RAPPORT D'ACTIVITÉS 2015
ACTIVITEITENVERSLAG 2015

Quis custodiet ipsos custodes ?

Quis custodiet ipsos custodes ? est une série de publications qui a pour objectif de stimuler une discussion approfondie sur le fonctionnement, les compétences et le contrôle des services de renseignement et de sécurité et sur le travail de renseignement. Cette série reprend notamment 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, boîte 4 à 1000 Bruxelles (02 286 29 88).

Déjà parus dans cette série

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Comité permanent R, *Rapport d'activités 2006,* 2007, 147 p.
3) Comité permanent R, *Rapport d'activités 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) 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.
10) W. Van Laethem et J. Vanderborght, *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, 2013, 565 p.
11) Comité permanent R, *Rapport d'activités 2012*, 2013, 127 p.
12) Comité permanent R, *Rapport d'activités 2013*, 2014, 212 p.
13) Comité permanent R, *Rapport d'activités 2014*, 2015, 141 p.
14) Comité permanent R, *Rapport d'activités 2015*, 2016, 131 p.

RAPPORT D'ACTIVITÉS 2015

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 2015* a été approuvé par le Comité permanent de contrôle des services de renseignements et de sécurité lors de la réunion du 16 septembre 2016.

(*soussignés*)
Guy Rapaille, président
Gérald Vande Walle, conseiller
Pieter-Alexander De Brock, conseiller
Wouter De Ridder, greffier

Rapport d'activités 2015
Comité permanent de contrôle des services de renseignements et de sécurité

ISBN 978-94-000-0782-6
D/2016/7849/167
NUR 823

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

A.M.	Arrêté ministériel
Ann. parl.	Annales parlementaires
ANS	Autorité nationale de sécurité
A.R.	Arrêté royal
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
BIA	*Belgian Intelligence Academy*
BISC	*Belgian Intelligence Studies Centre*
BNB	Banque nationale de Belgique
BNG	Banque de données nationale générale
CCB	Centre pour la cybersécurité Belgique
CEDH	Convention européenne des droits de l'homme
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 de données par les services de renseignement et de sécurité
Commission vie privée	Commission de la protection de la vie privée
CNCIS	Commission nationale de contrôle des interceptions de sécurité
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNS	Conseil national de sécurité
COC	Organe de contrôle de l'information policière
CP	Code pénal
CRIV	Compte Rendu Intégral – *Integraal Verslag*
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten* (Pays-Bas)

DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
DGCC	Direction générale du centre de crise
Doc. parl.	Documents parlementaires de la Chambre et du Sénat
EI	État islamique
EIIL	État islamique en Irak et au Levant
FRA	Agence des droits fondamentaux de l'Union européenne – *European Agency for Fundamental Rights*
FTF	*Foreign terrorist fighters*
GIA	Groupe Interforces antiterroriste
HUMINT	*Human intelligence*
INT (réglementation)	Compétence d'interception basée sur les articles 259*bis* § 5 du Code pénal et 44*bis* L.R&S
JIB	*Joint Information Box*
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	Méthode de recueil des données
NSA	*National Security Agency*
OCAM	Organe de coordination pour l'analyse de la menace
ONU	Organisation des Nations Unies
OSINT	*Open sources intelligence*
PCC	Point de contact central
PSE	Potentiel scientifique et économique
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
RUSRA	Royale Union des Services de Renseignement et d'Action
SGRS	Service général du renseignement et de la sécurité des Forces Armées
SIGINT	*Signal intelligence*

SOCMINT	*Social media intelligence*
SPF	Service public fédéral
SRS	Service/Site de réseautage social
TFN	Task Force nationale
TFUE	Traité sur le fonctionnement de l'Union européenne
TIC	Technologies de l'information et de la communication
TSA	*Transportation Security Agency* (États-Unis)
VSSE	Sûreté de l'État

PRÉFACE

Début janvier 2015, douze personnes perdent la vie lors d'une fusillade au siège de l'hebdomadaire satirique français 'Charlie Hebdo'. À peu près au même moment, une prise d'otages a lieu dans un supermarché à Paris, où cinq autres vies sont fauchées. Les auteurs sont des musulmans radicalisés qui sont liés à l'EI.

À peine quelques jours plus tard, une intervention anti-terroriste massive est menée à Verviers. Deux combattants rentrés de Syrie sont tués et un troisième est blessé. Depuis lors, les attaques terroristes (ou les projets avortés) se sont succédé en Europe et dans le reste du monde. Les 14 et 15 février, des fusillades éclatent dans le centre de la capitale danoise et font plusieurs victimes. Deux mois plus tard, un homme est arrêté en France pour avoir planifié des attaques contre des églises à Paris. Le 26 juin, un employeur est égorgé dans l'Isère, en France, et le 21 août, quelques militaires réactifs déjouent une attaque dans le Thalys. D'autres attentats sont perpétrés en dehors de l'Europe. La Tunisie, entre autres, est durement touchée.

Le 13 novembre 2015, plusieurs attentats ont lieu à Paris. Le bilan atteint 130 morts. Ces atrocités sont l'œuvre de *foreign terrorist fighters* rentrés au pays. Assez vite après les attentats, des informations indiquant l'existence d'un lien étroit avec la Belgique apparaissent. La menace terroriste n'a pas desserré son étau autour de la Belgique jusqu'à l'ultime seconde de 2015. Le feu d'artifice du Nouvel An est annulé pour la deuxième fois en quelques années[1] et le niveau de la menace est porté à 4. Mais ce n'était qu'un début : Bruxelles, Istanbul, Nice, Munich, entre autres, allaient être frappées à leur tour.

La vague d'attentats a bien entendu largement déterminé l'agenda du Comité permanent R. Des enquêtes ont été initiées sur la position d'information des services de renseignement et de l'OCAM avant les attentats de Paris, de Zaventem et de Bruxelles.

Le Comité avait toutefois ouvert, il y a longtemps déjà, plusieurs enquêtes de contrôle mettant en exergue certains aspects du suivi de l'islamisme radical. Une première enquête sur ce thème avait même été lancée avant les attentats du 11 septembre 2001. Mais à compter de 2012, le Comité a démarré nombre d'enquêtes spécifiques sur cette problématique. Le Comité a par exemple enquêté sur le suivi des extrémistes au sein de l'armée, dont l'islam radical était un des

1 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 7-19 ('II.1. L'alerte terroriste pendant les fêtes de fin d'année').

aspects examinés. Et en 2014, des enquêtes ont été ouvertes sur la *Joint Information Box* de l'OCAM (il s'agit d'une liste de personnes et de groupements radicalisés), sur l'échange d'informations entre la VSSE et l'administration pénitentiaire (où l'accent était mis sur les renseignements relatifs à des extrémistes et à des terroristes) ainsi que sur la position d'information des services de renseignement sur la problématique des *foreign terrorist fighters* et sur l'attaque manquée dans le Thalys. Les résultats de plusieurs de ces enquêtes figurent dans ce rapport annuel.

Ces mêmes attentats ont évidemment aussi déterminé l'agenda du Gouvernement belge, dont on ne compte plus les initiatives. Plusieurs de ces initiatives impactent directement le fonctionnement du Comité permanent R. Par exemple, il a récemment été chargé de contrôler – avec l'Organe de contrôle de l'information policière (COC) – la nouvelle banque de données dynamique '*foreign terrorist fighters*'. Et dans le cadre de la future réglementation '*Passenger Name Record*', une nouvelle mission de contrôle se profile pour le Comité. Il en va de même pour le contrôle des interceptions étrangères effectuées par le SGRS, qui pourrait être élargi. En effet, une révision approfondie de la Loi sur les services de renseignement du 30 novembre 1998 est en cours. Enfin, il n'est pas exclu que le nombre de dossiers à gérer par l'Organe de recours en matière d'habilitations, d'attestions et d'avis de sécurité augmente de manière significative. Et pour cause, les screenings de sécurité sont toujours plus nombreux (et plus sévères).

Dans la lutte menée actuellement contre le terrorisme barbare, chaque acteur de la chaîne de renseignement doit prendre ses responsabilités et « mettre les bouchées doubles ». À l'instar du Comité permanent R qui, là où il le peut, continuera de formuler des propositions afin d'améliorer l'efficacité des services de renseignement et de sécurité, dans le respect des valeurs démocratiques et de l'État de droit.

