intercepties' moeten duidelijk worden onderscheiden van '*het zoeken*[124]*, het onderscheppen, het afluisteren, het kennisnemen of het opnemen door de Algemene Dienst inlichting en veiligheid van de Krijgsmacht van elke vorm van communicatie uitgezonden in het buitenland*.' Deze vorm van afluisteren kan zowel om redenen van militaire aard in het kader van de opdrachten gedefinieerd in artikel 11 § 2, 1° en 2°, W.I&V als om redenen van veiligheid en bescherming van Belgische en van geallieerde troepen tijdens opdrachten in het buitenland alsook van onze onderdanen die in het buitenland gevestigd zijn (art. 11 § 2, 3° en 4° W.I&V). Ook dit worden klassiek 'veiligheidsintercepties' genoemd, maar zij kennen een volkomen ander controlekader. Het toezicht erop is namelijk uitsluitend opgedragen aan het Vast Comité I, en dit zowel voor, tijdens als na de intercepties (art. 44*bis* W.I&V). Het Comité heeft hierbij de bevoegdheid om lopende intercepties te doen stopzetten wanneer blijkt dat de voorwaarden waarin ze uitgevoerd worden, de wettelijke bepalingen en/of de ministeriële toelating niet respecteren (art. 44*ter* W.I&V). Elk jaar, begin december, dient de ADIV immers aan de minister van Landsverdediging zijn gemotiveerde lijst voor te leggen met organisaties of instellingen, van wie de communicatie het komende jaar mag onderschept worden. Dit gebeurt met het oog op de ministeriële toelating van deze intercepties. De minister dient zijn beslissing te nemen binnen tien werkdagen en moet ze vervolgens meedelen aan de ADIV. Nadien moeten zowel de lijst als de ministeriële toelating door de ADIV worden overgezonden aan het Vast

123 Zie hierover uitvoerig Hoofdstuk III van het *Activiteitenverslag 2010*, p. 51-73.

124 De wettelijke mogelijkheid tot zoeken werd pas ingevoerd in 2010.

Comité I. Aan de hand van deze jaarlijkse lijst voert het Comité zijn 'controle voorafgaand aan de interceptie' uit.

Vorig jaar drong het Comité er op aan nauwgezet de wettelijke termijnen te respecteren. Voor 2011 beschikte het Comité tijdig over de vereiste documenten. Ook werden de door het Comité gevraagde SIGINT[125]-procesbeschrijvingen in de loop van 2011 gefinaliseerd.[126]

Zoals vereist door de wet, werden in 2011 installaties waar de ADIV intercepties uitvoert (onaangekondigd) bezocht door het Comité. Daarbij werd het logboek geverifieerd. Tevens werden de aanwezigheden en het gebruik en de beveiliging van de lokalen gecontroleerd.

Het Comité heeft niet kunnen vaststellen dat er communicaties werden afgeluisterd en geëxploiteerd die niet overeenstemden met de door de minister van Landsverdediging goedgekeurde lijst. Evenmin kwamen bij de controle van het logboek onregelmatigheden aan het licht. Wel merkte het Comité op dat de interceptielijst ook een 'fenomeen' vermeldde. Echter, het afluisteren en kennis nemen van communicatie is slechts toegelaten indien dit betrekking heeft op 'organisaties en instellingen' (art. 44*bis* W.I&V) en uiteraard in zoverre dit kadert binnen de opdrachten van de ADIV. De dienst benadrukte hiermee rekening te zullen houden bij de redactie van zijn volgende beluisteringsplan.

125 *Signals Intelligence*.
126 Het Comité had hier reeds meermaals op aangedrongen. Zie ook Hoofdstuk I.1.8.

HOOFDSTUK V.
ADVIEZEN, STUDIES EN ANDERE ACTIVITEITEN

In dit hoofdstuk wordt vooreerst stilgestaan bij de adviesverlenende opdracht van het Vast Comité I. In 2011 verleende het Comité drie specifieke adviezen onder de vorm van een juridische analyse, een voorstel van resolutie en een ontwerp van Koninklijk besluit (V.1 tot V.3). Daarnaast worden enkele andere activiteiten toegelicht die een belangrijke impact hadden op de werking van het Comité (V.4 tot V.7).

V.1. DE WETTELIJKE REGELING INZAKE ARCHIVERING EN VERNIETIGING VAN GEGEVENS VAN DE VSSE EN DE ADIV

Na verloop van tijd verliezen ingezamelde en verwerkte gegevens veelal hun waarde voor de inlichtingendiensten. Op dat moment moet worden beslist of zij worden vernietigd dan wel gearchiveerd.

Deze thematiek wordt voornamelijk geregeld in de Archiefwet van 24 juni 1955 en in zijn uitvoeringsbesluiten.[127] Maar, zeker in relatie tot de inlichtingendiensten zijn er tal van andere relevante wetten op dat vlak: de Wet Verwerking Persoonsgegevens van 8 december 1992, de Wet betreffende de openbaarheid van bestuur van 11 april 1994, de Classificatiewet van 11 december 1998 en de Wet op de inlichtingen- en veiligheidsdiensten van 30 november 1998.

Omdat de toepassing van deze wetgeving onvermijdelijk implicaties heeft op de efficiënte werking van de inlichtingendiensten en op de privacy van diegenen die opgenomen zijn in de bestanden van deze diensten, wijdde het Vast Comité een juridische analyse aan dit thema. Ze werd midden september 2011 toegezonden aan de VSSE en de ADIV.

[127] K.B. van 18 augustus 2010 tot uitvoering van artikelen 1, 5 en 6*bis* van de Archiefwet van 24 juni 1955 (K.B. Archiefwet I) en K.B. van 18 augustus 2010 tot uitvoering van artikelen 5 en 6 van de Archiefwet van 24 juni 1955 (K.B. Archiefwet II).

De analyse[128] toonde aan dat de verschillende wetten – die elk een deelaspect regelen van de problematiek van het vernietigen en archiveren van documenten van inlichtingendiensten – complementair én werkbaar zijn omdat het toepassingsgebied van de Archiefwet beperkt is tot de zogenaamde 'dode archieven'. Het Vast Comité I oordeelde bovendien dat de diverse in het geding zijnde belangen perfect te verzoenen zijn indien de inlichtingendiensten de geest en de letter van de verschillende bepalingen naleven (bijvoorbeeld door documenten die geen nut meer hebben ook als dusdanig aan te duiden en informatie, indien mogelijk, te declassificeren). Wel toonde het Comité zich voorstander van een systeem waarbij classificaties na een bepaalde termijn – bijvoorbeeld 30 jaar voor documenten die als 'geheim' zijn geclassificeerd en 50 jaar voor 'zeer geheime' documenten – van rechtswege vervallen, tenzij zij expliciet worden hernieuwd. Dit vereist echter een aanpassing van de Classificatiewet.

V.2. ADVIES INZAKE DREIGINGSANALYSES VOOR PRIVATE ONDERNEMINGEN

In een gemeenschappelijk toezichtonderzoek uit 2009 oordeelden de Vaste Comités P en I dat het niet evident was dat het Coördinatieorgaan voor de dreigingsanalyse (OCAD) evaluaties inzake extremisme en terrorisme meedeelde aan private ondernemingen. Dit gelet op de artikelen 3 en 10 van de Wet van 10 juli 2006 betreffende de analyse van de dreiging (W.OCAD).[129]

Naar aanleiding van de parlementaire bespreking van het *Activiteitenverslag 2010* van het Vast Comité I oordeelden de Begeleidingscommissies van de Kamer en de Senaat dat het opportuun zou zijn dat bedrijven die Belgen tewerkstellen in het buitenland, alsnog kennis kunnen krijgen van bepaalde evaluaties inzake terroristische en extremistische dreigingen. De Begeleidingscommissies vroegen de Comités daarom een voorstel van reglementering uit te werken die aan deze bekommernis tegemoet kon komen.

De Comités stelden een ontwerp van reglementering op dat het OCAD moet toelaten een punctuele evaluatie uit te voeren op verzoek van de betrokken bedrijven.[130] De minister van Buitenlandse Zaken zou dan beoordelen of de gemotiveerde vraag van de onderneming beantwoordt aan de wettelijke opdracht van het OCAD. Tevens werd de mogelijkheid ingebouwd om ondernemingen in ken-

---

128 Voor de integrale versie van deze analyse verwijzen we naar de Bijlage D van onderhavig activiteitenverslag ('De wettelijke regeling inzake archivering en vernietiging van gegevens van de VSSE en de ADIV').

129 VAST COMITÉ I, *Activiteitenverslag 2010*, 42-43.

130 Om aan de problematiek te verhelpen bleek het niet noodzakelijk om de Wet van 10 juli 2006 te wijzigen. De Comités stelden voor een 'Hoofdstuk I*bis*' in te voeren in het Koninklijk besluit van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging.

nis te stellen van de resultaten van bepaalde evaluaties en dit met respect voor de vertrouwelijkheid van geclassificeerde informatie. Het ontwerp werd toegezonden aan de Voorzitters van Kamer en Senaat.

V.3. VOORSTEL VAN RESOLUTIE INZAKE DE BEVEILIGING VAN INFORMATIE- EN COMMUNICATIESYSTEMEN

Midden 2011 stelde het Comité zijn toezichtonderzoek '*naar de houding van de Belgische inlichtingendiensten tegenover de noodzaak om informatie- en communicatiesystemen te beschermen tegen intercepties en cyberaanvallen uit het buitenland*' (zie II.2) voor aan de Begeleidingscommissie van de Senaat. Daaruit was onder meer gebleken dat de bedreigingen waaraan de Belgische informatie- en communicatiesystemen bloot staan, afbreuk kunnen doen aan de veiligheid en de fundamentele belangen van de Staat. Het ontbrak ook aan een globale federale strategie voor de beveiliging van informatie- en communicatiesystemen.

Naar aanleiding van de bespreking van de onderzoeksresultaten, uitte de Senaatscommissie haar voornemen om deze bij de regering aan te kaarten. Ze vroeg het Comité om ter zake een nota uit te werken.

Deze omvatte de vraag aan de regering om een federale strategie voor de beveiliging van informatie- en communicatiesystemen uit te werken, om daartoe een agentschap op te richten en om een overheid aan te duiden die belast zou zijn met de certificatie en homologatie van systemen die gevoelige informatie verwerken. Het regeerakkoord van 1 december 2011 verwoordde dit als volgt: '*De regering zal, met eerbied voor de privacy, een federaal veiligheidsbeleid inzake informatienetwerken en -systemen uitwerken en zo de aanbevelingen van het Comité I volgen.*'

V.4. INFORMATIEDOSSIERS

Naast toezichtonderzoeken, opent het Vast Comité I ook zogenaamde informatiedossiers. De bedoeling hiervan is om een gestructureerde respons te bieden op elementen met betrekking tot de werking van de inlichtingendiensten en het OCAD die vanuit diverse hoeken worden aangedragen.[131] Deze dossiers en de wijze waarop ze worden behandeld, bieden het voordeel dat er met een minimum

[131] De aanleiding voor het opstarten van informatiedossiers is zeer divers: er wordt een klacht neergelegd en het Vast Comité I wil via een snelle verificatie de manifeste ongegrondheid zo snel als mogelijk uitsluiten; de directie van een inlichtingendienst maakt melding van een incident en het Comité wil nagaan hoe het werd afgehandeld; de media melden een voorval en het Comité wil weten of dit strookt met de realiteit en of er een meer algemene problematiek achter schuilgaat…

aan vormvereisten een brede opvolging van de inlichtingensector kan geschieden. Mochten dergelijke dossiers aanwijzingen van disfuncties aan het licht brengen of van aspecten van de werking van inlichtingendiensten die nader onderzoek behoeven, gaat het Comité uiteraard over tot het initiëren van een toezichtonderzoek. Indien echter duidelijk is dat een dergelijk onderzoek geen meerwaarde ressorteert vanuit de doelstellingen van het Vast Comité I, wordt het informatiedossier gesloten.

In 2011 werd in dit kader aandacht besteed aan diverse geïsoleerde voorvallen bij de inlichtingendiensten (bijvoorbeeld veiligheidsincidenten), aan bepaalde aspecten van de werking van de Dienst Protectie van de VSSE en aan de problematiek van het lidmaatschap van een criminele motorbende in het licht van de reglementering inzake veiligheidsmachtigingen.

V.5. DE CONFERENTIE VAN EUROPESE TOEZICHTHOUDERS EN HET *EUROPEAN NETWORK OF NATIONAL INTELLIGENCE REVIEWERS* (ENNIR)

De *7de Conferentie van de parlementaire commissies van toezicht op de inlichtingen- en veiligheidsdiensten van de Lidstaten van de Europese Unie, Noorwegen en Zwitserland* vond plaats op 27 en 28 oktober 2011 in Berlijn. Zowat twintig delegaties namen deel aan deze conferentie. Er werden debatten georganiseerd rond thema's als de uitdagingen voor de inlichtingendiensten twintig jaar na de Koude Oorlog; het recht op informatie van parlementsleden in het kader van de activiteiten van inlichtingendiensten; de parlementaire controle op inlichtingenactiviteiten (concurrentie of complementariteit van administratieve en parlementaire controle, bevoegdheden, middelen…); de parlementaire controle op nationaal vlak *versus* de internationale samenwerking tussen inlichtingendiensten.

Door de Belgische delegatie werden de stappen toegelicht die waren gezet in het kader van de realisatie van het *European Network of National Intelligence Reviewers (ENNIR)*.[132] Dit betreft een door het Vast Comité I gelanceerd project met betrekking tot een netwerk – in de vorm van een gemeenschappelijke website – voor de uitwisseling van informatie tussen de parlementaire commissies en/of toezichtsorganen op de inlichtingen- en veiligheidsdiensten in de Europese Unie. De delegatie, samengesteld uit twee Senatoren van de Begeleidingscommissie en vertegenwoordigers van het Vast Comité I, stelde tijdens de conferentie ook een ontwerp van *guidelines* voor. In de 'Declaration of Berlin' verklaarden de diverse deelnemers zich akkoord om in dit Belgisch initiatief actief te participeren

[132] Eerder werden de diverse deelnemers bereid gevonden om in de loop van 2011 aan de verdere ontwikkeling van dit initiatief mee te werken. Zie hierover VAST COMITÉ I, *Activiteitenverslag 2010*, 81-82 en bijlage D. De oprichting van ENNIR werd tevens besproken op de *EU Speakers Conference* die plaatsvond op 3 tot 5 april 2011 in het Belgische parlement (www.europarl.europa.eu/webnp/cms/pid/1593).

en het verder mee te ontwikkelen. De internetsite *(www.ennir.be)* werd op 12 december 2011 geactiveerd; ter promotie van het netwerk werd een folder verspreid naar alle lidstaten van de Europese Unie, Noorwegen en Zwitserland. Met resultaat, gezien ondertussen naast België, ook Nederland, Luxemburg en Portugal formeel hun medewerking aan dit initiatief toezegden, terwijl nog tal van andere landen hun belangstelling toonden.

V.6. MEDEWERKING AAN EEN EUROPESE STUDIE INZAKE PARLEMENTAIRE CONTROLE OP DE INLICHTINGENDIENSTEN

In opdracht van het Europese Parlement voerde het *Geneva Centre for the Democratic Control of Armed Forces (DCAF)* samen met het *European University Institute (EUI)* een studie uit naar '*Parliamentary Oversight of Security and Intelligence Agencies in the European Union*'.[133] Dit onderzoek evalueerde het toezicht over nationale inlichtingen- en veiligheidsdiensten door parlementen en door gespecialiseerde niet-parlementaire toezichtorganen. Het doel was om *good practices* te identificeren zodat het Europese Parlement haar eigen toezicht op Europol, Eurojust, Frontex en Sitcen kan verbeteren.

Het Vast Comité I werd nauw betrokken bij deze studie. Vooreerst werd het gevraagd een uitgebreide vragenlijst te beantwoorden over zijn opdrachten, bevoegdheden en middelen. Verder maakte het Comité deel uit van de *Project advisory board* en formuleerde het in deze hoedanigheid zijn bedenkingen bij diverse andere bijdragen tot de studie.[134]

V.7. EXPERT OP DIVERSE FORA

Zoals in de vorige jaren, werd het Vast Comité I opnieuw diverse malen gesolliciteerd als expert op nationale en internationale fora.

Op internationaal vlak werd begin mei 2011 ingegaan op de uitnodiging van het *Open Society Justice Initiative* in Genève om deel te nemen aan een besloten conferentie waarin onder meer de informatiepositie van controleorganen onder de loep werd genomen.

---

133 A. WILLS en M. VERMEULEN, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union*, 2011, 442 p. (www.europarl.europa.eu/activities/committees/studies.do?language=EN).

134 België werd, naast elf andere landen, uitgekozen om meer in detail te beschrijven op welke wijze de parlementaire en gespecialiseerde controle op de inlichtingendiensten verloopt. Zie hierover W. VAN LAETHEM, 'Parliamentary And Specialised Oversight of Security And Intelligence Agencies In Belgium', in A. WILLS en M. VERMEULEN (eds.), *Parliamentary Oversight Of Security And Intelligence Agencies In The European Union*, 2011, 191-203.

In het verlengde daarvan werd in december 2011 ingegaan op een uitnodiging van de Nederlandse Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), het *Geneva Centre for the Democratic Control of Armed Forces* (DCAF) en het *Clingendael Institute* om, samen met een beperkt aantal andere Europese toezichtorganen, een toelichting te geven over de praktische organisatie van toezicht op inlichtingendiensten aan een delegatie vanuit de Balkan ('*Strenghtening Intelligence Oversight in the Western Balkans',* Den Haag).

Ook werd, samen met de collega's van de Nederlandse, Noorse en Zweedse toezichtorganen, halfweg maart in Den Haag een besloten werkvergadering georganiseerd met het oog op de onderlinge uitwisseling van *best practices*.

Het Vast Comité I droeg verder ook bij aan de organisatie van de *Community of Interest on the Practice and Organization of Intelligence (COI POI*[135]*)* die plaatsvond in Antwerpen (oktober 2011). Het centrale thema daar was *'Analytic Management for Surprise and Crisis Response';* een vertegenwoordiger van het Vast Comité I leverde een bijdrage inzake *'Oversight Perspectives on Surprise and Crisis Response'*.

Op bilateraal niveau werd deelgenomen aan de *Groupe européen de recherche sur l'éthique du renseignement (GERER).* Deze werkgroep werd opgericht op initiatief van de Franse *Ecoles de Saint-Cyr Coëtquidan* en de Koninklijke Militaire School (KMS) en wordt gesteund door de *Fondation Saint-Cyr.* Ze is samengesteld uit vertegenwoordigers vanuit het academische milieu en practici (vertegenwoordigers vanuit de Franse (militaire) en Belgische inlichtingendiensten, het Vast Comité I…) en wil reflecteren over de relatie 'ethiek – inlichtingen'. De werkzaamheden van de werkgroep resulteerden in 2011 in een eerste publicatie.[136]

In eigen land zorgde het Vast Comité I mee voor de 'doorstart' van het *Belgian Intelligence Studies Centre (BISC).* Dit centrum voor inlichtingenstudies wil de inlichtingen- en veiligheidsdiensten en de wetenschappelijke gemeenschap dichter bij elkaar brengen en een bijdrage leveren aan het oplossen van maatschappelijke inlichtingenvraagstukken. In die zin organiseerde het BISC twee studienamiddagen: in maart 2011 over 'Inlichtingen- en veiligheidsdiensten: geschiedenis en vooruitblik', en in december over 'Ethiek en inlichtingen: oxymoron?'.

Ten slotte werden de werkzaamheden in de zogenaamde Werkgroep Analyse verder gezet. De werkgroep, die is samengesteld uit vertegenwoordigers van de VSSE en de ADIV en de steun geniet van het Vast Comité I, boog zich over de voorstellen inzake de opleiding (basis en gevorderd) voor analisten voor zowel de burgerlijke als de militaire inlichtingendienst.

---

135 Zie hierover VAST COMITÉ I, *Activiteitenverslag 2008,* 88-89.

136 Groupe Européen de Recherche en Ethique et Renseignement (GERER), sous la direction de T. PICHEVIN, *Ethique et renseignement. La difficile cohabitation bu bien et de la nécessité*, Paris, Editions ESKA, 2011, 141.

V.8. ACADEMISCHE ZITTING

De traditionele jaarlijkse academische zitting van het Vast Comité I had in 2011 als thema de controle op de bijzondere inlichtingenmethoden. Daarbij waren drie niveaus aan de orde. Met Rémi Récio, Délégué général van de *Commission nationale de contrôle des interceptions de sécurité* (CNCIS) werd over de grens gekeken naar de wijze waarop Frankrijk het toezicht op intercepties organiseert. Voor een internationale invalshoek, kon het Comité een beroep doen op *UN Special Rapporteur on the Protection of Human Rights While Countering Terrorism*, professor Martin Scheinin. Peter De Smet, Raadsheer bij het Vast Comité I, lichtte op zijn beurt de resultaten toe van de eerste vier maanden BIM-werking.

HOOFDSTUK VI.
DE OPSPORINGS- EN GERECHTELIJKE ONDERZOEKEN

Naast zijn medewerking aan de toezichtonderzoeken, voert de Dienst Enquêtes I van het Comité ook onderzoeken naar leden van de inlichtingendiensten die verdacht worden van een misdaad of wanbedrijf. Dit doet de enquêtedienst in opdracht van de gerechtelijke overheden. Deze bevoegdheid staat omschreven in artikel 40, derde lid van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse. Met de Wet van 10 juli 2006 betreffende de analyse van de dreiging werd deze bevoegdheid uitgebreid tot misdaden of wanbedrijven gepleegd door de leden van het Coördinatieorgaan voor de dreigingsanalyse (OCAD). Wat betreft de leden van de andere 'ondersteunende diensten' geldt deze bepaling alleen ten aanzien van de verplichting om relevante inlichtingen aan het OCAD mee te delen (artt. 6 en 14 W.OCAD).

Wanneer zij een opdracht van gerechtelijke politie vervullen, staan de leden en de directeur van de Dienst Enquêtes I onder het toezicht van de procureur-generaal bij het hof van beroep of van de federaal procureur (art. 39 W.Toezicht). Op dat ogenblik heeft het Vast Comité I geen zeggenschap over hen. De voorzitter van het Vast Comité I moet er echter zorg voor dragen dat de uitvoering van de opdrachten van gerechtelijke politie de uitvoering van de toezichtonderzoeken niet hindert. De reden daarvoor ligt voor de hand: het controleorgaan staat in de eerste plaats ter beschikking van het parlement. Die opdracht zou in het gedrang kunnen komen indien een te aanzienlijk deel van de tijd zou besteed worden aan gerechtelijke dossiers. De voorzitter kan in dat geval overleg plegen met de gerechtelijke autoriteiten over de inzet van de leden van de Dienst Enquêtes I in strafonderzoeken (art. 61*bis* W.Toezicht). Gelet op het beperkte aantal strafonderzoeken is van deze mogelijkheid nog nooit gebruik gemaakt.

In de gevallen waarin de Dienst Enquêtes I strafonderzoeken voert, moet de directeur na het afronden van dit onderzoek verslag uitbrengen bij het Vast Comité I. In dat geval '*beperkt het verslag zich evenwel tot de informatie die nuttig is voor de uitoefening door het Vast Comité I van zijn opdrachten*' (art. 43, derde lid, W.Toezicht).

In 2011 had het merendeel van de door de Dienst Enquêtes I uitgevoerde gerechtelijke opdrachten betrekking op een dossier dat in onderzoek is bij de

gerechtelijke overheden te Luik. De Dienst Enquêtes I onderzocht samen met de Federale Gerechtelijke Politie Luik de mogelijke betrokkenheid van een of meerdere leden van een inlichtingendienst bij strafbare feiten.

Daarnaast werd de Dienst Enquêtes I eind 2011 door het Federaal Parket belast met een opdracht in een opsporingsonderzoek naar een mogelijke fraude door een inlichtingenagent.

HOOFDSTUK VII.
DE GRIFFIE VAN HET BEROEPS-ORGAAN INZAKE VEILIGHEIDS-MACHTIGINGEN, -ATTESTEN EN -ADVIEZEN

De voorzitter van het Vast Comité I neemt ook het voorzitterschap van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen waar.[137] De griffiefunctie wordt uitgeoefend door de griffier (of zijn plaatsvervanger) en door de administratie van het Vast Comité I.

Het Beroepsorgaan is bevoegd voor geschillen die betrekking hebben op beslissingen in vier domeinen: de veiligheidsmachtigingen, de veiligheidsattesten die toegang moeten verlenen tot plaatsen waar zich geclassificeerde documenten bevinden, de veiligheidsattesten die toegang moeten verlenen tot welbepaalde plaatsen waar zich een dreiging voordoet en, ten slotte, de veiligheidsadviezen. Daarnaast treedt het Beroepsorgaan ook op als 'annulatierechter' tegen beslissingen van publieke of administratieve overheden om in een bepaalde sector of voor een bepaalde plaats of evenement veiligheidsattesten of -adviezen aan te vragen.[138]

Deze activiteiten van het Beroepsorgaan hebben een directe impact op zowel de budgettaire als personele middelen van het Vast Comité I. Immers worden alle werkingskosten gedragen door het Vast Comité I, dat daarnaast niet enkel én de voorzitter én griffier levert, doch ook het nodige administratief personeel dat moet instaan voor de tijdsintensieve voorbereiding, de behandeling en de afhandeling van de beroepen.

In dit hoofdstuk worden de aard van de bestreden beslissingen, de hoedanigheid van de bevoegde overheden en van de verzoekers en de aard van de beslissingen van het Beroepsorgaan binnen de verschillende beroepsprocedures cijfermatig weergegeven. Om enige vergelijking mogelijk te maken, werden de cijfers van de afgelopen twee jaar eveneens opgenomen.

---

137 Bij diens afwezigheid wordt het voorzitterschap waargenomen door een raadsheer van het Vast Comité I die tevens de hoedanigheid van magistraat heeft.

138 Zie hierover uitgebreid het *Activiteitenverslag 2006* van het Vast Comité I (91-119).

In 2011 viel een lichte daling van het aantal beroepen en beslissingen te noteren tegenover 2010: 71 tegenover 83 beroepen en 70 tegenover 85 beslissingen. Voor het overige konden geen opvallende tendensen worden vastgesteld.

Tot slot kan nog gemeld worden dat het Beroepsorgaan midden 2011 het bezoek mocht ontvangen van de secretaris van het Britse *Security Vetting Appeals Panel*. Hij gaf een uiteenzetting over de wijze waarop het beroep tegen negatieve veiligheidsscreenings in het Verenigd Koninkrijk is georganiseerd. De vergelijking tussen beide systemen leverde interessante inzichten op.

Tabel 1. Betrokken veiligheidsoverheid

	2009	2010	2011
NVO	18	36	21
VSSE	2	3	2
ADIV	19	33	39
ADCC	0	0	0
FANC	5	5	7
Federale politie	1	0	1
Lokale politie	0	0	0
Lokale luchthavencommissie[139]	3	5	1
Onbekend	0	1	0
TOTAAL	**48**	**83**	**71**

Tabel 2. Aard van de bestreden beslissing

	2009	2010	2011
Veiligheidsmachtigingen			
Vertrouwelijk	7	13	14
Geheim	18	38	31
Zeer geheim	7	9	9
Totaal veiligheidsmachtigingen	32	60	54

139 In iedere luchthaven werd door het Directoraat-generaal Luchtvaart een lokale luchthavencommissie opgericht. Bij wijze van overgangsmaatregel levert deze commissie de veiligheidsadviezen af voor personen die over een luchthavenidentificatiebadge moeten beschikken. Gelet op het K.B van 22 maart 2011 tot wijziging van het Koninklijk besluit van 3 juni 2005 tot wijziging van het Koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen (*BS* 2 mei 2011) zijn deze commissies bevoegd voor verzoeken inzake identificatiebadges die geformuleerd zijn vóór 31 december 2011.

	2009	2010	2011
Weigering	25	47	32
Intrekking	5	12	21
Machtiging voor beperkte duur	1	1	0
Machtiging voor lager niveau	1	0	1
Geen beslissing binnen termijn	0	0	0
Geen beslissing binnen verlengde termijn	0	0	0
Totaal veiligheidsmachtigingen	32	60	54
SUBTOTAAL VEILIGHEIDSMACHTIGINGEN	**32**	**60**	**54**
Veiligheidsattesten geclassificeerde documenten			
Weigering	4	1	0
Intrekking	0	0	0
Geen beslissing binnen termijn	0	0	0
Veiligheidsattesten plaats of gebeurtenis			
Weigering	9	14	14
Intrekking	0	0	0
Geen beslissing binnen termijn	0	0	0
Veiligheidsadviezen	0	0	0
Negatief advies	6	8	3
'Herroeping' van een positief advies	0	0	0
Normatieve rechtshandelingen		0	0
Beslissing van publieke overheid om attesten te eisen	0	0	0
Weigering NVO om verificaties voor attesten te verrichten	0	0	0
Beslissing van administratieve overheid om adviezen te eisen	0	0	0
Weigering NVO om verificaties voor adviezen te verrichten	0	0	0
SUBTOTAAL ATTESTEN EN ADVIEZEN	**16**	**23**	**17**
TOTAAL BESTREDEN BESLISSINGEN	**48**	**83**	**71**

Tabel 3. Hoedanigheid van de verzoeker

	2009	2010	2011
Ambtenaar	3	10	4
Militair	19	31	37
Particulier	26	39	29
Rechtspersoon	0	3	1

Tabel 4. Taal van de verzoeker

	2009	2010	2011
Franstalig	28	39	32
Nederlandstalig	20	44	39
Duitstalig	0	0	0
Anderstalig	0	0	0

Tabel 5. Aard van de door het Beroepsorgaan genomen voorbereidende beslissingen[140]

	2009	2010	2011
Volledig dossier opvragen (1)	48	82	68
Aanvullende informatie opvragen (2)	6	13	5
Horen lid overheid (3)	1	12	4
Beslissing voorzitter (4)	0	0	0
Informatie uit dossier halen door Beroepsorgaan (5)	14	31	24
Informatie uit dossier halen door inlichtingendienst (6)	0	0	0

(1) Het Beroepsorgaan beschikt over de mogelijkheid het gehele onderzoeksdossier bij de veiligheidsoverheden op te vragen. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan.
(2) Het Beroepsorgaan heeft de mogelijkheid om tijdens de procedure aanvullende informatie die het nuttig acht, op te vragen.
(3) Het Beroepsorgaan kan beslissen om de leden van de inlichtingen- en politiediensten of van de veiligheidsoverheden die aan het veiligheidsonderzoek of de -verificatie hebben meegewerkt, te horen.
(4) De voorzitter van het Beroepsorgaan kan beslissen dat het lid van de inlichtingendienst bepaalde gegevens geheim houdt tijdens zijn verhoor.

140 Het 'aantal genomen voorbereidende beslissingen' (tabel 5), de 'wijze waarop de verzoeker zijn rechten van verdediging gebruikt' (tabel 6) of nog, de 'aard van de beslissingen van het beroepsorgaan' (tabel 7) is niet noodzakelijkerwijs gelijklopend met het aantal ingediende verzoeken uit de tabellen 1 tot en met 4. Immers, sommige dossiers werden bijvoorbeeld al opgestart in 2010, terwijl de beslissing pas viel in 2011.

(5) Indien de betrokken inlichtingendienst hierom verzoekt, kan het Beroepsorgaan beslissen dat bepaalde informatie uit het dossier dat aan de verzoeker ter inzage zal worden voorgelegd, wordt gehaald.
(6) Indien het informatie betreft die afkomstig is van een buitenlandse inlichtingendienst, beslist de Belgische inlichtingendienst zelf of de informatie ter inzage is. Dit is een aspect van de toepassing van de zogenaamde 'derdenregel'.

Tabel 6. Wijze waarop de verzoeker zijn rechten van verdediging gebruikt

	2009	2010	2011
Dossierinzage door klager / advocaat	32	70	48
Horen van de klager / advocaat[141]	45	79	55

Tabel 7. Aard van de beslissingen van het beroepsorgaan

	2009	2010	2011
Veiligheidsmachtigingen			
Onontvankelijk	1	0	5[142]
Zonder voorwerp	0	0	1
Ongegrond	15	30	29
Gegrond (volledige of gedeeltelijke toekenning)	11	29	19
Bijkomende onderzoeksdaden door overheid	0	0	1
Bijkomende termijn voor overheid	0	1	0
Veiligheidsattesten geclassificeerde documenten			
Onontvankelijk	0	0	0
Zonder voorwerp	0	0	0
Ongegrond	0	0	0
Gegrond (toekenning)	0	0	0
Veiligheidsattesten plaats of gebeurtenis			
Onontvankelijk	0	1	1
Zonder voorwerp	0	0	0
Ongegrond	6	7	7
Gegrond (toekenning)	4	8	4
Veiligheidsadviezen			
Onbevoegd	1	0	0
Onontvankelijk	0	0	0

141 In bepaalde dossiers wordt de klager/advocaat meermaals gehoord.
142 In de vijf gevallen was het beroep laattijdig ingediend.

	2009	2010	2011
Zonder voorwerp	1	1	0
Negatief advies	2	7	0
Positief advies	2	1	3
Normatieve rechtshandelingen			
Onontvankelijk	0	0	0
Zonder voorwerp	0	0	0
Gegrond	0	0	0
Ongegrond	0	0	0
TOTAAL	**43**	**85**	**70**

HOOFDSTUK VIII.
DE INTERNE WERKING VAN HET VAST COMITÉ I

VIII.1. SAMENSTELLING VAN HET VAST COMITÉ I

De samenstelling van het Vast Comité I onderging in 2011 geen wijzigingen. Het voorzitterschap werd waargenomen door Guy Rapaille (F), advocaat-generaal bij het hof van beroep te Luik. De twee raadsheren waren Gérald Vande Walle (F), ambtenaar, en Peter De Smet (N), substituut-procureur-generaal bij het hof van beroep te Gent.[143]

Ook bij de Dienst Enquêtes I vielen geen verschuivingen te noteren. Het personeelsbestand van deze dienst, die onder leiding staat van directeur Pierre Nivelle, bleef op 6 *fulltime equivalenten*.

De administratieve staf van het Vast Comité I ten slotte, onder leiding van griffier Wouter De Ridder, kende evenmin uitbreiding, en bleef daarmee op een totaal van 16 personeelsleden. Wel werd gedurende negen maanden op contractuele basis een jurist tewerkgesteld.

VIII.2. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE(S)

In de loop van 2011 vonden vier vergaderingen plaats met de Senatoriële Begeleidingscommissie aan wie het Vast Comité I rapporteert en die de uiteindelijke controle uitoefent op zijn werking. Tijdens deze vergaderingen werden diverse afgesloten toezichtonderzoeken besproken. Met het oog op de bespreking van het *Activiteitenverslag 2010* van het Vast Comité I werd vergaderd met de gezamenlijke Begeleidingscommissie P en I.[144]

Eind 2011 wijzigde de samenstelling van de Senaatscommissie. Sabine de Bethune (CD&V) nam het voorzitterschap van de Senaat en dienvolgens ook van de Senatoriële Begeleidingscommissie over van Danny Pieters (NV-A), die even-

143 Ondanks een oproep in het Staatsblad (*BS* 3 december 2010) werden vooralsnog geen plaatsvervangende voorzitters en geen twee tweede plaatsvervangers voor de raadsheren aangeduid.

144 *Parl.St.* Senaat 2010-11, nr. 5-1080/1 en *Parl.St.* Kamer 2010-11, nr. 53-1695/1.

wel lid bleef[145] ter vervanging van Liesbeth Homans (NV-A). Verder maakten Armand De Decker (MR), Philippe Mahoux (PS) en Dirk Claes (CD&V) deel uit van deze commissie. In de nieuwe samenstelling bracht zij half december 2011 een bezoek aan de nieuwe zetel van het Comité in het Forumgebouw.