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

1er juin 2016

CHAPITRE I
LE SUIVI DES RECOMMANDATIONS DU COMITÉ PERMANENT R

Chaque année, le Comité permanent R formule, pour les pouvoirs législatif et exécutif, des recommandations qui portent en particulier 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 émises par le Comité en 2015 figurent au dernier chapitre du présent rapport d'activités. Ce chapitre introductif énumère les principales initiatives prises par les différents acteurs 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

I.1.1. L'OCAM ET LES DIRECTIVES EN MATIÈRE DE COOPÉRATION AVEC DES SERVICES ÉTRANGERS

L'Organe de coordination pour l'analyse de la menace a notamment pour mission d'assurer les relations internationales spécifiques avec des services étrangers ou internationaux homologues (article 8, 3° L.OCAM). Les Comités permanents R et P insistaient pour qu'une directive soit prise en la matière.[1] Il incombe en effet au Conseil national de sécurité de définir la notion de « services homologues » avec lesquels l'OCAM peut entretenir des « contacts spécifiques ». Début 2016, le Conseil national de sécurité a émis une directive en ce sens.

[1] COMITÉ PERMANENT R, *Rapport d'activités 2011*, 111 ('IX.2.4.8. La « mission à l'étranger » de l'OCAM') et 'IX.2.5. Les contacts internationaux de l'OCAM' du présent rapport.

I.1.2. ORIENTATION POLITIQUE DÉFINIE PAR LE CONSEIL NATIONAL DE SÉCURITÉ

L'ancien Comité ministériel du renseignement et de la sécurité (CMRS) a été créé comme un organe de pilotage du travail de renseignement. Sa mission était notamment, par le biais de directives, de définir la politique générale en matière de renseignements et de fixer les priorités des deux services de renseignement. En 2015, le CMRS s'est mué en Conseil national de sécurité, qui est assisté d'un Comité stratégique du renseignement et de la sécurité et d'un Comité de coordination.[2]

Le Comité estimait souhaitable que le nouveau Conseil national de sécurité – également sur indication des deux services de renseignement – reprenne son rôle de pilote.[3] Entre autres en raison des attentats survenus en 2015, le rythme des réunions s'est accéléré, et divers projets de directives ont été discutés au sein du Conseil et de ses comités exécutifs. Le pilotage s'est également concrétisé par la création de plusieurs plateformes thématiques, où sont élaborés différents aspects de la politique (de renseignement). Par exemple, en 2015, des travaux préparatoires ont été lancés en vue de développer un « plan (directeur) national du renseignement ».

I.1.3. FORMATION PERMANENTE DU PERSONNEL

La formation constitue évidemment un élément clé d'une bonne organisation. Lors de l'audit sur le fonctionnement de la Sûreté de l'État, il a cependant été constaté que « *la volonté de dispenser aux analystes une formation spécifique adaptée aux besoins de la VSSE, en ce qui concerne l'analyse* » était entravée.[4] La création officielle en 2015 de la *Belgian Intelligence Academy* (BIA) y a remédié.

I.1.4. DU PERSONNEL QUALIFIÉ EN SUFFISANCE EN MATIÈRE DE *CYBERSECURITY*, *ICT-SECURITY* ET *CYBERINTELLIGENCE*

Le Comité permanent R a constaté un manque criant de personnel qualifié pour remplir la mission relative à la sécurité de l'information. Il recommandait que

---

2 Voir J. VANDERBORGHT, 'De Trinitas 'Nationale Veiligheidsraad', 'Strategisch Comité' et 'Coördinatiecomité voor inlichting en veiligheid'', *Vigiles. Tijdschrift voor politierecht*, 2016, 1, 57-68.

3 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 118 ('IX.1.4. La nécessité d'une orientation politique par le Conseil national de sécurité').

4 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 16-17.

des moyens soient enfin alloués aux services pour leur permettre de recruter le personnel nécessaire.[5]

À la mi-2015, les appels à candidatures sont parus pour le recrutement de 24 *cyber security* et *risk prevention experts* en vue de renforcer le *Cyber Security Operations Center* du SGRS.

I.1.5. RECRUTEMENT D'UN CONSEILLER EN PRÉVENTION À LA VSSE

À la mi-2016, un conseiller en prévention a été désigné à la VSSE. En effet, dans le cadre du bien-être au travail, il est prévu que toute entité occupant de 200 à 1.000 travailleurs doit créer un service interne de prévention et de protection au travail.[6]

À la VSSE, la fonction était officiellement vacante depuis mars 2013. Jusqu'en 2015, la VSSE a fait appel au service prévention du SPF Justice (qui, chaque semaine et pendant une journée, mettait un conseiller en prévention à disposition).

I.1.6. DIRECTIVES RELATIVES AU TRAVAIL AVEC LES SOURCES HUMAINES (HUMINT)

Dans le passé, le Comité permanent R a dû constater que les directives relatives au travail avec les informateurs étaient disséminées dans plusieurs documents. C'était d'autant plus problématique que la base légale du travail avec les informateurs n'est que très sommaire (article 18 L.R&S). Bien que le Comité ait plaidé à plusieurs reprises en faveur d'une réglementation légale plus détaillée en la matière, aucune initiative législative n'avait encore été prise en ce sens. Aussi le Comité recommandait-il que la VSSE développe davantage ses directives internes et ses meilleures pratiques en ce qui concerne le travail avec les informateurs, et les transcrive dans des notes de service claires.[7] En 2011, c'était en grande partie chose faite, avec l'élaboration des *« Instructies over het werken met menselijke bronnen »*[8] et une note de service sur *« l'évaluation des informations émanant de sources humaines »*.[9] À la fin janvier 2014, la VSSE

---

5 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 109 ('IX.2.3. Recommandations relatives à la sécurité de l'information', en particulier 'IX.2.3.3. Du personnel qualifié en suffisance').

6 Arrêté royal du 27 mars 1998 relatif au Service interne pour la prévention et la protection au travail. En ce qui concerne la recommandation pour la désignation d'un conseiller en prévention, voir 'IX.2.9. La finalisation du règlement de travail' de ce rapport d'activités.

7 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 84-85 ('VIII.2.2. Une directive claire et exhaustive en matière de travail avec les informateurs').

8 « Instructions concernant le travail avec les sources humaines » (traduction libre).

9 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 3.

diffusait une nouvelle note détaillée sur la gestion des sources humaines. En janvier 2015, paraissait la note de service détaillée intitulée «*Instructions relatives au traitement des sources humaines*», qui prenait notamment en considération les recommandations formulées par le Comité.

Le Comité rappelle toutefois qu'il revient au Conseil national de sécurité d'édicter des directives en matière de travail avec les sources humaines (art. 18 L.R&S).

I.1.7. DÉSIGNATION D'UN SUPPLÉANT À LA FONCTION DE COMPTABLE EXTRAORDINAIRE

En référence aux recommandations[10] du Comité dans le cadre de son enquête de contrôle sur l'utilisation et le contrôle des «fonds spéciaux»[11], la VSSE a procédé à la désignation d'un suppléant à la fonction de comptable extraordinaire.

I.1.8. ALTERNATIVES À L'UTILISATION DES «FONDS SPÉCIAUX»

Le Comité a établi dans ses recommandations[12] que pour certaines dépenses que les fonds spéciaux ne sont pas destinés à couvrir, le SGRS doit rechercher un financement alternatif, en partenariat avec d'autres services de la Défense.

En 2015, le SGRS a déjà pu acquérir du matériel pour une somme conséquente sans puiser dans ces fonds.

I.1.9. GARANTIR LA TRANSMISSION DES COMPÉTENCES

Dans le cadre de l'audit réalisé à la VSSE, la garantie de continuité pour les fonctions dirigeantes a été examinée. Il a pu être constaté que l'outil de transmission des connaissances entre un membre du personnel en partance et son successeur se limitait à une description de tâches. Une réflexion globale sur l'organisation optimale du maintien et de la transmission des connaissances n'avait pas encore été menée. Aussi le Comité recommandait-il d'entreprendre des démarches en ce sens.[13] En 2015, le service Formation et Développement a élaboré une méthode de transmission des connaissances, mise à la disposition de tous les membres du personnel de la VSSE.

---

10 Voir 'IX.2.2. Recommandations en matière de gestion et de contrôle des «fonds spéciaux»' dans ce rapport.

11 Voir 'II.2. La gestion, l'utilisation et le contrôle des «fonds spéciaux»'.

12 Voir 'IX.2.2. Recommandations en matière de gestion et de contrôle des «fonds spéciaux»' dans ce rapport.

13 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 83.