VIII.3. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITÉ P

De artikelen 52 tot 55 W.Toezicht bepalen de gevallen waarin en de wijze waarop het Vast Comité I en het Vast Comité P gemeenschappelijke vergaderingen dienen te organiseren. Het doel van deze vergaderingen is tweeërlei: het uitwisselen van informatie en het bespreken van gemeenschappelijke toezichtonderzoeken. In 2011 vonden zes gemeenschappelijke vergaderingen plaats. Daarin werden onder meer de uitbreiding van de evaluatiebevoegdheid van het OCAD ten aanzien van particuliere ondernemingen en de mate waarin het geheim van het strafrechtelijk onderzoek tegensprekelijk is aan de controle van het Vast Comité I, geagendeerd. De gemeenschappelijke onderzoeken hadden allen betrekking op aspecten van de werking van het OCAD.[146]

VIII.4. FINANCIËLE MIDDELEN EN BEHEERS-ACTIVITEITEN

Voor het werkingsjaar 2011 werd aan het Vast Comité I een dotatie toegekend van 4,5 miljoen euro tegenover 4 miljoen euro in 2010. De stijging was gerechtvaardigd door de nieuwe taken in het kader van de BIM-Wet en door de toename in de voorbije jaren van de werklast in het kader van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen. Bovendien verhuisde het Comité in 2011 zijn zetel naar het gebouwencomplex 'Forum' dat eigendom is van de Kamer van Volksvertegenwoordigers. De noodzakelijke aanpassingswerken *qua* beveiliging van de nieuwe site, de eigenlijke verhuis en het feit dat het Comité nog gedurende een half jaar moest instaan voor de huur van de voormalige locatie, bracht een aanzienlijke maar eenmalige meerkost met zich. Deze werd deels in de begroting van 2011 opgenomen en deels – met akkoord van de Kamercommissie voor de Comptabiliteit – gefinancierd via de boni die het Comité realiseerde voor het werkingsjaar 2009.[147]

---

145 *Hand.* Senaat 2010-11, 10 november 2011, nr. 5-34, 38-39.

146 Zie Hoofdstuk II.4, Hoofdstuk II.5 en Hoofdstuk II.8.

147 De Voorzitter van het Vast Comité I gaf tijdens de vergadering van 22 november 2011 toelichting bij de rekeningen van 2010, de begrotingsaanpassing van 2011 en de begroting van 2012. Zie *Parl.St.* Kamer 2011-12, nr. 53K2015/1, 21 e.v.

VIII.5. VERHUIS NAAR HET NIEUWE FORUM-GEBOUW

Het Vast Comité I verhuisde in 2011 vanuit de Wetstraat naar het nieuwe Forumgebouw van het Parlement in de Leuvenseweg. Dit gebeurde op verzoek van het Parlement dat hiermee schaalvoordelen en dus besparingen wil realiseren: enerzijds door het samenbrengen in één gebouw van diverse dotatiegerechtigde instellingen, anderzijds door de mogelijkheid om synergiën te creëren tussen de instellingen onderling en met het Parlement (bijvoorbeeld door een beroep te doen op de drukkerij van het Parlement, nauwer samen te werken met de bibliotheek…).

Aan de verhuis, die plaatsvond eind maart, gingen heel wat voorbereidingen vooraf, onder meer om de *business continuity* van het Comité zo veel als mogelijk te garanderen. Bij de eigenlijke verhuis diende bovendien permanent te worden gewaakt over de beveiliging van de geclassificeerde documenten.

De verhuis verliep zonder incidenten en het Comité was in een minimum van tijd opnieuw operationeel.

Het Comité beschikt vandaag over een moderne infrastructuur die beantwoordt aan alle normen inzake beveiliging en bewaring van geclassificeerd materiaal.

VIII.6. VORMING

Omwille van het belang voor de organisatie, moedigt het Vast Comité I zijn medewerkers aan tot het volgen van algemene (informatica, management…) of sectoreigen opleidingen. Wat betreft deze laatste categorie werden onderstaande studiedagen door een of meerdere (personeels)leden van het Vast Comité I bijgewoond.

DATUM	TITEL	ORGANISATIE	PLAATS
2011	Hogere Studies Veiligheid en Defensie	KHID	Brussel
27 januari 2011	Academische zitting – Controle op bijzondere inlichtingenmethoden	Vast Comité I	Brussel
15 februari 2011	Menace terroriste et réponse institutionnelle	KHID|KMS	Brussel
16 februari 2011	Single Table lunch – Meeting with Mr Stephen Hutchins – director of Security European Commission	ECSA	Brussel

DATUM	TITEL	ORGANISATIE	PLAATS
21 februari 2011	Woordvoerders, persattachés en communicatieverantwoordelijken	Politeia|Kortom|VVSG	Brussel
1 maart 2011	Inlichtingen- en veiligheidsdiensten -Geschiedenis en vooruitblik	Belgian Intelligence Studies Centre (BISC)	Brussel
17 en 18 maart 2011	Meeting – Intelligence Oversight Committees (Zweden, Noorwegen, België en Nederland)	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD)	Den Haag
25 maart 2011	De Wapenwet en zijn praktijk	KU Leuven|UGent	Leuven
4 april 2011	Usages et mésusages du fichier STIC par les forces de l'ordre	Métis	Parijs
27 april 2011	Googelen in het politioneel onderzoek – Rechercheren op het internet – Wat kan en wat mag?	Federale gerechtelijke politie|Politeia	Brussel
27 april 2011	Vraagtekens bij de Arabische Lente	KHID	Brussel
3 mei 2011	La loi sur la vie privée dans la pratique policière quotidienne	Politeia|Commission de la protection de la vie privée	Hélécine
4 – 5 mei 2011	Workshop – Open Society Justice Initiative	DCAF|Open Society Institute (OSI)	Montreux
9 mei 2011	Les procédures de création et de contrôle des fichiers des organes de renseignement	Métis	Parijs
13 mei 2011	Le point sur l'archivage électronique	JuriTIC|CRIDS|FUNDP	Namen
19 mei 2011	Défis et opportunités pour l'agenda de l'énergie nucléaire et le régime de non-prolifération	IRSD	Brussel
16 juni 2011	The importance of a secure work environment	ECSA	Brussel
20 – 24 juni 2011	Forum Interdépartemental – Optimalisation de la sécurité dans l'exécution des tâches policières en rationalisant l'usage d'une contrainte proportionnée	Police fédérale|(Police judiciaire Arlon)	Aarlen
7 september 2011	Activités de renseignement et activités de police	Fastes, Police deLiège	Luik

DATUM	TITEL	ORGANISATIE	PLAATS
22 september 2011	Militaire uitgaven belicht	Vlaams Vredesinstituut|i.s.m. Vlaams Parlement	Brussel
22 september 2011	Hautes études Police, Justice et Sécurité d'Entreprise – session 2011-2012	ECSA|ULg|UGent	Brussel
26 september 2011	Aux origines d'un renseignement européen. Les coopérations françaises en matière de renseignement au début de la guerre froide	Métis	Parijs
30 september 2011	Cloud Law or Legal Cloud?	JuriTIC|CRIDS|FUNDP	Brussel
10 oktober 2011	De la guerre froide à un monde durable – Mikhaïl Gorbatchev	SRIW|ULg	Luik
14 oktober 2011	11de BTS-dag (DJO) – Een open blik op alternatieven in toepassing BOM…	Federale politie (Directie gerechtelijke operaties)|KMS	Brussel
16-18 oktober 2011	GFF – COI/POI	VSSE|ADIV|Vast Comité I	Antwerpen
17 oktober 2011	AMOK – Incidenten	Nationale Officierenschool (KMS)	Brussel
17-19 oktober 2011	4th International Risk Assessment and Horizon Scanning Symposium (IRAHSS 2011)	National Security Coordination Secretariat	Singapore
24-28 oktober 2011	10th Annual Combined Technical Surveillance Countermeasures Working Group	ACCI|SHAPE	SHAPE
27-28 oktober 2011	7th Conference of Parliamentary Committees for Oversight of Intelligence and Security Services EU	G10-Commission|Deutsche Bundestag	Berlijn
14 november 2011	Figures du renseignement européen	Métis	Parijs
16 november 2011	Meeting – EU SitCen	ECSA	Brussel
17 november 2011	Assises de l'Intelligence Stratégique	Agence de Stimulation Economique|Cercle de Wallonie	Seraing
21 november 2011	The Navy in the 21st Century	KHID	Brussel
23 november 2011	Vijfjarig bestaan Adviesraad van de Magistratuur (ARM)	ARM|FOD Justitie	Brussel

DATUM	TITEL	ORGANISATIE	PLAATS
23 november 2011	UK – SECURITY & DEFENCE CAPABILITIES Exhibition 2011	UK Trade and Investment Section of UK Embassy Brussels	Brussel
28 november 2011	Incidents AMOK – concept tactique	Ecole Nationale des Officier|Federale politie|ERM	Brussel
30 november 2011	De gerechtelijke hervorming	Koninklijke Vlaamse Academie van België	Brussel
1 december 2011	Renseignement et éthique: un oxymore?	KHID|BISC	Brussel
2 december 2011	International Conference – Strengthening Intelligence Oversight in the Western Balkans	CTIVD|DCAF|Clingendael Institute	Den Haag
6 december 2011	Entre toge et uniforme – les conséquences de l'arrêt Salduz pour la police la justice et le barreau	Politeia|Fédération royale des officiers et hauts fonctionnaires de la police belge	Wépion
16 december 2011	Human Resources Management en Leiderschap in de publieke sector	KU Leuven	Leuven
19 december 2011	Le contrôle politique du renseignement en Europe	Métis	Parijs

HOOFDSTUK IX.
AANBEVELINGEN

Op basis van de in 2011 afgesloten toezichtonderzoeken, formuleert het Vast Comité I onderstaande aanbevelingen. Zij hebben in het bijzonder betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen (IX.1), op de coördinatie en de efficiëntie van de inlichtingendiensten, het OCAD en de ondersteunende diensten (IX.2) en – ten slotte – op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I (IX.3).

IX.1. AANBEVELINGEN IN VERBAND MET DE BESCHERMING VAN DE RECHTEN DIE DE GRONDWET EN DE WET AAN PERSONEN WAARBORGEN

IX.1.1. VERNIETIGEN EN ARCHIVEREN VAN DOCUMENTEN VAN DE INLICHTINGENDIENSTEN EN EEN AUTOMATISCHE DECLASSIFICATIE[148]

Het al dan niet vernietigen en/of archiveren van documenten van inlichtingendiensten is nauw gelieerd met '*de rechten die de Grondwet en de wet aan de personen waarborgen*'. De problematiek wordt geregeld door een hele reeks wettelijke bepalingen. Het Vast Comité I kwam tot de bevinding dat de diverse in het geding zijnde belangen perfect verzoenbaar zijn mits rekening wordt gehouden met het onderscheid tussen de zogenaamde 'levende' en 'dode' archieven. Wel heeft het Comité zich voorstander getoond van een systeem waarbij classificaties na een bepaalde termijn – bijvoorbeeld 30 jaar voor documenten die 'geheim' zijn geclassificeerd en 50 jaar voor 'zeer geheime' documenten – van rechtswege vervallen, tenzij zij expliciet worden hernieuwd. Dit vereist een aanpassing van de Classificatiewet.

[148] Zie Hoofdstuk V.1. De wettelijke regeling inzake archivering en vernietiging van gegevens van de VSSE en de ADIV.

IX.1.2. AANBEVELING IN HET KADER VAN DE INTERCEPTIE VAN BUITENLANDSE COMMUNICATIE[149]

In het beluisteringsplan van de ADIV mogen alleen organisaties en instellingen worden opgenomen als *target*, geen fenomenen. Dit blijkt duidelijk uit artikel 44*bis* W.I&V.

IX.2. AANBEVELINGEN IN VERBAND MET DE COÖRDINATIE EN DE EFFICIËNTIE VAN DE INLICHTINGENDIENSTEN, HET OCAD EN DE ONDERSTEUNENDE DIENSTEN

IX.2.1. AANBEVELINGEN MET BETREKKING TOT DE AUDIT BIJ DE ADIV[150]

In het kader van de audit bij de ADIV formuleerde het Vast Comité I talrijke aanbevelingen aangaande de organisatorische voorwaarden noodzakelijk voor een goede inzet van de middelen (IX.2.1.1), het beheer en de leiding van het personeel (IX.2.1.2), de informatiestromen en ICT (IX.2.1.3) en ten slotte het risicobeheer (IX.2.1.4). Een onderscheid werd daarbij gemaakt tussen 'aanbevelingen voor verandering' (het betreft aanbevelingen die essentieel zijn voor de goede werking van de ADIV en een belangrijke wijziging van de huidige manier van werken of voor de organisatie inhouden) en 'aanbevelingen voor verbetering' (deze gaan meer in op detailmateries waarbij de werkwijze niet fundamenteel moet worden gewijzigd, maar eerder bijgeschaafd en verbeterd). Beide vormen zijn complementair en worden hieronder verkort weergegeven.

IX.2.1.1. Aanbevelingen inzake organisatorische voorwaarden noodzakelijk voor een goede inzet van de middelen

- de personeels- en organisatiefunctie (P&O-functie) binnen de ADIV moet dringend versterkt worden. Deze versterking is een aanbeveling tot verandering en vormt dus een *conditio sine qua non* teneinde andere aanbevelingen met kans op succes uit te kunnen voeren;
- het Comité beveelt aan dat een recurrent proces wordt opgestart om duidelijke en SMART-geformuleerde doelstellingen – in termen van af te leveren producten en *service levels agreements* (SLA) – te definiëren;

[149] Zie Hoofdstuk IV. Het toezicht op de interceptie van communicatie uitgezonden in het buitenland.

[150] Zie Hoofdstuk II.1. Een audit bij de militaire inlichtingendienst.

- er dient te worden bepaald welke samenwerking tussen en binnen divisies opportuun én noodzakelijk is om deze doelstellingen te realiseren. De voorgestelde producten en SLA moeten daarenboven worden afgetoetst bij de interne en externe gebruikers en 'klanten';
- met het bepalen van de producten en de SLA, moet ook de vereiste personeelsinvestering in termen van tijdsbesteding en competenties worden ingeschat;
- het competentiebeheer binnen de ADIV en het afstemmen van taken, functies en competenties vereist een meer professionele aanpak;
- het Vast Comité I is van oordeel dat creativiteit voor een inlichtingendienst een waardevol goed is en dus moet worden gestimuleerd[151];
- voor elke doelstelling moet een planning, de betrokken actoren alsook de wijze van opvolging, worden vastgelegd. Dit is een aanbeveling voor verandering;
- er dient in alle collecteplannen te worden bepaald welke de vereiste informatie is om de producten tot stand te kunnen brengen en wie deze informatie kan aanleveren. Met het oog hierop moet een informatiebeheerder worden aangesteld en moet het geautomatiseerde zoeken in bestanden worden vergemakkelijkt;
- elke divisie dient periodiek zowel de eigen personeelsleden als deze van andere divisies voor te lichten over 'wie' 'welke' informatie heeft en 'wat' ter beschikking kan worden gesteld;
- een *feedback*-mechanisme dient te worden ingebouwd voor alle afgeleverde producten. Ook dienen de interne en externe klanten hierover stelselmatig te worden bevraagd zodat zij een beter inzicht krijgen in hun noden en in wat ze vanwege de ADIV mogen verwachten;
- de ADIV en de Algemene Directie *Material Resources* van de Krijgsmacht moeten, elk binnen hun budgettaire mogelijkheden, de werkingsmiddelen en de arbeidsomstandigheden permanent trachten te verbeteren. Daarbij moet duidelijk de nadruk liggen op de ICT-middelen, zonder evenwel de veiligheidsaspecten (beveiliging van documenten, infrastructuur en personen) uit het oog te verliezen.

IX.2.1.2. Aanbevelingen inzake het beheer en de leiding van het personeel van de ADIV

- het Vast Comité I beveelt aan om duidelijke functiebeschrijvingen op te stellen;
- de (permanente) vorming dient te worden gewijzigd. De actuele en vereiste competenties moeten in kaart worden gebracht, een vormingsplan opgesteld en het in- en externe vormingsaanbod geïnventariseerd[152];

---

151 Bijvoorbeeld via verbetercirkels of een 'intrapreneurschap' (dit is het ondernemerschap binnen de grenzen van de eigen organisatie).

152 Wat het specifieke geval van de gecertificeerde opleiding voor de statutaire burgerpersoneelsleden van het statuut Camu betreft, moet overleg worden gepleegd met de DG HR en de FOD Personeel en Organisatie, om te onderzoeken of het mogelijk is 'functies' in het leven te

- het Vast Comité I is van mening dat het creëren van een 'inlichtingentak'[153] een aantal van de vastgestelde problemen (gedeeltelijk) kan oplossen en een reële verandering kan teweegbrengen;
- er dient te worden verholpen aan de vele geldelijke en administratieve verschillen die bestaan tussen de diverse personeelsgroepen binnen de ADIV en tussen deze van de ADIV en andere diensten uit de inlichtingensector (VSSE en OCAD). Deze verschillen zijn immers nefast voor een degelijk personeelsbeheer;
- bijzondere aandacht moet worden besteed aan de *coaching*, begeleiding en ondersteuning van het personeel van de ADIV en dit rekening houdend met hun specifieke situatie;
- het Vast Comité I beveelt aan dat in het kader van de (versterkte) P&O-functie een cel wordt opgericht waar de burgerpersoneelsleden terecht kunnen met de problemen die eigen zijn aan hun statuut en situatie;
- de beoordeling van personeelsleden van de ADIV gebeurt momenteel op basis van een reglementair kader dat deze dienst overstijgt. De P&O-functie moet er mee over waken dat de evaluaties goed worden uitgevoerd en begeleid. Ook dient per doelstelling en af te leveren product te worden omschreven op welke wijze de evaluatie zal gebeuren;
- het Vast Comité I beveelt aan dat de ongelijkheden in het statuut van de personeelsleden binnen de ADIV, worden aangepakt. Daarbij wordt bij voorkeur een 'functionele logica' gevolgd in plaats van een 'groepslogica'. De analysefunctie verdient daarbij prioritaire aandacht. Immers, daar zijn de grootste verschillen, waardoor sneller een risico op discontinuïteit ontstaat;
- het Comité beveelt aan dat binnen de ADIV een functie wordt gecreëerd met als hoofdopdracht 'het beheer van de interne communicatie'.

IX.2.1.3. Aanbevelingen inzake informatiestromen en ICT

- het Vast Comité I is van mening dat het nieuwe *Request for Information (RFI)*-systeem de behandeling, de opvolging en de afhandeling van informatieverzoeken (sterk) zal verbeteren. Het Comité beveelt de ADIV aan pas na een bepaalde testperiode te onderzoeken of er zich bijkomend nog een reorganisatie opdringt. In tussentijd kan de ADIV zich concentreren op het technische aspect van het RFI-managementsysteem zonder daarbij onmiddellijk met organisatorische kwesties te worden geconfronteerd;
- het Comité beveelt aan om de aangevatte integratie van de gegevensverzameling en de databanken voort te zetten en zo mogelijk te versnellen;

---

roepen die nauw aansluiten bij het inlichtingen- en analysewerk en/of aangepaste gecertificeerde opleidingen te ontwikkelen.

153 Vanzelfsprekend stelt zich de vraag welke onderdelen in een dergelijke inlichtingentak zouden moeten verenigd zijn. Het viel buiten de *scope* van de audit om daarop een definitief antwoord te geven. Dit vereist een afzonderlijke studie.

– om het grote volume aan gegevens en documentatie te kunnen beheersen, moet de ADIV verschillende initiatieven nemen. Vooreerst moet worden bepaald welke informatie nodig is voor het realiseren van de doelstellingen en de af te leveren producten. Daarnaast moet gezorgd worden voor een goede samenwerking tussen de collecte-afdelingen en de analysebureaus. Ten slotte dient evident geïnvesteerd te worden in de absoluut benodigde ICT- en personele middelen;
– in het algemeen beveelt het Comité aan voldoende middelen in ICT-technologie te investeren, en dit sneller dan voorzien in de investeringsplannen.

IX.2.1.4. Aanbevelingen inzake het risicobeheer

– het Comité beveelt aan acties te ondernemen om de risico's inzake discontinuïteit van de functie-uitoefening en verlies van kennis te beperken. Meer bepaald dient een previsioneel personeelsbeheer te worden gevoerd, dient de creatie van een 'inlichtingentak' (waarbij het verlies aan kennis minder groot is en de vervanging van personen vlotter kan verlopen) te worden overwogen en dient – opnieuw – geïnvesteerd in ICT;
– het is aangewezen dat er binnen de ADIV uitgesproken aandacht wordt betoond voor kennismanagement. Er moeten duidelijke instructies worden uitgewerkt om de aanwezige kennis in kaart te brengen, de relevantie ervan te beoordelen en maatregelen te nemen om ze op te slaan, te bewaren en te verspreiden. Het strekt tot aanbeveling binnen elke divisie een kennisbeheerder aan te stellen die het kennismanagement ondersteunt;
– het Vast Comité I meent dat het risico op 'pragmatische prioriteitvorming'[154] beperkt is, maar dat er wel waakzaamheid aan de dag moet worden gelegd. Een goede werving en een uitgebouwd systeem van functiebeschrijvingen kan dit risico nog inperken;
– het Vast Comité I beveelt aan dat de ADIV werk zou maken van het ontwikkelen van het risicobeheer.

IX.2.2. AANBEVELINGEN MET BETREKKING TOT DE BIM-WET[155]

IX.2.2.1. Hoogdringendheidsprocedure voor specifieke en uitzonderlijke methoden

Voor alle specifieke en uitzonderlijke methoden moet in een hoogdringendheidprocedure worden voorzien die de diensten enerzijds toelaat onmiddellijk te

[154] Daarbij gaat de aandacht prioritair naar zaken die goed worden beheerst; zaken waar men niet sterk staat krijgen dienvolgens om pragmatische redenen minder aandacht.
[155] Deze aanbevelingen komen voort uit de vaststellingen gedaan in het kader van de jurisdictionele controle van het Vast Comité I op de bijzondere inlichtingenmethoden (zie Hoofdstuk III).

reageren op acute dreigingen, terwijl zij anderzijds een gedegen controle mogelijk maakt.

IX.2.2.2. Aanstelling van plaatsvervangers voor de BIM-commissie

Er dient zo spoedig mogelijk te worden overgegaan tot de aanstelling van plaatsvervangende leden voor de BIM-commissie. Dit is absoluut noodzakelijk om de continuïteit van de administratieve controle op bijzondere inlichtingenmethoden te kunnen garanderen.

IX.2.2.3. Identificatie van gebruikers van communicatiemiddelen als specifieke methode

Inzake de identificatie van gebruikers van bepaalde communicatiemiddelen, zoals bijvoorbeeld een GSM, meent het Vast Comité I dat een reflectie aangewezen is over de opportuniteit van het behoud van deze maatregel als een specifieke methode. Terwijl de intrusiviteit van dergelijke methode als gering tot zeer gering wordt ervaren, is deze maatregel niettemin aan dezelfde stringente eisen onderworpen als alle andere specifieke methoden die nochtans een meer verregaande inbreuk op het privéleven kunnen inhouden. Gelet op de zeer aanzienlijke inzet van dergelijke methoden, houdt dit een zware administratieve werklast in voor deze diensten.

IX.2.3. AANBEVELINGEN MET BETREKKING TOT DE INFORMATIEVEILIGHEID[156]

IX.2.3.1. Veiligheidsbeleid rond cyberaanvallen

Zowel in België als binnen Europees en NAVO-verband werden heel wat initiatieven ontwikkeld met betrekking tot informatieveiligheid.[157] Het Vast Comité I acht het voor ons land niet alleen belangrijk om deze initiatieven goed te coördineren, maar ook daadwerkelijk op te nemen in een geïntegreerd veiligheidsbeleid rond cyberaanvallen tegen de nationale belangen. Daarbij is de oprichting van een agentschap dat de activiteiten rond informatieveiligheid kan coördineren, onontbeerlijk.

IX.2.3.2. Bevoegdheidsuitbreiding van de ADIV en de VSSE

De BIM-Wet gaf aan de ADIV een bijkomende opdracht om *'in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die*

---

156 Zie Hoofdstuk II.2. De bescherming van communicatiesystemen tegen mogelijke buitenlandse intercepties en cyberaanvallen.

157 Zie bijvoorbeeld het *Witboek voor een nationaal beleid voor de informatieveiligheid*, de *NATO cyber defence policy* en het *European Programme for Critical Infrastructure Protection*.

de minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren' (art. 11 § 1, 2° W.I&V). Het Vast Comité I beveelt echter aan dat in dezelfde mogelijkheid wordt voorzien in geval van aanvallen tegen informatiesystemen van andere overheidsdiensten of tegen de nationale kritieke infrastructuur. De VSSE zou met deze opdracht kunnen worden belast.

IX.2.3.3. Voldoende gekwalificeerde personeelsleden

Het Vast Comité I stelde bij de inlichtingendiensten een ernstig tekort vast aan gekwalificeerde personeelsleden om de opdracht inzake informatieveiligheid uit te oefenen. Het beveelt aan deze diensten eindelijk de middelen te verschaffen die moeten toelaten het benodigde personeel te rekruteren.

IX.2.3.4. Voldoende beveiligd materiaal voor de verwerking van gevoelige en geclassificeerde informatie

Het Vast Comité I beveelt de grootste omzichtigheid aan bij de keuze van beveiligde technische uitrustingen voor de verwerking van gevoelige en geclassificeerde informatie. Het Comité neemt de aanbevelingen over van het *Witboek van het Overlegplatform voor de informatieveiligheid* en beveelt aan dat technische uitrustingen worden geëvalueerd, gecertificeerd en gehomologeerd – wat betreft hun betrouwbaarheid en veiligheid – volgens criteria en procedures die beantwoorden aan de normen van de Europese Unie.

Het Vast Comité I beveelt daarenboven aan dat bij de gunning van opdrachten aan leveranciers van dergelijk materieel het bezit van een veiligheidsmachtiging wordt opgelegd. In het kader van het voorafgaandelijke veiligheidsonderzoek zou bijzondere aandacht moeten worden besteed aan de eventuele banden van die leveranciers met sommige buitenlandse inlichtingendiensten.

IX.2.3.5. Voldoende technische certificatie- en homologatiemiddelen

Het Vast Comité I ziet ook het tekort aan technische certificatie- en homologatiemiddelen als een ernstig probleem op het vlak van de informatieveiligheid. Het beveelt dan ook aan om in de noodzakelijke middelen te voorzien opdat de certificatie en homologatie van de systemen die in België worden gebruikt om geclassificeerde informatie te verwerken, eindelijk kan plaatsvinden zonder dat men daarbij afhankelijk is van buitenlandse overheden en diensten.

IX.2.4. AANBEVELINGEN MET BETREKKING TOT HET OCAD EN ZIJN ONDERSTEUNENDE DIENSTEN[158]

IX.2.4.1. Een duidelijk centraal contactpunt

In sommige ondersteunende diensten van het OCAD ontbreekt een als dusdanig gekend en erkend centraal contactpunt. Alhoewel de experts die afkomstig zijn van die betrokken diensten deze lacune gedeeltelijk opvangen, blijft het zo dat er geen enkele garantie is naar opspoorbaarheid van de informatiestromen, noch naar organisatie van de ambtshalve mededeling van inlichtingen. Hier moet, naar het oordeel van de Vaste Comités P en I, op korte termijn een ernstige inspanning worden geleverd.

IX.2.4.2. Een duidelijk zicht op de informatiestromen

Het centrale contactpunt binnen elke ondersteunende dienst van het OCAD zou een volledig zicht moeten hebben op de uitgewisselde inlichtingen en/of evaluaties. Binnen elke dienst zou bovendien de traceerbaarheid van de inlichtingen gegarandeerd moeten worden.

IX.2.4.3. Ontvangstmeldingen en dringendheidsgraden

Het toezichtonderzoek wees uit dat de verplichtingen uit artikel 11 §§ 2 en 3 KB. OCAD om ontvangstmelding te geven en dringendheidsgraden na te leven, niet steeds werd gerespecteerd. De Comités waren van oordeel dat mochten deze verplichtingen voor de diensten geen meerwaarde bieden, de regelgeving in die zin moet worden aangepast. In het andere geval, dient het Koninklijk besluit verder te worden verfijnd in die zin dat de reglementaire mogelijkheid moet ingebouwd worden om niet te antwoorden indien men over geen informatie beschikt. Tevens waren de Comités van oordeel dat een duidelijk onderscheid gemaakt moet worden tussen bestemmelingen van berichten 'ter info' en bestemmelingen van wie een (re)actie wordt verwacht.

IX.2.4.4. Begripsverwarring inzake diverse embargoprocedures

De mogelijke begripsverwarring tussen de embargoprocedures *ex* artikelen 11 en 12 W.OCAD en gelijkaardige procedures uit bijvoorbeeld de Wet op het Politieambt moeten volledig worden uitgesloten.

---

158 De eerste zes aanbevelingen vormen het resultaat van de vaststellingen gedaan in het kader van het toezichtonderzoek 'De informatiestromen tussen het OCAD en zijn ondersteunende diensten' (zie Hoofdstuk II.4). De zevende aanbeveling komt voort uit het gemeenschappelijk onderzoek naar 'Een gepland werkbezoek in het buitenland door het OCAD (zie Hoofdstuk II.5). De laatste aanbeveling vloeit voort uit beide onderzoeken.

IX.2.4.5. 'Operationaliseren' van het beveiligd communicatie- en informatieplatform

De Vaste Comités P en I bevelen aan dat voor het beveiligde en gecodeerde communicatie- en informatieplatform een toekomstvisie zou ontwikkeld worden en dat op korte termijn een reeks obstakels weggewerkt zouden worden om de reeds geplande verbindingen eindelijk operationeel te maken.

IX.2.4.6. Uitklaring van het begrip 'relevante inlichtingen'

Sommige ondersteunende diensten hebben problemen om een concrete invulling te geven aan de notie 'relevante inlichtingen'. De invulling van dit begrip moet duidelijk uitgeklaard moeten, eventueel in gemeenschappelijke werkgroepen.

IX.2.4.7. Verwarring omtrent de identiteit van het OCAD

Het verdient aanbeveling dat het OCAD er steeds zou over waken dat er omtrent zijn unieke identiteit geen enkele verwarring kan ontstaan. Het OCAD is, in tegenstelling tot de ADIV en de VSSE, namelijk geen inlichtingendienst. Een actieve en consequente aandacht hiervoor in zijn communicatie en werking, en dit zowel in het binnen- als het buitenland, is dan ook essentieel. In dit kader verdient het aanbeveling dat het OCAD uiterst behoedzaam is bij het ondernemen van buitenlandse zendingen en dat het zijn studiereizen strikt zou aflijnen.

IX.2.4.8. De 'buitenlandopdracht' van het OCAD

Wat betreft de relatie tussen het OCAD en de twee inlichtingendiensten, stelt de ADIV het mandaat van het OCAD in het buitenland in vraag en heeft de VSSE bedenkingen bij de contacten tussen het OCAD en buitenlandse inlichtingendiensten. Dit zou verder uitgeklaard moeten worden tussen de betrokken diensten. Belangrijker is evenwel dat uiteindelijk het Ministerieel Comité voor inlichting en veiligheid ter zake een richtlijn zou uitvaardigen en dit in uitvoering van artikel 8, 3° W.OCAD.

IX.2.5. AANBEVELINGEN MET BETREKKING TOT DE STRIJD TEGEN PROLIFERATIE EN DE BESCHERMING VAN HET WEP[159]

Het Vast Comité I beveelt de VSSE aan om van een reactieve en *adhoc*-benadering over te stappen naar een meer proactieve aanpak van de strijd tegen proliferatie waarbij ook aandacht is voor meer strategische analyses. In die analyses mogen ook de aspecten 'economische belangen' en mogelijke 'inmenging' door buitenlandse (inlichtingen)diensten niet uit het oog worden verloren. Dergelijke analyses vereisen een gedegen informatiepositie die alleen kan bereikt worden door het intensifiëren van contacten met de Belgische administraties, bedrijven, laboratoria en onderzoekscentra en via samenwerkingsakkoorden met de instanties die betrokken zijn bij de strijd tegen de proliferatie.[160] Vanuit dezelfde bekommernis beveelt het Comité aan de analisten en operationele agenten die werken op het gebied van de bescherming van het WEP enerzijds en van de proliferatie anderzijds, samen te brengen om een gemeenschappelijke methodologie op te stellen. Dit moet er eveneens toe bijdragen dat de VSSE een eenduidig standpunt kan innemen ten aanzien van de bevoegde politieke instanties.

Tot slot herhaalt het Comité de aanbeveling van de Senaat die tot doel heeft om in de wet houdende regeling van de inlichtingen- en veiligheidsdienst een specifieke bevoegdheid op te nemen betreffende de controle van de wettelijkheid van de activiteiten van de buitenlandse inlichtingendiensten op ons grondgebied.[161]

IX.2.6. RECHTSTREEKSE INFORMATIE-UITWISSELING TUSSEN POLITIE- EN INLICHTINGENDIENSTEN[162]

Het Vast Comité I beveelt aan dat er tussen de inlichtingendiensten enerzijds en de (federale en lokale) politiediensten anderzijds, gestructureerd overleg zou plaatsvinden om via welbepaalde procedures gegevens uit te wisselen. Het ontbreken van een samenwerkingsakkoord tussen deze diensten vormt zonder twijfel een tekortkoming in ons veiligheidssysteem. Het Vast Comité I heeft hier in het verleden al meermaals op gewezen.[163]

---

159 Zie Hoofdstuk II.2. De bescherming van communicatiesystemen tegen mogelijke buitenlandse intercepties en cyberaanvallen.

160 Zoals bijvoorbeeld met de FOD Buitenlandse Zaken, de Administratie der Douane en Accijnzen, het CANVEK en de regionale overheden die ter zake bevoegd zijn.

161 VAST COMITÉ I, *Activiteitenverslag 2006*, 128.

162 Zie Hoofdstuk II.3. De informatiepositie en de acties van de inlichtingendiensten met betrekking tot Lors Doukaev.

163 VAST COMITÉ I, *Activiteitenverslag 2006*, 131; *Activiteitenverslag 2007*, 75 en *Activiteitenverslag 2009*, 86-87.

Alvorens de creatie van een databank over terrorisme en radicalisme te overwegen, beveelt het Vast Comité I aan om snel een systeem van informatie-uitwisseling op te zetten tussen de politie- en de inlichtingendiensten.

IX.2.7. COÖRDINATIE VAN DE VERTEGENWOORDIGING VAN VEILIGHEIDSDIENSTEN OP INTERNATIONALE FORA[164]

De Vaste Comités P en I vragen de haalbaarheid te onderzoeken van één specifieke structuur die kan worden belast met de coördinatie en/of de vertegenwoordiging van de diverse Belgische diensten die deelnemen aan internationale fora of vergaderingen in het kader van de strijd tegen het terrorisme en het extremisme. Meer in het bijzonder kan het Ministerieel Comité voor inlichting en veiligheid in deze een initiatief nemen en kan het College voor inlichting en veiligheid op zijn beurt aangeduid worden om te waken over de uitvoering ervan.

Dergelijke structuur is uiteraard niet bedoeld voor fora die zich specifiek richten op één of meerdere welbepaalde diensten.

IX.2.8. EEN DEONTOLOGISCHE CODE VOOR DE AGENTEN VAN DE VSSE[165]

Het Vast Comité I beveelt aan dat de VSSE in uitvoering van artikel 17 van het K.B. van 13 december 2006 houdende het statuut van de ambtenaren van de buitendiensten van de VSSE een (voorstel van) deontologische code zou opstellen en ter goedkeuring aan de minister van Justitie zou voorleggen.