I.2. RETOUR SUR DES RECOMMANDATIONS ANTÉRIEURES

En vertu de l'article 35, alinéa 3 L.Contrôle, le Comité permanent R doit faire rapport au Parlement «*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*». Dans ce cadre, le Comité reprend chaque année une ou plusieurs recommandations qu'il estime essentielles à la lumière de sa double finalité: le fonctionnement efficace des services et la garantie des droits fondamentaux.

I.2.1. MODALITÉS PARTICULIÈRES POUR L'ÉCHANGE DE DONNÉES ET LA COOPÉRATION AU NIVEAU INTERNATIONAL

Le Comité permanent R continue de répéter avec insistance qu'il faut mettre en œuvre les obligations visées aux articles 19 et 20 L.R&S afin de régler les modalités pour l'échange d'informations et la coopération des services de renseignement belges avec d'autres autorités, y compris étrangères.[14] Certainement en raison de la nécessité d'approfondir la coopération internationale dans la lutte contre le terrorisme, l'absence d'une telle réglementation n'est plus acceptable. Le Comité demande expressément qu'une attention spécifique soit accordée à cette matière délicate, en particulier par le Conseil national de sécurité.

I.2.2. MODALITÉS PARTICULIÈRES POUR L'ÉCHANGE DE DONNÉES ET LA COOPÉRATION AVEC LES SERVICES DE POLICE

En ce qui concerne la coopération au niveau national, le Comité avait recommandé[15] la mise en place d'une concertation structurée entre les services de renseignement et les services de police (fédérale et locale), et ce afin d'échanger des données via des procédures bien déterminées. L'absence d'accord de coopération entre ces services constitue sans aucun doute une défaillance persistante dans notre système de sécurité. Le Comité permanent R rappelle une nouvelle fois cet aspect très important.[16]

---

14 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 3-4 et *Rapport d'activités 2011*, 5-6. Les Commissions de suivi ont toujours souscrit à cette recommandation. Pour plus de détails: COMITÉ PERMANENT R, *Rapport d'activités 2013*, 4-5 et *Rapport d'activités 2014*, 5-6.

15 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 112-113.

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

I.2.3. GESTION DES INFORMATIONS AU SEIN DU SGRS

Le Comité permanent R veut attirer l'attention sur les carences persistantes dans la gestion des informations au SGRS. Les problèmes ont été signalés dès novembre 2005, à l'occasion de l'enquête de contrôle sur la manière dont le service de renseignement militaire gère et exploite les informations recueillies.[17] Le SGRS a annoncé que la structure du service serait radicalement modifiée afin de remédier à ce problème. C'est aussi pour cette raison que le thème « gestion de l'information » a été repris dans l'audit initié en 2010. Lors de cet audit, le Comité a constaté que les activités de renseignement ne bénéficiaient pas (plus) d'un appui suffisant au niveau des TIC et a attiré l'attention sur les risques évidents qui en découlent.[18] Divers devoirs d'enquête posés par le Comité en 2014 et 2015 dans le cadre d'enquêtes importantes[19] ont montré que le stockage et la gestion des informations restaient problématiques. Dès lors, le Comité recommande avec insistance le développement urgent des banques de données du SGRS (entrée de données, classification claire et générale des données, droits d'accès à partir de plusieurs divisions, digitalisation des collectes « papier », élaboration de systèmes de recherche performants…).

17 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 73-74 ('II.11.2. Gestion de l'information au sein du service de renseignement militaire').

18 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 12-13 ('II.1.5.2. Gestion de l'information' et 'IX.2.1.3. Recommandations en matière de flux d'informations et de TIC').

19 Notamment sur les *foreign terrorist fighters* (II.11.2) et sur les attentats de Paris (II.11.11).

CHAPITRE II
LES ENQUÊTES DE CONTRÔLE

En 2015, le Comité permanent R a finalisé neuf rapports d'enquête. Il a en outre rédigé deux rapports d'enquête complémentaires, à la demande de la Commission de suivi, et un rapport intermédiaire de sa propre initiative.

Sur les neuf enquêtes de contrôle finalisées, deux ont été ouvertes à l'initiative du Comité ; deux à l'initiative conjointe des Comités permanents R et P, puisqu'il s'agissait d'aspects du fonctionnement de l'OCAM ; trois l'ont été à la suite d'une plainte, et deux à la demande de la Commission de suivi parlementaire.

Les sections qui suivent traitent brièvement des neuf rapports finaux et du rapport intermédiaire (II.1 à II.10).

Les enquêtes toujours en cours (II.11) sont ensuite énumérées et brièvement décrites. Dans cette dernière rubrique, il est également fait mention des huit enquêtes de contrôle ouvertes en 2015. Six de ces nouvelles enquêtes ont été initiées à la suite d'une plainte, une à l'initiative du Comité, et une à la demande de la Commission de suivi.

Au total, le Comité a reçu 22 plaintes ou dénonciations en 2015. Après vérification de plusieurs données objectives, le Comité a rejeté 14 de ces plaintes ou dénonciations, soit parce qu'elles étaient manifestement non fondées (art. 34 L.Contrôle), soit parce que le Comité n'était pas compétent pour en traiter les motifs. Dans ces derniers cas, les plaignants ont été renvoyés, si possible, aux instances compétentes. Les huit autres plaintes introduites en 2015 ont donné lieu à l'ouverture de sept enquêtes de contrôle distinctes.

II.1. ENQUÊTE DE CONTRÔLE COMMUNE SUR LA *JOINT INFORMATION BOX* DE L'OCAM

En septembre 2012, un article de presse faisait état de problèmes avec la *Joint Information Box* (JIB).[20] Cette liste, gérée par l'OCAM, reprenait les noms de personnes et d'organisations qui jouaient un rôle clé dans le processus de radicalisation, et à l'égard desquelles certaines mesures administratives ou judiciaires pouvaient être prises. Il ne s'agissait donc pas d'une liste de

[20] K. CLERIX, 'Sharia4Belgium helpt strijd tegen radicalisering', MO* Magazine, septembre 2012.

personnes radicalisées, mais de personnes ou de groupes ayant une influence « radicalisante ». À partir de 2006, c'est la Task Force nationale (TFN), qui regroupe des représentants des différents services participant à la lutte contre la radicalisation, qui a été chargée de déterminer qui devait figurer dans la liste. Selon l'article de presse, la collaboration à l'élaboration et à l'actualisation de la JIB n'était pas toujours suffisante au sein de la TFN. Les Comités permanents R et P ont alors ouvert une enquête de contrôle afin de vérifier si cet outil contribuait de manière efficiente et efficace à l'identification et à la connaissance des éléments « radicalisants » par toutes les autorités concernées.[21] Les Comités se sont intéressés à la JIB à son niveau d'opérationnalité de 2009 à 2014.[22]

II.1.1. LA CRÉATION DE LA JIB

La JIB a été établie pour la première fois en 2005. Elle était une des émanations du Plan d'action Radicalisme (Plan R) de 2004, qui offrait un aperçu de la radicalisation au sein de la société belge et des moyens administratifs et judiciaires existants pour aborder la problématique. À l'instar du Plan d'action, la JIB visait toutes les formes de radicalisme (extrémisme musulman, extrême gauche, extrême droite et activistes défenseurs des droits des animaux). Le Plan d'action Radicalisme distinguait différents « axes » ou canaux utilisés à des fins de radicalisation : radio, télévision, prisons, centres culturels… Ces axes se retrouveront également dans la JIB.

À l'origine, la JIB a été établie en l'absence d'accords de travail concrets.[23] Au départ, la liste a été brièvement gérée par la VSSE, et ensuite par le Groupe interforces antiterroriste (GIA), qui est devenu l'OCAM en 2006. Depuis lors, l'organe de coordination a repris la gestion de cette liste.

Lors de sa création en 2006, la Task Force nationale s'est vu confier la mission de « *coordonner et suivre le recueil de renseignements dans le but de les analyser et de décider de la mention ou non dans la JIB* ». Mais il faudra attendre 2009 pour que des accords soient réellement conclus.

---

21 L'enquête a été ouverte le 13 novembre 2012 et a été finalisée en avril 2015.

22 Au cours de l'enquête, l'OCAM a fait savoir qu'il adapterait le fonctionnement de la JIB. Un groupe de travail au sein de l'OCAM a formulé plusieurs propositions dans ce cadre. L'enquête de contrôle s'est toutefois clôturée avant la mise en œuvre des modifications proposées. Les Comités permanents R et P ont constaté une intention claire de réfléchir à un nouveau processus de travail. L'OCAM a déjà tenté de pallier un des manquements signalés par les Comités, à savoir l'absence de description claire de la finalité de la JIB. Pour le reste, dans sa réaction, l'OCAM n'a fourni, à l'époque, aucun autre élément remettant en question les constats des Comités.

23 La note portant création de la JIB aurait néanmoins défini plusieurs modalités relatives au contenu et au fonctionnement de la JIB.

En attendant, les services ont tenté de suivre les matières mentionnées dans le Plan R initial. Mais sans directives claires, ils ont été confrontés à de nombreux problèmes.

II.1.2. LE FONCTIONNEMENT DE LA JIB DE 2009 À 2014

En 2009, les représentants des services concernés sont parvenus à un accord formel sur le fonctionnement de la JIB, mais pas sur la finalité ultime de cette liste. Ce point a été vivement critiqué par la majorité des acteurs et pouvait expliquer la différence de vision sur la portée des mentions des personnes ou des entités dans la liste.[24] Autre critique : le lien avec d'autres listes (comme les plans d'action des services de renseignement, la liste « groupements à suivre » et, par la suite, la liste « combattants syriens ») n'était pas toujours évident.

Depuis 2009, la mention ou la suppression d'une entité sur la liste était soumise à une procédure claire, qui s'appuyait sur des critères stricts (lesdits « paramètres »[25]) et qui requérait un consensus entre tous les services concernés.[26] C'est ainsi que collaborer à la JIB est devenu une activité assez formaliste, impliquant un investissement en temps considérable.

La JIB allait fonctionner autour des sept axes suivants : « Idéologues et prédicateurs », « Centres culturels et ASBL », « Centres de propagande », « Internet et web », « Radio et télévision », « Groupements » et « Prisons ». Les membres de la TFN étaient officiellement désignés : l'OCAM, la VSSE, le SGRS, les Polices locale et fédérale, la Cellule Antiterrorisme du SPF Affaires étrangères, la Direction générale centre de crise (DGCC) et le Parquet fédéral. Certains de ces services ont été désignés pour « piloter » un ou plusieurs axes.[27]

Pour chaque entité ajoutée à la liste, l'OCAM rédigeait une fiche reprenant toutes[28] les informations pertinentes et les mesures à prendre. L'OCAM a attiré l'attention sur les différences significatives dans le flux d'informations. Ainsi, au départ, la contribution de la VSSE était restreinte. Il est également apparu que les mesures à prendre à l'égard d'une entité faisaient souvent l'objet de longs débats entre les participants. Certains services affirmaient également qu'il ne ressortait ni de leur compétence ni de leur expertise de proposer des mesures.

---

24 Autrement dit, deux opinions circulaient : les partisans d'une JIB qui reste limitée *vs* les partisans d'un ajout beaucoup plus rapide d'entités.

25 Parmi ces paramètres figurait par exemple « l'appel au recours à la violence ». La liste des paramètres constituait une tentative d'objectivation nécessaire visant à empêcher toute mention inconsidérée d'une entité. Une entité devait répondre à au moins deux paramètres.

26 Le Collège du renseignement et de la sécurité de l'époque était informé de l'absence de consensus sur une proposition de mention à l'issue des débats.

27 Par exemple, la VSSE était le « pilote » de cinq axes.

28 À noter que certaines entités contenaient beaucoup informations, et d'autres très peu.

L'élaboration et la conservation des fiches incombaient à l'OCAM.[29] Mais ce service estimait qu'enrichir les informations fournies, en procédant à des analyses ou en demandant des informations complémentaires, ne relevait pas de ses tâches. Sa contribution était relativement minimaliste, alors que sa mission légale consiste à réaliser des analyses de la menace en matière d'extrémisme.[30]

Les services qui contribuaient à la JIB ne pouvaient pas consulter directement cette liste et les informations qu'elle contenait. Initialement, l'OCAM leur envoyait tous les six mois (ensuite, un peu plus souvent) des fiches imprimées ou un CD-ROM avec un état des lieux.

II.1.3. LE CONTENU DE LA JIB EN 2014

Les Comités permanents R et P ont contrôlé le contenu de la liste JIB en septembre 2014. La liste ne reprenait alors que les noms de 97 « entités », dont environ deux tiers de personnes et un tiers de groupements.[31]

La grande majorité des entités était liée à l'axe « Centres de propagande », suivi de l'axe « Internet et web ».

Quant aux « mesures à prendre » à l'égard des personnes mentionnées, il s'est avéré qu'elles faisaient toutes l'objet d'un signalement dans le système d'information Schengen.[32] Quatorze d'entre elles étaient également signalées dans la Banque de données nationale générale (BNG) ; deux personnes étaient spécifiquement signalées dans la BNG au niveau du contre-terrorisme. Pour le reste, il est à peine question de « mesures à prendre » dans la liste. Les Comités n'ont pas toujours pu déterminer clairement de quelle manière ces mesures à prendre pouvaient contribuer à restreindre le caractère « radicalisant » d'une personne.

Les mêmes constats ont pu être établis pour les groupements mentionnés dans la liste. Il était surtout question d'une seule mesure, à savoir la « mention dans la liste des groupements à suivre ». Cette liste est gérée par la Police fédérale sous la responsabilité du ministre de l'Intérieur. Les entités qui figurent dans cette liste font (doivent pouvoir faire) l'objet d'une attention particulière. Comme pour les personnes, les « autres mesures » citées à l'égard des groupements étaient en nombre restreint. Ici aussi, les Comités ont estimé que la plus-value de la JIB en matière de lutte contre la radicalisation était très limitée.

---

29 La conservation des données de la JIB par l'OCAM est ancrée légalement dans l'art. 9, §§ 1er et 2 L.OCAM.

30 Voir art. 8 L.OCAM.

31 En outre, les Comités ont été surpris de constater que certains noms, dont on peut raisonnablement admettre qu'ils devaient figurer dans la JIB, n'y étaient pas mentionnés, tandis que d'autres noms ne semblaient pas répondre à la finalité de la liste.

32 Ces signalements ont pour objectif de suivre les déplacements transfrontaliers d'une personne dans l'espace Schengen. Cependant, la plupart des personnes faisaient déjà l'objet d'un signalement au moment où elles ont été reprises dans la JIB.

II.1.4. CONCLUSIONS GÉNÉRALES DES COMITÉS PERMANENTS R ET P

Les Comités ont constaté que la collaboration entre les différents services dans le cadre de la JIB peut avoir des effets positifs importants. Par exemple, les services sont encouragés à se rencontrer sur une base régulière et structurée et à échanger des informations opérationnelles dans le domaine de la radicalisation. Ils sont également exhortés à présenter des résultats communs concrets, à savoir une liste des éléments radicalisants et des mesures associées. Les Comités ont toutefois estimé que le fonctionnement de la *Joint Information Box*, malgré ses 12 années d'existence, y avait peu contribué. La JIB n'offrait pas non plus une grande plus-value en matière de lutte contre la radicalisation.

Les services eux-mêmes considéraient que le fonctionnement de la JIB était fastidieux et complexe. Ils estimaient que les résultats n'étaient pas proportionnels aux efforts consentis. Plusieurs causes ont pu être avancées.

Tout d'abord, la finalité exacte de la liste était loin d'être claire. Les Comités étaient d'avis qu'une liste de personnes et de groupements qui ont un effet « radicalisant » sur leur entourage et qui doivent dès lors faire l'objet de mesures administratives, policières et judiciaires coordonnées, est précieuse, tant pour les services de sécurité que pour les responsables politiques. Cette finalité doit être formulée de façon univoque et communiquée à tous les acteurs concernés (aux niveaux fédéral, communautaire et local). À lumière de cette finalité, il convient de définir des critères objectivés qui régissent la mention ou la suppression de noms dans cette liste.

Deuxièmement, les Comités ont constaté que les mesures élaborées dans le cadre de la JIB à l'égard de vecteurs connus de radicalisation étaient marginales. La recherche de mesures adaptées était loin d'être aboutie. Les Comités ont toutefois concédé que les services qui participent au fonctionnement de la JIB ne sont pas toujours bien placés pour proposer, le cas échéant, un large éventail de mesures, soit parce qu'ils ne disposent pas toujours d'une connaissance optimale des mesures possibles, soit parce qu'ils ne sont peut-être pas responsables de leur mise en œuvre.