In die code moet duidelijk omschreven worden wat de neutraliteits- en discretieplicht van de ambtenaren van de VSSE inhouden. Tevens moet gewaakt worden over de strikte naleving van deze deontologische code door een snelle en consequente toepassing van de tuchtprocedure in geval van niet-naleving. Die tuchtprocedure mag zeker niet verward worden met een veiligheidsonderzoek die een eigen finaliteit kent.

---

164 Zie Hoofdstuk II.8. De Belgische vertegenwoordiging bij internationale vergaderingen inzake terrorisme.

165 Zie Hoofdstuk II.7. Klacht van een lid van de VSSE en zijn echtgenote.

IX.3. AANBEVELINGEN IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

IX.3.1. SPONTANE MELDING VAN PROBLEMEN AAN DE TOEZICHTORGANEN

Het OCAD en de ondersteunende diensten dienen de Vaste Comités P en I spontaan in te lichten indien zij in hun onderlinge relatie structurele disfuncties op legaliteits-, efficiëntie- of coördinatievlak menen waar te nemen.

IX.3.2. CONTROLE VAN HET LOGBOEK INZAKE BUITENLANDSE INTERCEPTIES[166]

Het Vast Comité I beveelt aan dat de bladzijden van het logboek inzake intercepties op voorhand zouden geparafeerd worden door het diensthoofd of een door hem aangewezen officier.

[166] Zie Hoofdstuk IV. Het toezicht op de interceptie van communicatie uitgezonden in het buitenland.

BIJLAGEN

BIJLAGE A.
OVERZICHT VAN DE BELANGRIJKSTE REGELGEVING MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2011 TOT 31 DECEMBER 2011)

Wet 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten – Duitse vertaling, *BS* 10 maart 2011

Wet 9 februari 2011 tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, *BS* 29 maart 2011

Wet 11 april 2011 tot opening van voorlopige kredieten voor de maanden april, mei en juni 2011, *BS* 26 april 2011

Wet 30 mei 2011 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2011, *BS* 16 juni 2011

Wet 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, *BS* 15 juli 2011

K.B. 1 juni 2011 tot wijziging van het koninklijk besluit van 13 december 2006 houdende het statuut van de ambtenaren van de buitendiensten van de Veiligheid van de Staat, *BS* 22 juni 2011

K.B. 17 oktober 2011 betreffende de veiligheidsattesten voor de nucleaire sector en tot regeling van de toegang tot de veiligheidszones, het kernmateriaal of tot de nucleaire documenten in bepaalde bijzondere omstandigheden – Erratum, *BS* 25 november 2011

K.B. 17 oktober 2011 houdende de categorisering en de bescherming van nucleaire documenten – Erratum, *BS* 25 november 2011

K.B. 17 oktober 2011 betreffende de categorisering van het kernmateriaal en de definiëring van veiligheidszones in de nucleaire installaties en de nucleaire vervoerbedrijven – Erratum, *BS* 25 november 2011

K.B. 17 oktober 2011 betreffende de fysieke beveiliging van het kernmateriaal en de nucleaire installaties – Erratum, *BS* 25 november 2011

K.B. 2 december 2011 betreffende de kritieke infrastructuren in de deelsector van het luchtvervoer, *BS* 27 december 2011

K.B. 21 december 2011 houdende aanwijzing van de leden van het Ministerieel Comité voor inlichting en veiligheid, *BS* 28 december 2011

M.B. 4 april 2011 tot wijziging van het ministerieel besluit van 4 mei 2007 betreffende de stage en de vorming van de ambtenaren van de buitendiensten van de Veiligheid van de Staat, *BS* 15 april 2011

M.B. 20 oktober 2011 betreffende de procedure van veiligheidsverificatie voor alle personeelsleden van de NV van publiek recht A.S.T.R.I.D. en van haar onderaannemers, *BS* 28 november 2011

Vergelijkende selectie van Nederlandstalige juristen (inlichtingendienst) (m/v) (niveau A) voor het Ministerie van Defensie (ANG11007), *BS* 2 september 2011

Openstaande betrekking van adjunct-directeur van het Coördinatieorgaan voor de dreigingsanalyse (wet van 10 juli 2006, *BS* van 20 juli 2006) – Oproep tot kandidaten, *BS* 13 september 2011

Personeel – Aanwijzing aanduiding van de administrateur-generaal van de Veiligheid van de Staat, *BS* 26 oktober 2011

Rechterlijke Orde – Aanwijzing in de hoedanigheid van directeur bij het Coördinatieorgaan voor dreigingsanalyse, *BS* 2 december 2011

Uittreksel uit arrest nr. 145/2011 van 22 september 2011: *In zake*: de beroepen tot gehele of gedeeltelijke vernietiging van de wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, ingesteld door de Orde van Vlaamse balies en Jo Stevens en door de vzw 'Liga voor Mensenrechten', *BS* 12 december 2011

BIJLAGE B.
OVERZICHT VAN DE BELANGRIJKSTE WETSVOORSTELLEN, WETSONTWERPEN, RESOLUTIES EN PARLEMENTAIRE BESPREKINGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2011 TOT 31 DECEMBER 2011)

Senaat

Beslissingen van de parlementaire overlegcommissie, *Parl. St.* Senaat 2010-11, nr. 5-82/6

Wetsvoorstel tot wijziging van het Wetboek van de Belgische nationaliteit, *Parl. St.* Senaat 2010-11, nr. 5-736/1

Voorstel van begroting voor het jaar 2011 van de Bestuurlijke commissie belast met de controle op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (Commissie BIM – C-BIM), *Parl. St.* Senaat 2010-11, nrs. 5-792/1 tot 5-792/3

Verslag over het toezicht op de activiteiten van Europol door het Europees Parlement in samenwerking met de nationale parlementen, *Parl. St.* Senaat 2010-11, nr. 5-774/1

Conferentie van Voorzitters van de parlementen van de Europese Unie (Brussel, 3-5 april 2011), *Parl. St.* Senaat 2010-11, nr. 5-1033/1

Voorstel van begroting voor het jaar 2012 van de Bestuurlijke commissie belast met de controle op de specifieke en uitzonderlijke methoden voor het verzamelen van gege-

vens door de inlichtingen- en veiligheidsdiensten (Commissie BIM – C-BIM), *Parl. St.* Senaat 2011-12, nr. 5-1386/1

Verzenden naar de Commissie belast met de begeleiding van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten van het halfjaarlijks verslag over de toepassing van de specifieke en uitzonderlijke methoden door de inlichtingen- en veiligheidsdiensten en de controle hierop uitgevoerd door het Vast Comité I voor de periode van 1 september 2010 tot en met 31 december 2010, *Hand.* Senaat 2010-11, 27 januari 2011, nr. 5-11, 58

Bespreking van het activiteitenverslag 2009 van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, (Stuk 5-545), *Hand.* Senaat 2010-11, 24 februari 2011, nr. 5-13, 38

Bespreking van het voorstel van begroting voor het jaar 2011 van de Bestuurlijke commissie belast met de controle op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de twee inlichtingen- en veiligheidsdiensten (Commissie BIM – C-BIM) (Stuk 5-792), *Hand.* Senaat 2010-11, 31 maart 2011, nr. 5-19, 35

Verzenden naar de Commissie belast met de begeleiding van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten van het activiteitenverslag 2010 van het Vast Comité I, *Hand.* Senaat 2011-12, 11 oktober 2011, nr. 5-33, 26

Benoeming van een lid van de commissie belast met de begeleiding van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten (Vast Comité I), *Hand.* Senaat 2011-12, 10 november 2011, nr. 5-34, 38

Kamer van Volksvertegenwoordigers

Wetsontwerp tot wijziging van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle en tot wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *Parl. St.* Kamer 2010-11, nrs. 53K1005/001 tot 53K1005/005, *Hand.* Kamer 2010-11, 17 februari 2011, CRIBV53PLEN019, 80

Wetsontwerp tot wijziging van het Wetboek van de Belgische nationaliteit teneinde het verkrijgen van de Belgische nationaliteit migratieneutraal te maken, *Parl. St.* Kamer 2010-11, nrs. 53K0476/007 en 53K0476/010

Beslissingen van de parlementaire overlegcommissie, *Parl. St.* Kamer 2010-11, nr. 53K0082/006

Wetsontwerp tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, *Parl. St.* Kamer 2010-11, nr. 53K0802/002

Wetsontwerp tot wijziging van het Strafwetboek met het oog op de strafbaarstelling van de mentale destabilisatie van personen en van het misbruik van personen in een verzwakte positie, *Parl. St.* Kamer 2010-11, nr. 53K1217/001

Toezicht op de activiteiten van Europol door het Europees Parlement in samenwerking met de nationale parlementen, *Parl. St.* Kamer 2010-11, nr. 53K1255/001

Wetsontwerp tot opening van voorlopige kredieten voor de maanden april, mei en juni 2011, *Parl. St.* Kamer 2010-11, nr. 53K1280/001

Voorstel van resolutie over de strijd tegen cyberaanvallen en cyberoorlogen, *Parl. St.* Kamer 2010-11, nr. 53K1289/001

Wetsontwerp tot wijziging van de wetgeving inzake de erkenning van de islamitische eredienst, *Parl. St.* Kamer 2010-11, nr. 53K1327/001

Wetsontwerp betreffende de kritieke infrastructuren, de andere punten van federaal belang en de punten van lokaal belang, *Parl. St.* Kamer 2010-11, nr. 53K1357/001

Ontwerp van de algemene uitgavenbegroting voor het begrotingsjaar 2011, *Parl. St.* Kamer 2010-11, nr. 53K1348/001

Conferentie van de Voorzitters van de parlementen van de Europese Unie Brussel, 3 – 5 april 2011, *Parl. St.* Kamer 2010-11, nr. 53K1497/001

Wetsontwerp betreffende de bescherming van bedreigde getuigen, *Parl. St.* Kamer 2010-11, nrs. 53K1472/001, 53K1472/003 en 53K1472/004

Voorstel van resolutie betreffende de bestrijding van islamitische satellietzenders, radiostations en websteks die op het Belgische en Europese grondgebied anti-Westerse haatpropaganda verspreiden, *Parl. St.* Kamer 2010-11, nr. 53K1518/001

Wetsontwerp tot invoeging van de artikelen 442*quater* en 442*quinquies* in het Strafwetboek, met het oog op de strafbaarstelling van de mentale destabilisatie van personen en van het misbruik van personen in een verzwakte positie; Wetsontwerp tot uitbreiding van de strafrechtelijke bescherming van bijzonder kwetsbare personen tegen mishandeling en misbehandeling; Wetsvoorstel tot wijziging van het Strafwetboek en het Wetboek van strafvordering in verband met de bescherming van kwetsbare personen; Wetsontwerp tot wijziging van het Strafwetboek met het oog op de strafbaarstelling van de mentale destabilisatie van personen en van het misbruik van personen in een verzwakte positie, *Parl. St.* Kamer 2010-11, nrs. 53K0080/007 en 53K0080/008

Ontwerp van Financiewet voor het begrotingsjaar 2012, *Parl. St.* Kamer 2011-12, nr. 53K1933/001

Wetsontwerp houdende diverse bepalingen, *Parl. St.* Kamer 2011-12, nr. 53K1952/001

Wetsontwerp houdende de middelenbegroting voor het begrotingsjaar 2012, *Parl. St.* Kamer 2011-12, nr. 53K1943/001

Ontwerp van algemene uitgavenbegroting voor het begrotingsjaar 2012 – Eerste deel, *Parl. St.* Kamer 2011-12, nr. 53K1944/001

Wetsontwerp tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse (802/1), *Hand.* Kamer 2010-11, 27 januari 2011, CRIV53PLEN015, 53

De toestand in Libië: uiteenzetting door de Eerste minister, de vice-eerste minister en minister van Buitenlandse Zaken en Institutionele Hervormingen en de minister van Landsverdediging en gedachtewisseling, *Hand.* Kamer 2010-11, 18 maart 2011, CRIV53COM162, 1

Bespreking over de voorstel van resolutie betreffende de toestand in Libië (1308/1-2), *Hand.* Kamer 2010-11, 21 maart 2011, CRIV53PLEN024, 1

Bespreking van de begrotingen en rekeningen van de Kamer en van de dotatiegerechtigde instellingen – de rekeningen van het begrotingsjaar 2009 – aanpassing van de begroting 2010 – de begrotingsvoorstellen voor het begrotingsjaar 2011 (1440/1); Kamer van Volksvertegenwoordigers: gewijzigde begroting van het begrotingsjaar 2011 (1452/1), *Hand.* Kamer 2010-11, 19 mei 2011, CRIV53PLEN035, 37

Wetsvoorstel tot wijziging van het Strafwetboek met het oog op de strafbaarstelling van de mentale destabilisatie van personen en van het misbruik van personen in een verzwakte positie (1217/1-2), *Hand.* Kamer 2010-11, 15 juin 2011, CRIBV53PLEN039, 1

Wetsvoorstel tot wijziging van de wetgeving wat de afschaffing van de Staatsveiligheid betreft (894/1-2), *Hand.* Kamer 2010-11, 23 juin 2011, CRIBV53PLEN041, 82

BIJLAGE C.
OVERZICHT VAN INTERPELLATIES, VRAGEN OM UITLEG EN MONDELINGE EN SCHRIFTELIJKE VRAGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2011 TOT 31 DECEMBER 2011)

Senaat

Vraag om uitleg van Z. Khattabi aan de minister van Justitie over 'de afzondering en de detentievoorwaarden van Nizar Trabelsi' (*Hand.* Senaat 2010-11, 19 januari 2011, nr. 5-25, 11, Vr. nr. 5-296)

Schriftelijke vraag van A. Van dermeersch aan de minister van Landsverdediging over 'Cybercriminaliteit – Stand van zaken in België – Cyberdefence' (Senaat 2010-11, 27 januari 2011, Vr. nr. 5-894)

Schriftelijke vraag van A. Van dermeersch aan de minister van Binnenlandse Zaken over 'Cybercriminaliteit – Stand van zaken in België – Cyberdefence' (Senaat 2010-11, 27 januari 2011, Vr. nr. 5-895)

Schriftelijke vraag van B. Anciaux aan de minister voor Ondernemen en Vereenvoudigen over 'Economische en industriële spionage – Maatregelen – Europees Overleg' (Senaat 2010-11, 27 januari 2011, Vr. nr. 5-966)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'Terrorisme – Recente maatregelen – Internationale samenwerking' (Senaat 2010-11, 27 januari 2011, Vr. nr. 5-976)

Schriftelijke vraag van B. Anciaux aan de minister van Binnenlandse Zaken over 'Politie – Aankoop van afluisterapparatuur – Lekken naar het buitenland' (Senaat 2010-11, 1 februari 2011, Vr. nr. 5-1114)

Vraag om uitleg van B. Anciaux aan de minister van Binnenlandse Zaken over 'de beveiliging van onze luchthavens tegen terroristische aanvallen' (*Hand.* Senaat 2010-11, 8 februari 2011, nr. 5-32, 8, Vr. nr. 5-370)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'Terrorisme – Politieraids – Evaluatie – Resultaten' (Senaat 2010-11, 8 februari 2011, Vr. nr. 5-1220)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'Veiligheid van de Staat – Werking – Parlementaire controle' (Senaat 2010-11, 8 februari 2011, Vr. nr. 5-1226)

Schriftelijke vraag van B. Anciaux aan de minister van Binnenlandse Zaken over 'Veiligheid van de Staat – Werking – Parlementaire controle' (Senaat 2010-11, 8 februari 2011, Vr. nr. 5-1227)

Vraag om uitleg van B. Anciaux aan de staatssecretaris voor Mobiliteit over 'de beveiligingsfirma op de luchthaven van Zaventem en andere strategische plaatsen in ons land' (*Hand.* Senaat 2010-11, 9 februari 2011, nr. 5-35, 4, Vr. nr. 5-372)

Schriftelijke vraag van B. Anciaux aan de minister van Binnenlandse Zaken over 'Luchthaven van Zaventem – Beveiligingsfirma – Aanbesteding' (Senaat 2010-11, 11 februari 2011, Vr. nr. 5-1329)

Schriftelijke vraag van B. Anciaux aan de minister van Landsverdediging over 'Algemene Dienst inlichting en veiligheid van de Krijgsmacht – Werking – Parlementaire controle' (Senaat 2010-11, 15 februari 2011, Vr. nr. 5-1350)

Schriftelijke vraag van A. De Croo aan de minister van Binnenlandse Zaken over 'Afluisteren van telefoongesprekken – Statistieken – Kostprijs – Transparantie' (Senaat 2010-11, 18 februari 2011, Vr. nr. 5-1379)

Schriftelijke vraag van A. De Croo aan de minister van Binnenlandse Zaken over 'Inlichtingendiensten en parketten – Afluisteren van telefoongesprekken – Frequentie – Skype' (Senaat 2010-11, 18 februari 2011, Vr. nr. 5-1381)

Schriftelijke vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'Extremistische en subversieve groeperingen – Criteria – Lijst' (Senaat 2010-11, 18 februari 2011, Vr. nr. 5-1386)

Vraag om uitleg van F. Boogaerts aan de minister van Justitie over 'terreurdreigingen' (*Hand.* Senaat 2010-11, 23 februari 2011, nr. 5-43, 9, Vr. nr. 5-295)

Vraag om uitleg van K. Vanlouwe aan de minister van Justitie over 'de inertie van de Veiligheid van de Staat bij de spionagezaak in het Justus Lipsiusgebouw' (*Hand.* Senaat 2010-11, 23 februari 2011, nr. 5-43, 12, Vr. nr. 5-305)

Vraag om uitleg van F. Bellot aan de minister van Justitie over 'het gebruik door justitie van beëdigde vertalers en tolken in strafrechtelijke onderzoeken' (*Hand.* Senaat 2010-11, 2 maart 2011, nr. 5-46, 5, Vr. nr. 5-441)

Vraag om uitleg van B. Anciaux aan de minister van Justitie over 'de zaak-Swift en de vermeende pogingen om deze zaak uit handen van het gerecht te houden' (*Hand.* Senaat 2010-11, 2 maart 2011, nr. 5-46, 14, Vr. nr. 5-475)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'de strijd tegen extreemrechtse organisaties' (Senaat 2010-11, 10 maart 2011, Vr. nr. 5-1702)

Vraag om uitleg van B. Anciaux aan de minister van Justitie over 'het advies van het Parket en van de Veiligheid van de Staat in een dossier rond een veiligheids- en bewakingsfirma' (*Hand.* Senaat 2010-11, 30 maart 2011, nr. 5-57, 14 Vr. nr. 5-592)

Vraag om uitleg van B. Laeremans aan de minister van Justitie over 'het dossier van de zes politieke moorden, toegeschreven aan Belliraj' (*Hand.* Senaat 2010-11, 30 maart 2011, nr. 5-57, 18, Vr. nr. 5-602)

Schriftelijke vraag van D. Claes aan de minister van Justitie over 'Informanten – Vergoedingen – Aantallen' (Senaat 2010-11, 30 maart 2011, Vr. nr. 5-1920)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'Belgisch afluistersysteem – Eventuele lekken naar een inlichtingendienst van een vreemde mogendheid – Maatregelen' (Senaat 2010-11, 8 april 2011, Vr. nr. 5-2058)

Schriftelijke vraag van Y. Buysse aan de minister van Justitie over 'Vaste Comités P en I – Geheim van het strafrechtelijk onderzoek – Overruling' (Senaat 2010-11, 5 mei 2011, Vr. nr. 5-2232)

Vraag om uitleg van B. Laeremans aan de minister van Justitie over 'het taalkader van de Veiligheid van de Staat' (*Hand.* Senaat 2010-11, 11 mei 2011, nr. 5-67, 23, Vr. nr. 5-765)

Schriftelijke vraag van A. De Croo aan de vice-eerste minister van Financiën over 'Cel voor financiële informatieverwerking (CFI) – Controlebevoegdheid – Terrorisme en extremisme' (Senaat 2010-11, 26 mei 2011, Vr. nr. 5-2390)

Schriftelijke vraag van A. De Croo aan de minister van Justitie over 'Cel voor financiële informatieverwerking (CFI) – Controlebevoegdheid – Terrorisme en extremisme' (Senaat 2010-11, 26 mei 2011, Vr. nr. 5-2391)

Schriftelijke vraag van B. Anciaux aan de vice-eerste minister van Financiën over 'Terrorisme – Financiering vanuit België – Gebruik van geld voortkomend uit sociale uitkeringen' (Senaat 2010-11, 26 mei 2011, Vr. nr. 5-2412)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over het 'Terrorisme – Financiering vanuit België – Gebruik van geld voortkomend uit sociale uitkeringen' (Senaat 2010-11, 26 mei 2011, Vr. nr. 5-2413)

Mondelinge vraag B. Anciaux aan de minister van Landsverdediging over 'de malaise bij de inlichtingendiensten van het leger' (*Hand.* Senaat 2010-11, 16 juni 2011, nr. 5-26, 14, Vr. nr. 5-210)

Schriftelijke vraag van R. Miller aan de minister van Buitenlandse Zaken over 'de mogelijke aanwezigheid van Belgische huurlingen in Libië' (Senaat 2010-11, 1 juli 2011, Vr. nr. 5-2664)

Schriftelijke vraag van B. Tommelein aan de minister van Justitie over 'Veiligheid van de Staat – Lezingen van haatpredikers in het buitenland – Aanwezigheid van landgenoten – Aantallen en handhaving' (Senaat 2010-11, 16 september 2011, Vr. nr. 5-3076)

Mondelinge vraag van D. Pieters aan de minister van Justitie over 'de installatie van de bestuurlijke commissie die moet toezien op de bijzondere inlichtingenmethoden' (*Hand.* Senaat 2012-11, 1 december 2011, nr. 5-37, 14, Vr. nr. 5-317)

Schriftelijke vraag van B. Anciaux aan de Eerste minister over 'Ministerieel Comité voor inlichtingen en veiligheid – Regels voor geheimhouding – Besproken onderwerpen – Parlementaire controle' (Senaat 2011-12, 23 december 2011, Vr. nr. 5-4617)

Schriftelijke vraag van K. Vanlouwe aan de Eerste minister over 'Cyberaanvallen en cybercrime – Cyberdefensie – Federaal beleid – Opmerkingen Comité I' (Senaat 2011-12, 23 december 2011, Vr. nr. 5-4291)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'Spionage – Inlichtingendiensten – Evolutie – Preventie' (Senaat 2011-12, 28 december 2011, Vr. nr. 5-4703)

Schriftelijke vraag van B. Anciaux aan de minister van Landsverdediging over 'Spionage – Inlichtingendiensten – Evolutie – Preventie' (Senaat 2011-12, 28 december 2011, Vr. nr. 5-4934)

Schriftelijke vraag van K. Vanlouwe aan de minister van Landsverdediging over 'Cyberaanvallen en cybercrime – Cyberdefensie – Noord-Atlantische Verdragsorganisatie (NAVO) – Computer Emergency Response Team (CERT) – Specifieke situatie Defensie' (Senaat 2011-12, 28 december 2011, Vr. nr. 5-4320)

Schriftelijke vraag van K. Vanlouwe aan de minister van Middenstand over 'Cyberaanvallen en cybercrime – Cyberdefensie – Computer Emergency Response Team (CERT) – BelNet – Specifieke situatie Overheidsdienst Wetenschapsbeleid' (Senaat 2011-12, 28 december 2011, Vr. nr. 5-4321)

Kamer van Volksvertegenwoordigers

Vraag van T. Veys aan de minister van Justitie over 'de radicaal islamitische vereniging 'De Middenweg' – Contacten met buitenlandse moslimextremisten' (*Vr. en Antw.* Kamer 2010-11, 14 januari 2011, QRVA53013, 33, Vr. nr. 44)

Vraag van T. Veys aan de minister van Justitie over 'de organisatie 'European Council for Fatwa and Research'' (*Vr. en Antw.* Kamer 2010-11, 14 januari 2011, QRVA53013, 35, Vr. nr. 45)

Vraag van T. Veys aan de minister van Justitie over 'de radicaal islamitische studentenbeweging 'The Union of Arab Students in Europe'' (*Vr. en Antw.* Kamer 2010-11, 14 januari 2011, QRVA53013, 41, Vr. nr. 48)

Vraag van D. Ducarme aan de minister van Justitie over 'Doorlichting van de Veiligheid van de Staat' (*Vr. en Antw.* Kamer 2010-11, 14 januari 2011, QRVA53013, 47, Vr. nr. 177)

Samengevoegde vragen van S. De Wit en S. Becq aan de minister van Justitie over 'het incident tussen een onderzoeksrechter en het gevangenispersoneel van de gevangenis van Sint-Gillis' (*Hand.* Kamer 2010-11, 18 januari 2011, CRIV53COM094, 28, Vr. nrs. 2108 en 2129)

Vraag van K. Calvo aan de minister van Binnenlandse Zaken over 'het afleveren van veiligheidsattesten door het FANC' (*Hand.* Kamer 2010-11, 26 januari 2011, CRIV53COM107, 19, Vr. nr. 2315)

Vraag van C. Brotcorne aan de minister van Binnenlandse Zaken over 'de veiligheid in onze luchthavens' (*Hand.* Kamer 2010-11, 27 januari 2011, CRIV53PLEN015, 32, Vr. nr. 017)

Vraag van R. Terwingen aan de minister voor Ondernemen en Vereenvoudigen over 'dataretentie' (*Hand.* Kamer 2010-11, 1 februari 2011, CRIV53COM113, 1, Vr. nr. 1298)

Vraag van P. Dedecker aan de minister van KMO's over 'de juridische actie door het Algemeen Rijksarchief tegen het Vlaamse archiefdecreet' (*Hand.* Kamer 2010-11, 1 februari 2011, CRIV53COM111, 3, Vr. nr. 2096)

Samengevoegde vragen van S. Van Hecke aan de minister van Binnenlandse Zaken over 'de veiligheid van de afluistersystemen van de federale politie' (*Hand.* Kamer 2010-11, 8 februari 2011, CRIV53COM121, 5, Vr. nrs. 2278 en 2279)

Samengevoegde vragen van D. Bacquelaine en B. Schoofs aan de minister van Justitie over 'de vestiging van een radicale moslimschool in Borgerhout' (*Hand.* Kamer 2010-11, 22 februari 2011, CRIV53COM139, 25, Vr. nrs. 2547 en 2587)

Vraag van J. Boulet aan de minister van Justitie over 'de afluisterapparatuur in het Justus Lipsiusgebouw' (*Hand.* Kamer 2010-11, 22 februari 2011, CRIV53COM139, 31, Vr. nr. 2578)

Samengevoegde vragen van T. Francken, K. Temmerman, R. Madrane en J. Galant aan de staatssecretaris voor Begroting over 'de rellen aan en in het gesloten asielcentrum 127*bis* te Steenokkerzeel' (*Hand.* Kamer 2010-11, 22 februari 2011, CRIV53COM140, 27, Vr. nrs. 2900, 2928, 2935 en 2946)

Vraag van B. Schoofs aan de minister van Justitie over 'de nieuwe plannen van de Moslimexecutieve' (*Hand.* Kamer 2010-11, 3 maart 2011, CRIV53PLEN021, 31, Vr. nr. 132)

Vraag van A. Colen aan de minister van Buitenlandse Zaken over 'de terreuraanslag in Moskou' (*Hand.* Kamer 2010-11, 16 maart 2011, CRIV53COM158, 19, Vr. nr. 2338)

Samengevoegde vragen van D. Thiéry en S. Bracke aan de minister van Landsverdediging over 'de beveiliging van de informatiesystemen van de Staat naar aanleiding van de

recente cyberaanvallen op Frankrijk' (*Hand.* Kamer 2010-11, 16 maart 2011, CRIV-53COM161, 34, Vr. nrs. 3280 en 3345)

Vraag van M. Gerkens aan de minister van KMO's over 'Financiering van de studie over de moord op Julien Lahaut' (*Vr. en Antw.* Kamer 2010-11, 22 maart 2011, QRVA53023, 171, Vr. nr. 107)

Vraag van E. Thiébaut aan de minister van Binnenlandse Zaken over 'Aanhouding in Antwerpen en Brussel van islamisten die verdacht worden van terrorisme' (*Vr. en Antw.* Kamer 2010-11, 23 maart 2011, QRVA53023, 239, Vr. nr. 235)

Vraag van P. Luykx aan de minister van Binnenlandse Zaken over 'de potentiële terreurdreiging' (*Hand.* Kamer 2010-11, 24 maart 2011, CRIV53PLEN025, 29, Vr. nr. 181)

Vraag van E. Thiébaut aan de minister van Justitie over 'Aanhouding in Antwerpen en Brussel van islamisten die verdacht worden van terrorisme' (*Vr. en Antw.* Kamer 2010-11, 29 maart 2011, QRVA53024, 66, Vr. nr. 385)

Vraag van T. Veys aan de minister van Binnenlandse Zaken over 'de milieugroep Groen Front!' (*Vr. en Antw.* Kamer 2010-11, 6 april 2011, QRVA53025, 35, Vr. nr. 58)

Vraag van L. Dierick aan de minister van Binnenlandse Zaken over 'opsporen van radicaliserende jongeren' (*Vr. en Antw.* Kamer 2010-11, 6 april 2011, QRVA53025, 55, Vr. nr. 244)

Vraag van G. Gilkinet aan de minister van Binnenlandse Zaken over 'Departementen – Studies – Financiering' (*Vr. en Antw.* Kamer 2010-11, 14 april 2011, QRVA53026, 73, Vr. nr. 250)

Vraag van R. Madrane aan de minister van Justitie over 'de ondertekening van een verklaring met het oog op een betere onderlinge afstemming van de initiatieven en inspanningen inzake de strijd tegen cybercriminaliteit door uzelf en uw Luxemburgse en Nederlandse ambtgenoten in Maastricht' (*Hand.* Kamer 2010-11, 27 april 2011, CRIV-53COM205, 4, Vr.nr. 3853)

Vraag van J. Van Esbroeck aan de minister van Binnenlandse Zaken over 'het bezoek aan ons land van aan terreurgroepen gelinkte Pakistani' (*Hand.* Kamer 2010-11, 27 april 2011, CRIV53COM204, 6, Vr. nr. 3930)

Vraag van S. Smeyers aan de minister van Justitie over 'de arrestatie van twee Belgen van Rwandese origine' (*Hand.* Kamer 2010-11, 27 april 2011, CRIV53COM205, 39, Vr. nr. 3958)

Samengevoegde vragen van E. Thiébaut, I. De Meulemeester en J. Van Esbroeck aan de minister van Binnenlandse Zaken over 'de mogelijke terreurdreiging in ons land naar aanleiding van de dood van Al Qaidaleider Osama bin Laden' (*Hand.* Kamer 2010-11, 4 mei 2011, CRIV53COM217, 28, Vr. nrs. 4394, 4402 en 4411)

Vraag van O. Maingain aan de minister van Justitie over 'de beveiliging van de informatiesystemen van de Staat naar aanleiding van de recente cyberaanvallen op België en Frankrijk' (*Hand.* Kamer 2010-11, 4 mei 2011, CRIV53COM219, 17, Vr. nr. 3891)

Vraag van S. Lahaye-Battheu aan de minister van Justitie over 'de risicoanalyse van het ontsnappingsgevaar bij het overbrengen van gedetineerden van de gevangenis naar het gerechtsgebouw' (*Hand.* Kamer 2010-11, 4 mei 2011, CRIV53COM219, 21, Vr. nr. 4002)

Samengevoegde vragen van I. De Meulemeester, P. Dewael, W. De Vriendt en D. Van der Maelen aan de minister van Buitenlandse Zaken over 'de dood van Osama Bin Laden' (*Hand.* Kamer 2010-11, 4 mei 2011, CRIV53COM220, 37, Vr. nrs. 4344, 4375, 4386 en 4405)

Samengevoegde vragen van C. Bastin en I. De Meulemeester aan de Eerste minister over 'de gevolgen van de dood van Osama bin Laden' (*Hand.* Kamer 2010-11, 5 mei 2011, CRIV53PLEN031, 1, Vr. nr. 265 en 266)

Samengevoegde vragen van A. Ponthier, G. Kindermans, C. Bastin, W. De Vriendt en D. Van der Maelen aan de minister van Landsverdediging over 'de gevolgen van de dood van Osama bin Laden' (Hand. Kamer 2010-11, 5 mei 2011, CRIV53PLEN031, 24, Vr. nrs. 277, 278, 279, 280 en 282)

Samengevoegde vragen van G. Annemans en P. Dewael aan de minister van Justitie over 'het profiel van de door de Staatsveiligheid gevolgde onderdanen' (*Hand.* Kamer 2010-11, 5 mei 2011, CRIV53PLEN031, 12, Vr. nrs. 273 en 274)

Vraag van S. Bracke aan de minister van Justitie over 'de doorvoer van wapens naar Iran' (*Vr. en Antw.* Kamer 2010-11, 6 mei 2011, QRVA53028, 182, Vr. nr. 407)

Vraag van K. Calvo aan de minister van Binnenlandse Zaken over 'de nieuwe kerncentrale in Borssele' (*Hand.* Kamer 2010-11, 18 mei 2011, CRIV53COM234, 19, Vr. nr. 4723)

Samengevoegde vragen van P. Vanvelthoven, E. Thiébaut, K. Calvo, C. Fonck en L. Dierick aan de minister van Binnenlandse Zaken over 'de stresstest voor kerncentrales' (*Hand.* Kamer 2010-11, 19 mei 2011, CRIV53PLEN035, 1, Vr. nrs. 307, 308, 309, 310 en 311)

Vraag van J. Van Esbroeck aan de minister van Binnenlandse Zaken over 'het bezoek aan ons land van een haatprediker' (*Hand.* Kamer 2010-11, 25 mei 2011, CRIV53COM244, 9, Vr. nr. 4756)

Vraag van K. Van Vaerenbergh aan de minister van Justitie over 'het afluisteren, kennisnemen en opnemen van privécommunicatie en -telecommunicatie' (*Hand.* Kamer 2010-11, 7 juni 2011, CRIV53COM255, 13, Vr. nr. 4855)

Vraag van P. Dewael aan de minister van Justitie over 'de aanpak van gewelddadige motorbendes' (*Hand.* Kamer 2010-11, 16 juni 2011, CRIV53PLEN040, 16, Vr. nr. 391)

Samengevoegde vragen van K. Grosemans, P. Moriau en G. Kindermans aan de minister van Landsverdediging over 'het jaarverslag van het Comité I in verband met de inlichtingendiensten van het leger' (*Hand.* Kamer 2010-11, 16 juni 2011, CRIV53PLEN040, 22, Vr. nrs. 394, 395 en 396)

Vraag van S. Bracke aan de minister van Landsverdediging over 'bedreigingen voor het Belgische grondgebied' (*Vr. en Antw.* Kamer 2010-11, 23 juni 2011, QRVA53033, 138, Vr. nr. 75)

Vraag van Z. Genot aan de minister van Justitie over 'de erkenning van de Brusselse moskeeën door de FOD Justitie' (*Hand.* Kamer 2010-11, 28 juni 2011, CRIV53COM277, 26, Vr. nr. 5436)

Samengevoegde vragen van D. Geerts en F. De Man aan de minister van Landsverdediging over 'de Algemene Dienst Inlichting en Veiligheid' (*Hand.* Kamer 2010-11, 29 juni 2011, CRIV53COM279, 4, Vr. nrs. 5317 en 5318)

Vraag van B. Somers aan de Eerste minister over 'de stijgende asielmigratie en de noodzaak om opnieuw een taskforce op te richten' (*Hand.* Kamer 2010-11, 30 juni 2011, CRIV53PLEN042, 8, Vr. nr. 428)