II.2. LA GESTION, L'UTILISATION ET LE CONTRÔLE DES « FONDS SPÉCIAUX »

Au cours des années 2011 et 2012, les autorités judiciaires ont ouvert deux enquêtes judiciaires sur l'éventuelle utilisation abusive par des agents de renseignement de fonds destinés à la rémunération d'informateurs.[33] En vertu de

[33] La première enquête, qui a été ouverte en 2011, portait sur d'éventuelles malversations financières par des agents de renseignement du SGRS. Cette enquête a été clôturée en 2013 :

sa mission judiciaire, le service d'Enquêtes R a été sollicité dans les deux enquêtes.[34] À la lumière des éléments dont le Comité permanent R a pu disposer, mettant au jour d'éventuels problèmes structurels, il a été décidé, début septembre 2012, d'ouvrir une enquête thématique sur la manière de gérer, d'employer et de contrôler les fonds destinés à la rémunération des informateurs de la VSSE et du SGRS.[35]

Toutefois, compte tenu des enquêtes judiciaires en cours, l'enquête de contrôle a été immédiatement suspendue. L'enquête a repris fin mars 2014, et le rapport final détaillé a été approuvé en juin 2015.

II.2.1. OBJET DE L'ENQUÊTE

À l'instar de tout service public, les services de renseignement se voient également allouer des fonds publics pour exercer leurs missions légales. La règle normale pour l'utilisation de ces fonds doit être une transparence parfaite et un contrôle total. Cependant, comme certaines tâches de la VSSE et du SGRS sont imprévisibles ou doivent être tenues secrètes, une partie de leur budget échappe à cette « règle normale ». Cette partie est mieux connue sous le nom de « fonds spéciaux ». Bien que le montant de ces fonds soit intégré dans le budget alloué aux services, des règles particulières s'appliquent à leur gestion, leur utilisation et leur contrôle.[36]

Le concept de « fonds spéciaux », qui n'est d'ailleurs pas légalement défini, fait d'abord penser à des fonds destinés à la rémunération d'informateurs. Or, ces fonds sont aussi utilisés à d'autres fins. Aussi le Comité a-t-il décidé d'inclure ces autres aspects dans son enquête.

Contrairement à d'autres pays, la Belgique ne dispose pas d'une instance spécifique chargée de contrôler les fonds spéciaux.[37] Dès lors, le contrôle de la bonne utilisation de ces fonds, qui représentent de l'argent public, relève en principe de la compétence de la Cour des comptes. Mais ce contrôle n'est pas vraiment effectif, vu le caractère particulier et secret de l'utilisation de cet

---

l'affaire a été classée sans suite. La seconde enquête a été ouverte en 2012 et concernait d'éventuelles malversations financières par un membre de la VSSE. Le service d'Enquêtes R a terminé ses investigations dans ce dossier en février 2014.

34 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 97-98. ('Chapitre VI. Les informations et instructions judiciaires').

35 Le Comité permanent R avait déjà réalisé, en 1994, une enquête de contrôle sur les budgets de la Sûreté de l'État et du SGRS (voir COMITÉ PERMANENT R, *Rapport d'activités 1995*, 104-108). À l'époque, l'enquête s'était limitée à une description de l'utilisation des fonds, des montants concernés, de la gestion et des procédures de contrôle.

36 En matière de planification budgétaire, les « fonds spéciaux » ne suivent pas non plus les mêmes règles que les autres rubriques budgétaires des services publics, puisque l'affectation des fonds ne doit pas être motivée ou décrite au moment de la planification.

37 En France, par exemple, où la Commission parlementaire de vérification des fonds spéciaux est chargée de cette mission.

argent.[38] Des raisons spécifiques plaident cependant pour un contrôle approprié de l'affectation de ces fonds.[39]

Le Comité s'est notamment attaché à déterminer la nature de ces « fonds spéciaux », leur montant et leur répartition. Il a également contrôlé l'utilisation des moyens et les interactions entre ces « fonds spéciaux » et les budgets « normaux ». Enfin, le Comité s'est penché sur le cadre réglementaire et a examiné quels sont les mécanismes de contrôle, et ce tant en interne (au sein des services) qu'en externe (Cour des comptes, Inspection des Finances, Comité permanent R…).

II.2.2. LE CADRE LÉGAL

Il n'existe aucune loi, aucun Arrêté royal ou ministériel, aucune circulaire ou directive ministérielle[40] définissant les fonds et réglementant leur utilisation et leur contrôle. D'un point de vue légal, il y a donc une carence.

Cependant, les deux services ont pris l'initiative d'édicter des directives sur l'utilisation des fonds, ce que le Comité a jugé positif. Mais ces directives ne suffisent pas à garantir une utilisation adéquate des fonds. Plus fondamentalement, le Comité a estimé qu'il n'appartient pas aux services de décider de l'affectation, de l'utilisation ni des procédures de contrôle des fonds, même si les services doivent évidemment garder leur autonomie dans l'utilisation opérationnelle des fonds.

Le Comité a pu constater que les membres du personnel des deux services de renseignement impliqués dans la gestion des fonds connaissent ces directives

---

38 L'affectation des fonds spéciaux de la VSSE est contrôlée par le directeur de la politique générale du ministre de la Justice. Depuis 2006, c'est le chef des Forces armées qui exerce seul le contrôle des fonds spéciaux du SGRS, et ce à raison de quatre fois par an. À la suggestion de la Cour des comptes, ce contrôle se déroule en présence du président du Comité permanent R depuis 2010 (COMITÉ PERMANENT R, *Rapport d'activités 2013*, 95 et *Rapport d'activités 2014*, 98).

39 *« There are four main reasons why external oversight of intelligence service finance is important :*
- *the principles of democratic governance require the allocation and use of public funds to be closely scrutinized ;*
- *financial records can provide insights into the behaviour and performance of intelligence services ;*
- *intelligence service secrecy limits the ability of the public to scrutinize service activity ;*
- *the nature of intelligence work creates a variety of financial risks, including the risk of the misuse of public funds. »*

in A. WILLS, 'Financial Oversight in Intelligence Services', in *Overseeing Intelligence Services – a toolkit,* H. BORN et A. WILLS (eds.), DCAF, 2012 (www.dcaf.ch), 151-180.

40 L'article 18 L.R&S stipule que dans l'exercice de leurs missions, les services peuvent avoir recours à des sources humaines « *conformément aux directives du Comité ministériel* » (devenu le Conseil national de sécurité). Ces directives devraient porter plus particulièrement sur la gestion et l'objectif de ces fonds spéciaux. De telles directives font actuellement défaut.

internes. Ce n'était pas nécessairement le cas pour les agents sur le terrain, qui n'ont recours aux fonds spéciaux que de manière occasionnelle.

II.2.3. CONSTATATIONS À L'ÉGARD DU SGRS

Contrairement à la VSSE, les fonds spéciaux alloués au SGRS ne sont pas détaillés dans la Loi budgétaire annuelle votée par le Parlement. Le budget global de fonctionnement du SGRS (frais de personnel, de fonctionnement et d'investissement) n'y figure pas non plus. Seul y est mentionné le budget global de la Défense. Les montants que le SGRS reçoit en définitive pour ses crédits ordinaires et les « fonds spéciaux » sont octroyés par la Direction générale budget et finances de la Défense.

Le Comité permanent R considère que la publication du budget global du SGRS *et* des fonds spéciaux – sans pour autant donner de détails sur, entre autres, les opérations, cibles, méthodes utilisées – contribue à la transparence des services.[41] Le Comité souligne que la publication du montant des fonds alloués à la VSSE n'a jamais mis en péril le caractère secret de ses activités. La divulgation de ces chiffres doit permettre au Parlement de mieux assumer son rôle de « contrôleur financier ».

Comme indiqué ci-dessus, le SGRS a élaboré plusieurs directives internes pour la gestion des fonds. La directive de base définit clairement les conditions d'engagement des fonds. En outre, des directives spécifiques portent sur l'utilisation de l'argent provenant des « sous-caisses ».[42] Certaines de ces directives – comme celle des sections HUMINT – sont extrêmement détaillées, tandis que d'autres « sous-caisses » ne font l'objet d'aucune mesure similaire. En ce qui concerne l'organisation de ces « sous-caisses », le Comité a constaté des manquements. Le Comité n'était pas non plus convaincu de la valeur ajoutée du recours à des « sous-caisses ». Cette méthode prêtait à confusion et augmentait considérablement le risque d'une utilisation non conforme des fonds alloués. Ainsi, le Comité a pu constater que certaines dépenses ne répondaient pas aux critères requis (par exemple, le caractère confidentiel ou secret de la mission et l'extrême urgence ne permettaient pas de suivre la procédure d'achat classique). D'autres dépenses devaient être imputées à d'autres budgets et non aux « sous-caisses » (par exemple, le paiement des indemnités réglementaires des agents civils du SGRS). Le Comité a toutefois constaté que certaines sections du SGRS (comme les sections HUMINT ou des sections déployées en zone opérationnelle) doivent être autonomes dans l'exercice de leurs missions : la mise à disposition de fonds en espèces est une

41 Voir dans le même sens : A. WILLS, *l.c.* 156 et suiv.

42 La « caisse centrale » du SGRS est subdivisée en une vingtaine de « sous-caisses » destinées à des dépenses spécifiques.

absolue nécessité. En revanche, pour d'autres « sous-caisses », le Comité s'est montré favorable à une centralisation de la gestion.