Vraag van E. Jadot aan de minister van Binnenlandse Zaken over 'Vooruitgang op het vlak van informatieveiligheid – Standpunt van het departement Binnenlandse Zaken' (*Vr. en Antw.* Kamer 2010-11, 7 juli 2011, QRVA53042, 65, Vr. nr. 410)

Vraag van A. Colen aan de minister van Buitenlandse Zaken over 'moslims die naar Libië zijn gereisd om deel te nemen aan de gevechten' (*Vr. en Antw.* Kamer 2010-11, 12 juli 2011, QRVA53035, 34, Vr. nr. 228)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'Saoedische moslimscholen' (*Vr. en Antw.* Kamer 2010-11, 12 juli 2011, QRVA53035, 215, Vr. nr. 183)

Vraag van K. Grosemans aan de minister van Pensioenen over 'financiering van terroristische groepen via Belgische pensioengelden' (*Vr. en Antw.* Kamer 2010-11, 18 juli 2011, QRVA53036, 150, Vr. nr. 81)

Vraag van S. Smeyers aan de minister van Sociale Zaken over de 'screening van asielzoekers door de Staatsveiligheid' (*Vr. en Antw.* Kamer 2010-11, 2 augustus 2011, QRVA53037, 245, Vr. nr. 65)

Vraag van D. Dumery aan de minister van Buitenlandse Zaken over 'het Europese 'Virtuosoproject' (*Vr. en Antw.* Kamer 2010-11, 11 augustus 2011, QRVA53038, 15, Vr. nr. 271)

Vraag van P. Dedecker aan de minister voor Ondernemen over de 'medewerkingsplicht voor internetondernemingen' (*Vr. en Antw.* Kamer 2010-11, 15 september 2011, QRVA53040, 216, Vr. nr. 156)

Samengevoegde vragen van S. De Wit, J. Galant, B. Schoofs, C. Van Cauter, S. Van Hecke, S. Verherstraeten en L. Musin aan de minister van Justitie over 'de oorzaken van de talrijke ontsnappingen dit jaar in de Belgische gevangenissen' (*Hand.* Kamer 2010-11, 4 oktober 2011, CRIV53COM303, 5, Vr. nrs. 5879, 5914, 6265, 6269, 6298, 6307, 6324, 6387 en 6388)

Samengevoegde vragen van J. Van Esbroeck en A. Ponthier aan de minister van Binnenlandse Zaken over 'een agent die werd geslagen bij een boerkacontrole' (*Hand.* Kamer 2010-11, 5 oktober 2011, CRIV53COM307, 27, Vr. nrs. 6337 en 6376)

Vraag van S. Van Hecke aan de minister van Justitie over 'een hulporganisatie als dekmantel voor inlichtingendiensten' (*Hand.* Kamer 2011-12, 12 oktober 2011, CRIV53COM309, 44, Vr. nr. 6099)

Vraag van N. Lanjri aan de staatssecretaris voor Begroting over 'Asielzoekers -Resettlementprogramma' (*Vr. en Antw.* Kamer 2011-12, 17 oktober 2011, QRVA53043, 143, Vr. nr. 157)

Vraag van B. Schoofs aan de minister van Justitie over 'de aanwezigheid van moslimfundamentalisten in de redactieraad van de Moslim Televisie en Radio Omroep' (*Hand.* Kamer 2011-12, 18 oktober 2011, CRIV53COM313, 51, Vr. nr. 6477)

Vraag van E. Jadot aan de minister van Justitie over de 'aanwezigheid van een Pakistaanse inlichtingenorganisatie op het Belgische grondgebied – Follow-up door de Veiligheid van de Staat' (*Vr. en Antw.* Kamer 2011-12, 26 oktober 2011, QRVA53044, 56, Vr. nr. 588)

Vraag van N. Lanjri aan de staatssecretaris voor Maatschappelijke Integratie over de 'beslissing om geen asielcentrum toe te laten in de buurt van het SHAPE-hoofdkwartier' (*Vr. en Antw.* Kamer 2011-12, 4 november 2011, QRVA53045, 161, Vr. nr. 87)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'de Standard Operating Procedure' (*Hand.* Kamer 2011-12, 9 november 2011, CRIV53COM331, 4, Vr. nr. 6666)

Samengevoegde vragen van D. Ducarme aan de minister van Justitie over 'de opstand in de gevangenis van Andenne' (*Hand.* Kamer 2011-12, 23 november 2011, CRIV-53COM343, 24, Vr. nrs. 7146 en 7147)

Vraag van C. Van Cauter aan de minister van Justitie over 'FOD Justitie – Personeelskosten' (*Vr. en Antw.* Kamer 2011-12, 5 december 2011, QRVA53048, 235, Vr. nr. 621)

Vraag van J. Van Esbroeck aan de minister van Binnenlandse Zaken over het 'Islamitisch-extremisme in kleinere steden en gemeenten – Personeelskosten' (*Vr. en Antw.* Kamer 2011-12, 5 december 2011, QRVA53048, 315, Vr. nr. 640)

BIJLAGE D.
DE VERKLARING VAN BERLIJN VAN DE CONFERENTIE VAN EUROPESE TOEZICHTHOUDERS[167]

7e conférence

des commissions parlementaires de contrôle des services de renseignements et de sécurité des États membres de l'Union européenne, ainsi que de Norvège et de Suisse

Berlin
les **27** et **28** octobre **2011**

Déclaration de Berlin

Les participants à la 7° conférence des commissions parlementaires de contrôle des services de renseignements et de sécurité des États membres de l'Union européenne, ainsi que de Norvège et de Suisse,

Considérant l'importance du contrôle parlementaire des services de renseignements et de sécurité dans la sauvegarde des droits fondamentaux et des principes de l'État de droit en Europe;

Conscients que l'acceptation par le grand public des activités déployées par les services de renseignements et de sécurité et la confiance en ces services dépendent aussi de l'efficacité du contrôle exercé par les parlementaires;

Conscients du rôle majeur joué par les services de renseignements et de sécurité dans les décisions de politique étrangère et de sécurité prises par les États membres de l'Union européenne;

Conscients de la contribution apportée par les activités des services de renseignements et de sécurité à la protection des régimes démocratiques en Europe face aux menaces terroristes;

Vu les conclusions des conférences de Rome, Bucarest, Lisbonne, Tallinn, Bruxelles et Berlin;

Déclarent ce qui suit:

1) plus de 20 ans après la fin de la Guerre froide et 10 ans après les attentats de New York et Washington, les services de renseignements et de sécurité sont confrontés à maints défis, au rang desquels figurent notamment les menaces que fait peser le terrorisme international sur l'État de droit démocratique;

167 Deze verklaring is alleen beschikbaar in het Frans, in het Duits en in het Engels.

2) dans un État de droit démocratique, les activités des services de renseignements et de sécurité doivent s'accompagner d'un devoir d'information et de contrôle parlementaire venant s'ajouter à la tutelle du ministre responsable, au contrôle du pouvoir judiciaire et à celui exercé par l'opinion publique;
3) les droits d'immixtion dont sont investis les services de renseignements et de sécurité pour maintenir et assurer la sécurité des citoyens européens imposent de soumettre ces services à un contrôle efficace en vue de sauvegarder les normes de l'État de droit. Il incombe dès lors d'investir les organes de contrôle parlementaire des services de renseignements et de sécurité des compétences adéquates et de leur assurer une dotation appropriée en termes de ressources humaines et matérielles;
4) face à l'internationalisation croissante de la coopération entre services de renseignements et de sécurité et à l'échange d'informations qu'induit cette évolution, il est nécessaire d'améliorer le contrôle parlementaire des services de renseignements et de sécurité en la matière;
5) nous prenons acte de la création à l'initiative de la Belgique d'un réseau d'expertise européen relatif au contrôle des services de renseignements. Baptisé ENNIR *(European Network of National Intelligence Reviewers)*, ce réseau basé sur un site internet a pour objet premier d'améliorer le contrôle démocratique des activités des services de renseignements et de sécurité et de permettre un meilleur échange entre les organes de contrôle ainsi mis en réseau. Nous soutenons la mise en œuvre de l'initiative belge, appelée à déboucher sur la constitution volontaire d'une plateforme la plus large d'échange d'expertise et d'expériences;
6) nous convenons de la nécessité et de l'utilité d'un échange d'informations intensif entre les États membres de l'UE, la Norvège et la Suisse dans le domaine du contrôle des services de renseignements et de sécurité;

BIJLAGE E.
DE WETTELIJKE REGELING INZAKE ARCHIVERING EN VERNIETIGING VAN GEGEVENS VAN DE VSSE EN DE ADIV

Na verloop van tijd verliezen ingezamelde en verwerkte gegevens veelal hun waarde voor de inlichtingendiensten. Op dat moment moet beslist worden of zij vernietigd dan wel gearchiveerd worden.

Die problematiek wordt voornamelijk geregeld in de Archiefwet van 24 juni 1955 en in zijn uitvoeringsbesluiten.[168] Maar zeker in relatie tot de inlichtingendiensten zijn er tal van andere relevante wetten: de Wet Verwerking Persoonsgegevens van 8 december 1992, de Wet betreffende de openbaarheid van bestuur van 11 april 1994, de Classificatiewet van 11 december 1998 en de Wet op de inlichtingendiensten van 30 november 1998.

Omdat de toepassing van deze wetgeving onvermijdelijk implicaties heeft op de efficiënte werking van de inlichtingendiensten en op de privacy van de personen die opgenomen zijn in de bestanden van deze diensten, heeft het Vast Comité besloten een korte juridische analyse te wijden aan dit thema.

---

168 K.B. van 18 augustus 2010 tot uitvoering van artikelen 1, 5 en 6*bis* van de Archiefwet van 24 juni 1955 (KB Archiefwet I) en K.B. van 18 augustus 2010 tot uitvoering van artikelen 5 en 6 van de Archiefwet van 24 juni 1955 (KB Archiefwet II).

1. Draagwijdte van de Archiefwet

De Archiefwet regelt verschillende aspecten: het ogenblik en de manier waarop archiefdocumenten[169] moeten overgebracht worden naar het Rijksarchief (artikel 1) waardoor zij in bepaalde gevallen openbaar worden (artikel 3), hun eventuele vernietiging (artikelen 2 en 5) en het toezicht op de stukken die niet naar het rijksarchief zijn overgebracht (artikel 6).

Tot voor kort was de verplichte overbrenging van documenten naar het Rijksarchief enkel van toepassing op '*[b]escheiden meer dan honderd jaar oud*'. In 2009 werd deze bepaling echter gewijzigd[170]: voortaan moeten '*[a]rchiefdocumenten meer dan dertig jaar oud*' via het Rijksarchief toegankelijk worden voor het publiek.[171]

Betekent dit dat de inlichtingendiensten voortaan alle documenten die 30 jaar oud zijn naar het Rijksarchief moeten overzenden? Zeker niet. Het toepassingsgebied van de Archiefwet is immers beperkt tot het zogenaamde 'dood' of statisch archief. Immers: '*Uit de verschillende bepalingen van de Archiefwet volgt dat de openbare dienstverlening van het Rijksarchief erin bestaat de dode archieven [wij onderlijnen] van de verschillende archiefvormers te bewaren en die open te stellen voor het publiek*'.[172] Dit zijn de archiefdocumenten waarvan een administratie oordeelt dat ze geen nut meer hebben voor haar werking. Het 'levend' of dynamisch archief – te weten documenten die wel nog van belang kunnen zijn en nog gebruikt kunnen worden[173] – valt niet onder de Archiefwet.[174]

Het is volkomen evident dat een document dat nog dienst doet als werkinstrument voor een overheid niet onder het toepassingsgebied van de Archiefwet kan vallen. Zo niet zou een administratie verplicht worden de documenten die zij nodig heeft in het kader van haar wettelijke opdrachten, af te staan en er desgevallend vooraf copies van te maken.

Het feit dat die administratie dergelijke documenten bewaart in wat zij mogelijks haar 'archief' noemt, verandert niets aan de zaak. Pas wanneer na verloop van tijd het praktisch nut van de 'gearchiveerde' stukken vermindert, kan bij de bezitter de wens ontstaan om zich van bepaalde overbodige stukken te ontdoen, hetzij door ze te vernietigen, hetzij door ze te verplaatsen naar een 'dood archief'. Vanaf dat ogenblik – en niet eerder – spelen de

169 Dit begrip wordt in de Archiefwet niet gedefinieerd.

170 Wet van 6 mei 2009, *BS* 19 mei 2009.

171 De inkorting van die termijn tot 30 jaar werd gekoppeld aan een overgangsperiode van 10 jaar waardoor de betrokken Rijksbesturen nog tot 23 september 2020 de tijd hebben om de nieuwe regeling toe te passen (art. 6*bis* Archiefwet en art. 2-3 KB Archiefwet I). Archiefdocumenten die op 23 september 2010 100 jaar zijn geworden moeten binnen het jaar naar het Rijksarchief worden overgebracht (art. 3, lid 2 KB Archiefwet I).

172 Advies van 23 februari 2010 van de Raad van State (*BS* 22 oktober 2010, 62835).

173 De begrippen 'levend' of dynamisch archief vormen in zekere zin een paradox. Zolang bepaalde documenten nog 'leven' – lees, nog gebruikt (kunnen) worden in het kader van de werking van de betrokken dienst – behoren zij immers niet tot het archief van die dienst, maar tot de werkdocumenten.

174 Zie Advies van 23 februari 2010 (*BS* 22 oktober 2010, 62832 e.v.) en Advies van 4 mei 2010 (*BS* 23 september 2010, 58713 e.v.) van de Raad van State. De Raad formuleerde zijn adviezen voornamelijk tegen de achtergrond van een reeds lang aanslepende discussie over de bevoegdheidsverdeling inzake Archiefbeheer tussen de federale overheid en de deelstaten. Volgens de Raad van State kan de federale overheid geen reglementering uitvaardigen die betrekking heeft op de werkdocumenten (het 'levend' archief) van overheden die onder de bevoegdheid van de deelstaten vallen. Niettemin geldt de benadering van de Raad van State ook buiten de context van deze bevoegdheidskwestie (zie voetnoot ???).

bepalingen van de Archiefwet. Immers, de documenten die voor de betrokken overheid hun praktisch nut verliezen, kunnen van belang blijven of worden omwille van hun wetenschappelijke of cultureel-historische waarde.[175]

Concreet betekent dit het volgende:

- stukken waarvan een overheidsdienst oordeelt dat hij ze niet meer nodig heeft voor zijn werking én[176] die ouder zijn dan 30 jaar, *moeten* naar het Rijksarchief worden overgebracht (art. 1, eerste en tweede lid, Archiefwet); deze stukken zijn in principe openbaar (art. 3 Archiefwet);
- stukken waarvan een overheidsdienst oordeelt dat hij ze niet meer nodig heeft voor zijn werking én die minder dan 30 jaar oud zijn, *mogen* naar het Rijksarchief worden overgebracht (art. 1, derde lid, Archiefwet); deze stukken zijn raadpleegbaar op de wijze bepaald door de Koning (art. 4 Archiefwet);
- stukken waarvan een overheidsdienst oordeelt dat hij ze niet meer nodig heeft voor zijn werking kunnen alleen vernietigd worden met toestemming van de algemene rijksarchivaris (art. 5 Archiefwet)[177];
- de archiefdocumenten die bij het Rijksarchief berusten, mogen alleen vernietigd worden met akkoord van de overheid van oorsprong (art. 2 Archiefwet);
- de (archief)stukken die bewaard worden door een Rijksbestuur staan onder het toezicht van de rijksarchivaris (art. 6 Archiefwet).

Voor de inlichtingendiensten spelen echter nog enkele bijzondere regels. Vooraleer daarop in te gaan, worden twee aspecten van de archiefwetgeving nader bekeken.

1.1. Vrijstelling(en) van overbrenging

Voor een aantal overheden – waaronder het ministerie van Defensie en dus de ADIV[178] – geldt een 'vrijstelling van overbrenging' voor archiefdocumenten van minder dan 50 jaar oud.[179] Wel moet de goede bewaring worden gewaarborgd en is de raadpleging door het publiek mogelijk is onder dezelfde voorwaarden als in het Rijksarchief. De vrijstelling geldt van rechtswege maar blijft dus beperkt tot een vrijstelling van de vereiste overbren-

---

175 Het is pas op dat ogenblik dat het volgens de Raad van State gerechtvaardigd kan zijn om een andere overheid – *in casu* de rijksarchivaris – te laten oordelen over het lot van deze documenten (Advies van 23 februari 2010 van de Raad van State (*BS* 22 oktober 2010, 62832).

176 Vóór de wetswijziging in 2009 was het evident dat stukken die de leeftijdsgrens uit de wet bereikt hadden (met name 100 jaar) meteen ook échte archiefstukken waren in de zin dat zij niet langer nodig waren voor de werking van de betrokken dienst. Het was daarom niet nodig om een onderscheid te maken tussen beide criteria. Sinds de wetswijziging in 2009 waarbij de termijn van 100 naar 30 jaar werd teruggebracht, is het daarentegen wel wenselijk om het belang van beide criteria te benadrukken. Het is immers niet onwaarschijnlijk dat stukken van 30 jaar nog nodig zijn voor de werking van bepaalde diensten zoals bijvoorbeeld politie- en inlichtingendiensten of de penitentiaire administratie. De 'bestemming die de overheid geeft aan een stuk' én de 'leeftijd ervan' moeten daarom beschouwd worden als twee apart te beoordelen en cumulatief toe te passen criteria.

177 De rijksarchivaris kan immers beslissen dat een vernietiging niet gewenst is omdat de documenten omwille van hun wetenschappelijke, historische of maatschappelijke waarde in het Rijksarchief bewaard dienen te worden.

178 Het ministerie van Justitie of de VSSE worden niet uitdrukkelijk vermeld waardoor zij niet zijn vrijgesteld.

179 Art. 9 KB Archiefwet I.

ging *sensu stricto*. Ze geldt met andere woorden enkel met betrekking tot de plaats van bewaring; niet met betrekking tot het al dan niet toegankelijk worden van de archieven. De ADIV kan zijn archiefdocumenten die niet ouder zijn dan 50 jaar dus wel zelf bewaren, maar zal niettemin moeten voorzien in de mogelijkheid voor het publiek om de archiefdocumenten die ouder dan 30 jaar zijn, te kunnen raadplegen onder dezelfde voorwaarden als in het Rijksarchief.

Artikel 10 van KB Archief I lijkt in nog een andere vrijstelling te voorzien: de rijksarchivaris kan op vraag van de overheid die het archief bezit vrijstelling van overbrenging verlenen voor een hernieuwbare termijn van tien jaar indien '*de aanvragende overheid kan aantonen dat de archieven nog een administratief nut hebben*'. Net zoals de Raad van State is het Vast Comité I van oordeel dat deze bepaling indruist tegen de Archiefwet.[180] Ze impliceert immers dat deze wet ook van toepassing is op documenten die een administratie nog gebruikt om haar wettelijke opdracht te vervullen. Het zou volkomen aberrant zijn dat een (inlichtingen)dienst ten aanzien van een archivaris moet 'bewijzen' dat bepaalde documenten nog nuttig kunnen zijn om zijn wettelijke opdracht (*in casu* de veiligheid van de Staat garanderen) uit te voeren.[181]

1.2. Toezicht door de rijksarchivaris

Artikel 6 Archiefwet geeft de rijksarchivaris de bevoegdheid toezicht uit te oefenen over de stukken die '*bewaard worden*' door een Rijksbestuur. Naar het oordeel van het Comité verwijst deze bepaling opnieuw naar 'dood archief' dat nog niet is overgebracht naar het Rijsarchief bijvoorbeeld omdat het document nog geen 30 jaar oud is.

Nu heeft de Koning deze bepaling opnieuw ruim geïnterpreteerd door het toezicht (dat betrekking heeft op de bewaring, ordening en toegankelijkheid van stukken) ook toe te laten op het 'levend' archief van besturen. De diensten zijn immers verplicht om de

---

180 Ondanks de door de Raad van State ter zake gemaakte opmerkingen heeft de Koning vastgehouden aan zijn ruime interpretatie van de Archiefwet: '*De ruime omschrijving van het begrip archieven wordt behouden in het ontwerp omdat de taken van het Rijksarchief noodzakelijk ook betrekking hebben op de levende archieven. Het Rijksarchief kan zijn taken ten aanzien van de dode archieven slechts zinvol uitoefenen in de mate het toezicht [eigen onderlijning] kan houden op de wijze waarop archieven bewaard worden op het ogenblik dat ze nog een administratief nut hebben en dus nog levend zijn. […] Ook de bevoegdheid van het Rijksarchief inzake vernietiging van levende archieven [eigen onderlijning] wordt om deze reden behouden*'. (Verslag aan de Koning bij het KB van 18 augustus 2010, *BS* 23 september 2010, 58712). Maar ook in de uitvoerende KB's zelf kunnen een aantal aanwijzingen gevonden worden die er op wijzen dat de Koning het toepassingsgebied van de Archiefwet wou uitrekken tot het 'levend' archief. Zo wordt het begrip 'archieven' erg ruim gedefinieerd als '*alle documenten die ongeacht hun datum[…] naar hun aard bestemd zijn om te berusten onder een overheid […] die ze heeft ontvangen of opgemaakt uit hoofde van zijn of haar activiteiten, zijn of haar taken of tot vastlegging van zijn of haar rechten en plichten [eigen onderlijning]*' (art. 1 KB Archiefwet I en art. 1 KB Archiefwet II).

181 Deze vrijstelling was reeds opgenomen in artikel 3 het oorspronkelijke KB van 12 december 1957 betreffende de uitvoering van de archiefwet van 24 juni 1955. Maar toen betrof het een automatisme: documenten die van onbetwistbaar administratief belang zijn moesten niet worden overgebracht. Op die manier verwoordde de Koning exact het toepassingsgebied van de Archiefwet: een document dat nog administratief nut heeft, is geen stuk dat tot het Rijksarchief kan behoren, hoe oud het ook moge wezen.

rijksarchivaris de toegang tot hun archieven (lees: alle documentatie gelet op de ruime toepassing die de Koning aan de Archiefwet heeft gegeven) te verlenen.[182] Wel is daarbij bepaald dat de noodzakelijke procedures en veiligheidsmaatregelen genomen worden om hem toegang te verlenen tot de archieven die een classificatie kregen of die persoonsgegevens bevatten en dit met inachtneming van de vigerende wetgeving.[183] Concreet betekent dit dat het toezicht geen betrekking heeft op de inhoud van documenten, maar slechts op de omstandigheden waarin 'archieven' worden bewaard en dat de betrokken inlichtingendienst kan eisen dat de archivaris over de vereiste veiligheidsmachtiging of veiligheidsattest beschikt (hij begeeft zich immers in geclassificeerde zones).

2. Bijzondere regels voor de VSSE en de ADIV[184]

2.1. Bestuursdocumenten versus archiefdocumenten

Met betrekking tot de openbaarheid/raadpleegbaarheid van bepaalde bij de inlichtingendiensten aanwezige stukken moet naast de Archiefwet ook rekening gehouden worden met de Wet Openbaarheid van Bestuur (WOB).[185] Daarin worden de voorwaarden bepaald waaronder bestuursdocumenten[186] geraadpleegd kunnen worden door het publiek. Aldus dringt zich de vraag op naar de verhouding tussen de WOB en de regels inzake openbaarheid / raadpleegbaarheid in de Archiefwet.

Het uitgangspunt daarbij is dat van zodra bestuursdocumenten zich in het Rijksarchief (of in het Rijksarchief in de provinciën) bevinden omdat zij verplicht overgebracht moesten worden (met andere woorden indien ze ouder zijn dan 30 jaar), wordt hun openbaarheid/raadpleegbaarheid geregeld overeenkomstig de bepalingen van de Archiefwet en niet langer door de Wet betreffende de openbaarheid van bestuur.[187] Datzelfde geldt ook met betrekking tot de bestuursdocumenten van de ADIV die ouder zijn dan 30 jaar maar nog niet zijn overgebracht naar het Rijksarchief.[188]

De openbaarheid/raadpleegbaarheid van bestuursdocumenten die nog geen 30 jaar oud zijn, wordt daarentegen geregeld overeenkomstig de bepalingen van de Wet van 11 april 1994. Het gaat dan om bestuursdocumenten die hetzij (1) nog nodig zijn voor de werking van de dienst en dus nog geen archiefstukken zijn; (2) hetzij niet meer nodig zijn voor de werking van de dienst en als dusdanig in 'een' archief werden neergelegd; (3) hetzij

182 Art. 10 KB Archiefwet II.

183 Art. 10 KB Archiefwet II.

184 De hieronder uiteengezette regeling is slechts ten dele van toepassing op de documenten die bij het OCAD berusten.

185 Wet van 11 april 1994 betreffende de openbaarheid van bestuur, *BS* 30 juni 1994.

186 Dit wordt zeer ruim gedefinieerd als alle informatie, in welke vorm dan ook, waarover een administratieve overheid beschikt (art. 1, lid 2, 2° WOB).

187 Dat volgt uit art. 11, lid 4 Wet betreffende de openbaarheid van bestuur. Zie *Parl.St.* Kamer 1992-93, nr. 1112/1, 22.

188 Op grond van artikel 9 KB Archiefwet I zijn de archiefdocumenten van de ADIV van minder dan 50 jaar oud vrijgesteld van overbrenging naar het Rijksarchief, althans in de mate hun goede bewaring, toegankelijkheid, *etc*… gewaarborgd blijft en het publiek deze archieven onder dezelfde voorwaarden als in het Rijksarchief kan raadplegen. De vrijstelling voor de overbrenging doet met andere geen afbreuk aan het feit dat de overige bepalingen van de Archiefwet van toepassing zijn op alle archiefstukken van de ADIV die ouder zijn dan 30 jaar.

niet meer nodig zijn voor de werking van de dienst en vrijwillig werden overgezonden aan het Rijksarchief.[189] Voor deze documenten beslist dus niet de Rijksarchivaris over de openbaarheid, maar wel de overheidsdienst zelf.[190] Net zoals voor de bestuursdocumenten die nog nuttig gebruikt worden, kan de openbaarheid geweigerd worden indien een van de uitzonderingen uit de wet kan worden ingeroepen. Voor de inlichtingendiensten is dat bijvoorbeeld '*de veiligheid of de verdediging van het land*' (art. 6 § 1, 4° WOB) of '*de belangen bedoeld in artikel 3 van de wet van 11 december 1998*' (art. 6 § 2°, 4° WOB).

2.2. Vernietiging van persoonsgegevens

Artikel 21 W.I&V stelt dat een inlichtingendienst de door hem verwerkte persoonsgegevens[191] maar mag bewaren zolang zij noodzakelijk zijn voor de doeleinden waarvoor zij werden opgeslagen.[192] Maar aangezien het artikel ook uitdrukkelijk bepaalt dat hierbij rekening gehouden moet worden met de wettelijke bepalingen betreffende het Rijksarchief, is er geen contradictie: op het ogenblik dat persoonsgegevens niet meer nuttig zijn voor de dienst (weze het na een jaar of pas na 40 jaar) moet de algemene rijksarchivaris met een eventuele vernietiging instemmen. Verzet hij zich tegen een vernietiging dan is het opnieuw aan de betrokken inlichtingendienst om te beslissen of deze gegevens bewaard worden in het eigen archief (voor de VSSE is dit enkel mogelijk voor stukken die niet ouder zijn dan 30 jaar) dan wel worden overgebracht naar het Rijksarchief (verplicht voor stukken die ouder zijn dan 30 jaar).

2.3. Vernietiging van onjuiste persoonsgegevens

Op deze algemene regel (de vernietiging kan alleen mits akkoord van de rijksarchivaris) bestaat één uitzondering: indien een persoonsgegeven onjuist blijkt, volgt onder meer uit artikel 16 § 2, 1° van de Wet Verwerking Persoonsgegevens dat dit moet worden verbeterd of vernietigd. In deze kan moeilijk de goedkeuring van de rijksarchivaris worden gevraagd. Er wordt in dit geval immers niet vernietigd omdat de persoonsgegevens in kwestie niet langer nodig zijn, maar wel omdat zij incorrect zijn. Ook vanuit historisch-wetenschappelijk oogpunt is het belangrijk dat foutieve gegevens uit databestanden verdwijnen.

---

189 Verwarring kan ontstaan omdat artikel 11, lid 1 WOB stelt dat de WOB ook van toepassing is op de bestuursdocumenten die 'in een archief zijn neergelegd'. Archief moet hier echter begrepen worden als elk archief, anders dan het Rijksarchief of het Rijksarchief in de provinciën. Overheidsdiensten kunnen immers op een bepaald moment beslissen dat de bestuursdocumenten die niet meer nuttig zijn in een archief (al dan niet in eigen beheer) worden bewaard, in afwachting van een (verplichte) overbrenging naar het Rijksarchief. De Wet van 11 april 1994 blijft ook van toepassing op de bestuursdocumenten in die archieven om te vermijden dat de openbaarheid omzeild zou kunnen worden door bepaalde documenten in een eigen archief onder te brengen (*Parl.St.* Kamer 1992-93, nr. 1112/1, 22).

190 Zie F. SCHRAM, "Archief en openbaarheid van bestuur" in R. OPSOMMER e.a. (eds.), *De archivaris, de wet en de rechtbank*, Brugge, die Keure, 2004, 16-17.

191 Deze regeling heeft dus geen betrekking op andere dan persoonsgegevens. Maar *de jure* is er geen verschil in behandeling met niet-persoonsgegevens: op het ogenblik dat ze niet meer nuttig zijn voor de inlichtingendienst, beslist de archivaris over hun verdere lot.

192 In principe moeten deze gegevens hoe dan ook vernietigd worden na een bepaalde termijn volgend op de laatste verwerking. Deze termijn moet door de Koning worden vastgelegd. Zoals het Comité reeds meermaals opmerkte, is dat tot op heden nog niet gebeurd.

2.4. Vernietiging van geclassificeerde (persoons)gegevens

Indien de inlichtingendiensten archiefdocumenten die geclassificeerd zijn maar niet langer nodig zijn voor de werking van de diensten[193], willen vernietigen, stelt zich een probleem. In principe moet de rijksarchivaris instemmen met een dergelijke vernietiging, wat impliceert dat hij – om een inschatting te kunnen maken van hun historische of wetenschappelijke waarde – kennis moet nemen van de inhoud van deze documenten. Dit veronderstelt dat hij houder is van een overeenkomstige veiligheidsmachtiging. De Classificatiewet – die van latere datum is dan de Archiefwet en als een *lex specialis* moet gezien worden – voorziet immers niet in een uitzondering voor de rijksarchivaris.[194]

2.5. Het overbrengen van geclassificeerde informatie naar het Rijksarchief

De overbrenging en opslag van geclassificeerde stukken naar het Rijksarchief impliceert enerzijds dat een aantal van zijn personeelsleden over de vereiste veiligheidsmachtiging beschikken en dat voldaan is aan alle materiële en procedurele veiligheidsvoorzieningen.

Bijkomend moet de toegang tot deze stukken beperkt blijven tot de houders van een veiligheidsmachtiging. Daarenboven mogen deze personen niet publiekelijk rapporteren over hun eventuele bevindingen.

2.6. De bescherming van de identiteit van informanten

De bescherming van de identiteit van informanten is van wezenlijk belang voor een inlichtingendienst. Deze bekommernis heeft zich ook vertaald in de Wet van 30 november 1998: artikel 13 draagt de inlichtingendiensten op te waken over de '*veiligheid van de gegevens die betrekking hebben op menselijke bronnen*'. Deze verplichting, die aanvankelijk was opgenomen in artikel 18 W.I&V, wou een 'daadwerkelijke vertrouwensovereenkomst'[195] instellen tussen elke informant en de inlichtingendienst, ook al verzocht hij niet om anonimiteit. Het was de bedoeling dit vertrouwensbeginsel vorm geven door de identiteit een classificatie te geven. Die piste werd niet weerhouden omdat men in de Kamer op dat ogenblik reeds de Classificatiewet had gestemd.[196] Concreet betekent dit dat de verplichting uit – nu – artikel 13 alleen kan nagekomen worden door de gegevens over de identiteit te classificeren. In dat geval is de identiteit van een informant een 'geclassificeerd persoonsgegeven' zodat de hierboven uiteengezette regels hierop van toepassing zijn.

---

193 Het feit dat een gegeven niet meer nuttig is voor de dienst, betekent niet automatisch dat de classificatie niet meer verantwoord zou zijn. Het document kan immers een indicatie geven van *modi operandi* die nog actueel zijn.

194 Dergelijke uitzonderingen gelden wel voor parketmagistraten, leden van de Cel voor financiële informatieverwerking en de leden van het Beroepsorgaan inzake veiligheidsmachtigingen, –attesten en -adviezen (art. 8 W.C&VM).

195 *Parl. St.* Senaat 1997-98, nr. 758/3, 11.

196 *Parl. St.* Senaat 1997-98, nr. 758/3, 18 en *Parl. St.* Senaat 1997-98, nr. 758/10, 157. In artikel 3 van de Classificatiewet staat de 'bescherming van bronnen' echter niet met zoveel woorden vermeld.

2.7. Gegevens opgenomen in veiligheids- of verificatiedossiers

Artikel 25 van de Classificatiewet bevat een bijzondere regeling voor de vernietiging van (persoons)gegevens die werden ingezameld in het kader van een veiligheidsverificatie of een veiligheidsonderzoek. Alhoewel deze bepaling verschillende hypothesen omvat, is er een gemene deler: 'Persoonlijke gegevens' – lees: persoonsgegevens – of zelfs het complete dossier moet worden vernietigd zodra het niet meer dienstig is vanuit de finaliteit waarin de gegevens waren ingewonnen of het dossier was samengesteld. Omdat de Classificatiewet een *lex specialis* vormt ten aanzien van de Archiefwet gebeurt de vernietiging hier buiten de archivaris om.

2.8. Vernietiging van illegaal verkregen BIM-gegevens

Ten slotte bevat artikel 43/6 W.I&V een specifieke regeling voor de vernietiging van gegevens die werden ingezameld op grond van een onwettig aangewende specifieke of uitzonderlijke methode. Indien het Vast Comité I een dergelijke onwettigheid vaststelt, moeten de ingezamelde gegevens worden vernietigd. In deze bepaling wordt niet uitdrukkelijk naar de Archiefwet verwezen. Bovendien handelt deze situatie niet over het vernietigen van gegevens die niet langer nodig zijn voor de inlichtingendiensten (artikel 21 W.I&V). Vanuit die invalshoek is het logisch dat de vernietiging niet afhankelijk is van de toestemming van de rijksarchivaris.

3. Conclusie en aanbevelingen

Deze analyse toont aan dat de verschillende wetten, die elk een deelaspect regelen van de problematiek van het vernietigen en archiveren van documenten van inlichtingendiensten, complementair en werkbaar zijn omdat het toepassingsgebied van de Archiefwet – zoals aangegeven door de Raad van State – beperkt is tot 'dode archieven'. Wie de Archiefwet ook van toepassing verklaart op 'levende archieven' creëert zowel op juridisch als op praktisch vlak een onwerkbaar en onontwarbaar kluwen.

Indien de inlichtingendiensten de geest en de letter van de verschillende besproken bepalingen naleven (bijvoorbeeld documenten die geen nut meer hebben ook als dusdanig aanduiden en informatie declassificeren indien mogelijk), dan zijn de diverse in het geding zijnde belangen perfect te verzoenen. Desgevallend kan Vast Comité I ter zake een toezichtonderzoek openen.

Dit neemt niet weg dat het Vast Comité I voorstander is van een systeem waarbij classificaties na een bepaalde termijn – bijvoorbeeld 30 jaar voor documenten die 'geheim' zijn geclassificeerd en 50 jaar voor 'zeer geheime' documenten – van rechtswege vervallen, tenzij zij expliciet worden hernieuwd. Dit vereist echter een aanpassing van de Classificatiewet.