Le Comité a constaté, au moment de l'enquête, que le SGRS n'utilisait pas la comptabilité relative à la gestion des fonds comme un outil de gestion. En d'autres termes, les données comptables ne servaient pas à améliorer l'efficience et l'efficacité de la gestion du service.

Au surplus, le Comité a constaté qu'il n'y avait aucune formalisation des procédures de dépenses. Les dépenses n'étaient pas suffisamment documentées, si bien que les contrôles ultérieurs pouvaient difficilement déterminer si elles étaient conformes aux directives. Pour ce faire, il convient en effet de connaître la raison d'être de la dépense et de savoir quelle instance a pris la décision d'achat et quelle instance peut confirmer le bien-fondé de la dépense.

Toujours en ce qui concerne les « sous-caisses », il est apparu que les programmes d'informatisation dédiés à la comptabilité permettaient des manipulations a posteriori. Le Comité a recommandé de veiller à ce qu'une écriture comptable enregistrée ne puisse plus être modifiée. Le Comité a également constaté qu'un système comptable propre avait été développé pour certaines caisses et qu'il n'était pas compatible avec celui de la caisse centrale.

Un dernier constat du Comité portait sur la rémunération des sources humaines. Elles ne signaient pas de reçu pour les indemnités perçues, contrairement aux sources de la VSSE.

II.2.4. CONSTATATIONS À L'ÉGARD DE LA VSSE

Comme indiqué ci-avant, le montant des fonds spéciaux alloués à la VSSE apparaît dans le budget de ce service. Ce montant figure dans la rubrique « mesures de sécurité » et s'élevait, en 2013, à environ un million et demi d'euros. Quant à la gestion de ce budget, la VSSE a pris des directives claires et précises pour son personnel.

Depuis 2014, la VSSE utilise une « caisse électronique ». Il s'agit d'un programme informatique qui gère la comptabilité des fonds. Ce système est performant car il permet au comptable extraordinaire de contrôler en permanence et directement la comptabilité. Ce programme enregistre les écritures comptables en temps réel et ne peut être modifié par la suite, ce qui constitue un dispositif anti-fraude important.

Le comptable extraordinaire joue un rôle majeur au sein de la VSSE. Il gère les fonds et exerce un contrôle sur leur utilisation au jour le jour. Le Comité a toutefois dû constater que les fonds n'ont pas été gérés de manière optimale en l'absence du comptable extraordinaire. Le Comité a dès lors estimé qu'il est essentiel de garantir la continuité de cette fonction : il est impératif d'assurer son remplacement en cas d'absence (ce qui n'était pas le cas au moment de

l'enquête). Dans un même souci de continuité, le Comité a jugé nécessaire de décrire les procédures de fonctionnement pour la fonction de comptable extraordinaire.

Enfin, l'enquête a révélé que la VSSE disposait d'un « fonds de roulement » restreint en espèces. Selon toute vraisemblance, cet « héritage du passé » a été constitué en transférant chaque année une partie des surplus des fonds spéciaux. Selon le Comité, l'existence d'un tel capital pouvait poser un problème de légalité, d'une part, parce que le surplus annuel des fonds conservés pour enrichir ce « fonds de roulement » était comptabilisé comme une dépense et, d'autre part, parce que, sans la moindre forme de contrôle externe, la VSSE déterminait annuellement la part de ce surplus à conserver. Le Comité a considéré qu'il était indispensable de procéder à l'analyse de la légalité de ce « fonds de roulement », en collaboration avec les instances ad hoc (SPF Justice et Cour des comptes). Il conviendrait également de déterminer en fonction de quels contrôles et de quelles procédures la VSSE peut conserver les éventuels surplus annuels.

II.3. LA DÉTECTION ET LE SUIVI D'ÉLÉMENTS EXTRÉMISTES AU SEIN DU PERSONNEL DE LA DÉFENSE

Au cours des années 2011 et 2012, le SGRS a présenté plusieurs briefings au Comité permanent R sur la problématique des militaires proches des milieux d'extrême droite et des bandes criminelles de motards. Durant cette même période, des articles de presse[43] ont également évoqué la présence, au sein des Forces armées belges, de militants extrémistes, voire djihadistes. Aussi le Comité permanent R a-t-il décidé, en juin 2012, d'ouvrir une enquête de contrôle sur la manière dont le SGRS appréhende cette problématique.[44] Le Comité a abordé cette thématique à partir de cinq questions.

II.3.1. QUELLES SONT LES RÈGLES APPLICABLES AU PERSONNEL DE LA DÉFENSE EN MATIÈRE DE LIBERTÉS FONDAMENTALES ?

Chaque militaire, ou membre civil du personnel de la Défense, bénéficie des droits constitutionnels reconnus à tous, et plus particulièrement de la liberté

43 P. HUYBERECHTS, *Het Nieuwsblad*, 22 novembre 2012 ('Leger vreest infiltratie door moslim-extremisten'); A. LALLEMAND, *Le Soir*, 22 novembre 2012 ('Des islamistes dans l'armée : L'État doit mieux se protéger').

44 Le rapport final de l'enquête a été approuvé en novembre 2015.

d'expression, d'association et de culte.[45] Diverses dispositions du statut des militaires et du personnel civil de la Défense prescrivent à ces personnes de respecter la Constitution, les lois et de défendre les intérêts moraux et matériels de l'État. Un accent spécifique est mis sur les dangers inhérents à l'appartenance à des « organisations à mauvaise réputation ». L' « extrémisme » n'est donc pas interdit en tant que tel, mais certains actes ou certaines expressions de conceptions extrémistes, que ce soit dans ou hors du contexte professionnel, peuvent être sanctionnés comme contraires au statut disciplinaire, à la déontologie et aux règlements militaires.

II.3.2. QUELLE EST LA COMPÉTENCE DU SGRS DANS CETTE MATIÈRE ?

Le législateur a explicitement confié le suivi d'activités extrémistes à la VSSE (articles 7 et 8, 1°, c° L.R&S). Le SGRS n'en suit pas moins légitimement les activités extrémistes de militaires ou de civils travaillant pour la Défense, du moins dans la mesure où celles-ci représentent une menace potentielle pour ce département et pour son fonctionnement. Le SGRS est effectivement compétent pour toutes les menaces pesant sur les intérêts qu'il doit défendre. Cette surveillance s'inscrit donc dans le cadre des missions légales du SGRS, c'est-à-dire le recueil de renseignements sur des activités susceptibles de menacer l'accomplissement des missions des Forces armées ou le maintien de la sécurité militaire du personnel et des installations, ou encore la protection des secrets militaires (art. 11 L.R&S).

Le SGRS est par ailleurs chargé d'effectuer des enquêtes de sécurité en vue de l'octroi d'habilitations de sécurité au personnel de la Défense et de procéder à des vérifications de sécurité sur des candidats militaires.[46] Ces compétences ont aussi toute leur importance dans la lutte contre l'extrémisme au sein de la Défense (voir plus loin).

II.3.3. QUI EST CONSIDÉRÉ COMME EXTRÉMISTE PAR LE SGRS ?

Le SGRS a identifié, dans son Plan Directeur du Renseignement, quatre mouvements extrémistes qu'il détecte et suit au sein de la Défense : l'islam

---

45 Le SGRS estime, par exemple, que le salafisme, en tant qu'interprétation stricte de l'islam, relève de la liberté de culte. Mais à partir du moment où un croyant rejette les droits et les devoirs reconnus par les conventions internationales, la Constitution et les lois nationales, il peut être question d'extrémisme ou de radicalisme.

46 Art. 9, alinéa 1er, 9° de la Loi du 28 février 2007 fixant le statut des militaires et candidats militaires du cadre actif des Forces armées.

radical, l'extrême droite, les bandes criminelles de motards[47] et l'extrême gauche/l'éco-pacifisme. Seuls les trois premiers mouvements sont jugés prioritaires.

Les chiffres du SGRS relatifs au suivi de ces trois phénomènes dans un passé récent ont montré qu'un nombre assez limité d'individus[48, 49] était concerné, ou que dans un cas exceptionnel, il s'agissait d'un petit groupe de personnes. La majorité des quelques cas cités dans les médias concernaient d'anciens militaires qui, après leur passage à l'armée, se sont fait remarquer par leur extrémisme et/ou sont partis combattre en Syrie par conviction islamiste radicale. Lors de la clôture de cette enquête, il n'y avait toutefois aucun cas connu de militaire en service actif qui aurait franchi ce cap. En revanche, des militaires en service actif ont déjà été condamnés pour leur appartenance à un groupement terroriste d'extrême droite.[50] Au surplus, un nombre restreint de personnes ont été suivies en raison de leurs convictions extrémistes (inspirées d'ailleurs de diverses idéologies), mais sans qu'aucun fait grave n'ait été constaté.

Le Comité a estimé que l'ampleur de la problématique de l'extrémisme au sein des Forces armées restait globalement assez limitée et n'était pas plus importante que dans des catégories de population et d'âge similaires issues de la société civile. Le Comité a cependant souligné que le phénomène ne pouvait pas être sous-estimé, compte tenu des missions confiées aux militaires et des possibilités dont ils disposent.

II.3.4. COMMENT LE SGRS SUIT-IL LES ÉLÉMENTS EXTRÉMISTES AU SEIN DE LA DÉFENSE ?

Les militaires extrémistes sont détectés et suivis de plusieurs manières.

---

47 L'appartenance à des bandes criminelles de motards ne relève pas *stricto sensu* de la description légale de l'extrémisme. Il n'empêche que le SGRS peut suivre cette matière : ce genre de clubs s'intéresse à l'expérience et aux connaissances techniques du personnel militaire ainsi qu'à son accès à de l'armement et à d'autres matériels militaires. Dans ce sens, ces clubs peuvent constituer une menace pour les intérêts que le SGRS doit défendre (voir II.3.2).

48 Dans le cadre de l'islam radical, une trentaine de personnes ont attiré l'attention du SGRS au cours de la période 2011-2012. Trois d'entre elles ont fait l'objet d'une attention soutenue en raison de leur prosélytisme religieux actif au sein des Forces armées. En 2013-2014, une trentaine de cas ont également été examinés. Treize militaires ont été suivis à des degrés divers. Rien qu'en 2015, une cinquantaine de cas ont été examinés, parmi lesquels quatre cas d'implication active dans l'islam radical.

49 En ce qui concerne les militaires proches de l'extrême droite, les chiffres suivants étaient disponibles : en 2006-2007, 76 militaires actifs avaient des liens présumés avec un mouvement d'extrême droite. Entre 2010 et 2012, aucun nouveau cas n'a été constaté. En 2013 et 2014, le service a examiné deux cas.

50 En 2014, quatorze membres du groupement néonazi *Bloed, Bodem, Eer en Trouw,* parmi lesquels figuraient onze militaires, ont été condamnés pour racisme et négationnisme. Plusieurs prévenus ont été reconnus coupables de faits de terrorisme, d'association de malfaiteurs et de détention illégale d'armes.

Tout d'abord, chaque candidat militaire est soumis à une vérification de sécurité. À la lecture des travaux préparatoires de la loi, ce screening, effectué par le SGRS, vise à écarter de la sélection les candidats au passé extrémiste et/ou judiciaire.

De nombreux militaires et agents civils (c'est-à-dire ceux pour qui une habilitation de sécurité est nécessaire), une fois recrutés, sont soumis à une enquête de sécurité. Cette enquête – qui est plus pointue que la vérification et doit être renouvelée au moins tous les cinq ans – peut faire apparaître des cas d'extrémisme. La détection de circonstances susceptibles d'affecter la fiabilité d'une personne (par exemple, des accointances extrémistes), au cours d'une enquête de sécurité, peut engendrer le refus ou le retrait d'une habilitation de sécurité.

En dehors du contexte des vérifications et des enquêtes de sécurité, le SGRS fait appel aux unités, à leurs chefs de corps et aux responsables du service pour détecter des comportements suspects et les signaler.[51] Le rendement de ces sources d'informations varie selon la qualité des contacts personnels que les enquêteurs du SGRS ont établis avec les commandants d'unités. Aussi le Comité a-t-il dû constater qu'en pratique, d'éventuels faits et incidents de sécurité ne sont portés à l'attention du SGRS qu'au moment de l'enquête destinée au renouvellement de l'habilitation de sécurité, et non au moment où ils se produisent. L'examen de plusieurs cas concrets a également démontré qu'il serait utile que le personnel du SGRS et des unités militaires dispose d'indicateurs mieux élaborés pour détecter à temps des situations suspectes.

Outre ces informations « internes », le SGRS reçoit aussi des informations et des renseignements d'autres autorités publiques, c'est-à-dire de la police, des autorités judiciaires et de la VSSE, mais ce n'est pas systématique.

Enfin, le SGRS peut prendre l'initiative de mener une enquête de renseignement lorsque des indices de comportements suspects sont portés à sa connaissance. Il convient de préciser que le service n'est pas autorisé à procéder à une vérification systématique et générale pour tous les membres du personnel de la Défense, indépendamment de toute indication.[52] Le Comité a souligné qu'au moment de l'enquête, une telle possibilité ne semblait pas non plus justifiée.

Bien que l'enquête ait démontré que le SGRS remplit sa mission avec sérieux, force est de constater que celle-ci n'était pas suffisamment documentée ni

---

51 Dans la directive de la Direction générale *Human Resources*, intitulée « Adhésion à des organisations de réputation suspecte ou mauvaise », il est demandé à tous les chefs de corps d'avertir le SGRS s'ils soupçonnent un membre du personnel d'activités susceptibles de mettre en péril la sécurité militaire. En 2013-2014, le SGRS a mené une campagne d'information et de sensibilisation auprès des chefs de corps sur la problématique des bandes criminelles de motards à la réputation suspecte. Des briefings ont été donnés et une note d'information a été diffusée.

52 Ce genre de screening général et systématique n'est possible que dans le cadre de la procédure de recrutement.

chiffrée. Cela s'expliquait notamment par l'intervention de plusieurs divisions et sous-divisions. Pour une gestion optimale de la problématique, le SGRS doit impérativement disposer d'un aperçu général et actualisé de la situation.

II.3.5. QUELLES MESURES PEUVENT ÊTRES PRISES ?

Sur la base d'une vérification préalable du SGRS, un candidat militaire peut, comme cela a été dit, être écarté de la sélection. Il convient de signaler à cet égard que le nombre de candidats militaires exclus pour motif d'extrémisme est très restreint. La plupart des avis négatifs sont motivés par des faits de délinquance « ordinaire », comme la consommation de produits stupéfiants.

Les personnes qui n'obtiennent pas une habilitation de sécurité, ou qui se sont vu retirer leur habilitation en raison d'activités extrémistes, ne perdent pas pour autant leur statut de militaire ou d'agent civil. Elles pourront seulement être écartées de fonctions qui requièrent une telle habilitation. En outre, les données recueillies dans le cadre d'une enquête de sécurité ne peuvent pas être utilisées à d'autres fins (par exemple, en matière disciplinaire).

Il va de soi que les collaborateurs de la Défense qui se rendent coupables de délits ou faits disciplinaires à motivation extrémiste peuvent être suspendus, mutés, licenciés.[53] Il ne relève pas de la responsabilité du SGRS de prendre ces mesures administratives et disciplinaires, et le service n'en est pas toujours informé.[54]

II.3.6. CONCLUSION GÉNÉRALE

Le Comité permanent R a conclu que le SGRS assurait un suivi correct et plutôt efficace de l'extrémisme au sein de la Défense. L'enquête a montré que les manifestations dangereuses ont été détectées à temps, mais aussi qu'il n'y a jusqu'à présent que peu – voire pas – de cas de personnes qui, pendant leur service, se sont manifestées comme dangereux extrémistes sans être remarquées. Dans la pratique, il apparaît que la crainte du militaire extrémiste ou de la personne qui, par convictions extrémistes, suit une formation militaire est moins fondée que ce que certains médias laissaient supposer.

---

53 Lorsqu'une personne n'est plus membre de la Défense, le SGRS met un terme au suivi, sauf si cette personne garde des contacts avec d'anciens collègues de la Défense.

54 Ainsi, le SGRS a déclaré n'avoir reçu aucun feedback du licenciement, à une période donnée, de quatre extrémistes par la Défense. À propos de ces licenciements, voir : *Ann. parl. C.R.I.*, Chambre 2012-13, 17 janvier 2013, PLEN125, 1442-1444.

II.4. LE SUIVI PAR LES DEUX SERVICES DE RENSEIGNEMENT BELGES DE PERSONNES PARTIES COMBATTRE EN SYRIE : UN RAPPORT INTERMÉDIAIRE

Depuis 2013, la zone de combat syrienne exerce un fort pouvoir d'attraction sur ce que l'on appelle les *foreign terrorist fighters* (FTF)[55] des quatre coins du monde. Il s'avère que de nombreuses personnes – certainement proportionnellement – proviennent de Belgique. Aussi le Comité permanent R a-t-il décidé, en octobre 2014 (donc avant les attentats perpétrés en 2015 en France et en Belgique), d'ouvrir une enquête de contrôle relative *« à la position d'information des deux services de renseignement (VSSE et SGRS) sur le recrutement, l'envoi, le séjour et le retour en Belgique de jeunes (belges et étrangers résidant en Belgique) qui partent ou sont partis combattre en Syrie ou Irak et au transfert des renseignements aux diverses autorités »*.[56] L'enquête devait répondre aux questions suivantes : comment les services de renseignement suivent-ils la problématique, comment sont-ils organisés et quelle est leur position d'information ? L'enquête de contrôle couvrait la période allant de 2012 (à l'époque des premières informations sur les *returnees,* c'est-à-dire les combattants qui sont rentrés dans leur pays d'origine) à 2015.

Début 2015, un premier rapport intermédiaire a été rédigé pour la Commission de suivi. Les conclusions provisoires de ce rapport sont reprises ci-après.[57]

Le Comité tient d'emblée à souligner que les services de renseignement (belges) font face à des défis colossaux. Les services de renseignement ont évidemment dû réagir à certaines « crises » par le passé, mais l'impact réel sur l'organisation était de toute façon limité. Le phénomène actuel est d'un autre ordre : il est particulièrement complexe, la menace s'est développée à une vitesse encore inédite, il concerne un nombre exceptionnellement élevé de personnes, et ses ramifications s'étendent pratiquement dans le monde entier.

---

55 Au départ, on ne parlait pas de FTF. Il était plutôt question de *Belgian freedom fighters* (qui partaient pour l'Irak, la Syrie… dans un contexte humanitaire) ou, par la suite, de *Belgian foreign fighters* (avec des objectifs militaires).

56 Le Comité permanent R avait déjà mené une enquête sur des thématiques similaires. En 1999, le Comité a cherché à comprendre comment les services de renseignement suivaient la menace émanant du GIA (COMITÉ PERMANENT R, *Rapport d'activités 2001*, 81 et suiv.). Et en 2007, il s'est intéressé au suivi de l'islamisme radical par les services de renseignement (COMITÉ PERMANENT R, *Rapport d'activités 2007*, 9 et suiv.). Il y était notamment question du suivi par la VSSE et le SGRS des filières qui avaient pour but de recruter des combattants du djihad pour rejoindre les zones dites « sensibles » (Afghanistan, Pakistan, Irak…).

57 L'enquête a été clôturée en février 2016.

II.4.1. LE CONTEXTE GÉOPOLITIQUE ET LES PRIORITÉS DE LA VSSE ET DU SGRS

À partir de décembre 2010, une vague de protestations, de révoltes et de révolutions, ce que l'on a appelé « le Printemps arabe », a secoué l'ensemble du monde arabe. Des révolutions ont ébranlé l'Égypte, la Libye et le Yémen, une guerre civile a éclaté en Syrie, des manifestations et des protestations ont eu lieu au Bahreïn, en Jordanie, au Maroc, en Algérie, en Irak, à Oman et dans les territoires palestiniens, tandis que la Mauritanie, l'Arabie saoudite, le Soudan, le Liban et le Koweït ont connu ça et là des protestations. Les causes différaient d'un pays à l'autre : oppression, élections irrégulières, corruption, hausses de prix, absence de liberté politique et chômage. Les gouvernements en place étaient systématiquement pointés du doigt.

La région était depuis longtemps déjà le théâtre de violences, entre autres en Irak, où l'organisation « État islamique en Irak » (EII) était active dès octobre 2006. L'EII s'est ensuite immiscé dans la guerre civile en Syrie. Par la suite, l'organisation a pris le nom d' « État islamique en Irak et en Syrie » ou encore « État islamique en Irak et au Levant » (EIIL). En juin 2014, Abu Bakr al-Baghdadi a proclamé avoir créé un nouveau califat mondial et s'est emparé du pouvoir tant civil que religieux. Depuis lors, le mouvement terroriste est connu sous le nom « État islamique » (EI) ou DAESH.

Si de nombreux jeunes partis pour la Syrie et l'Irak depuis la Belgique et d'autres pays ont rejoint l'EI, certains ont choisi d'autres groupements armés qui luttaient contre le président syrien Assad ou qui étaient impliqués dans les conflits fratricides.

La VSSE connaissait déjà l'existence et le fonctionnement des « filières » depuis la Belgique vers des zones de conflit à l'étranger. Dès 2001, le service s'est penché sur le problème des filières irakiennes et afghanes.[58] Par exemple, la VSSE a eu affaire aux *moudjahidines* qui partaient suivre des formations paramilitaires ou participer à des combats. La problématique du retour de ces personnes et le risque de voir s'établir des réseaux ici étaient également connus à l'époque de la crise en Irak. En 2005-2006, ces filières constituaient une des priorités de la Sûreté de l'État, qui a continué à suivre la problématique dans les années qui ont suivi. Les filières depuis la Belgique vers des zones de conflit à l'étranger avaient beau être connues, la VSSE n'a pas pu prévoir en 2011 que la filière vers la Syrie deviendrait une priorité absolue. Cette année-là, la VSSE s'est intéressée, dans son Rapport d'activités, à l'insurrection populaire grandissante en Syrie, mais en ce qui concerne les filières, la Sûreté de l'État notait « *que les candidats européens en partance vont se tourner vers d'autres zones de djihad, particulièrement la Somalie et le Yémen* ». Et plus loin : « *Si la Belgique n'est, le plus souvent, pas menacée directement, notre territoire est néanmoins un lieu de passage […]. Ces*

58 COMITÉ PERMANENT R, *Rapport d'activités 2007*, 21-22.

passages fréquents d'islamistes radicaux par la Belgique peuvent s'expliquer par divers facteurs, dont la présence […] de réseaux de soutien et de falsification de documents, mais également la situation géographique centrale du pays en Europe et la présence de compagnies aériennes à bon prix.» À la mi-2012, le service faisait mention d'un premier cas de retour, et dans le *Plan d'action 2013*, il abordait pour la première fois la problématique en tant que telle. Depuis lors, la problématique syrienne est évidemment abordée de manière beaucoup plus explicite dans les Plans d'action de ce service.

Le SGRS connaissait lui aussi depuis longtemps le phénomène des filières. En 2007, le service déclarait encore, il est vrai, que par manque de personnel et d'*input*, il n'accordait pas une attention particulière aux déplacements de personnes vers des zones sensibles (Pakistan et Afghanistan). À l'en croire, il n'exerçait pas de contrôle systématique sur le phénomène, mais recevait de temps à autres des informations à ce sujet en provenance de l'étranger.

Le SGRS dispose de deux plans directeurs définissant les priorités annuelles. Le plan directeur de la Division Renseignements de sécurité est principalement axé sur les phénomènes[59] et les menaces (militaires) au niveau national, tandis que celui de la Division Renseignements porte sur les menaces étrangères. Au fil des ans, la thématique du djihadisme transnational et de l'islam radical a toujours figuré dans les deux plans directeurs, mais ce n'est qu'en 2013 que la problématique syrienne a été traitée explicitement dans le Plan directeur de la Division Renseignements. C'est cette division qui suit particulièrement la problématique des *foreign fighters* et des *returnees*. Elle joue surtout un rôle important dans la contextualisation du phénomène du terrorisme dans les régions concernées. Cette tâche s'inscrit d'ailleurs dans la mission que le SGRS s'est vu confiée par la Circulaire du 25 septembre 2014 relative à la politique d'information et aux mesures prises dans le cadre des poursuites à l'encontre des *foreign fighters* résidant en Belgique.[60] Pour aboutir à une approche globale du phénomène du «terrorisme», le SGRS a réuni le personnel de ces deux divisions pour former une *Joint Cell*. Comme cela a été dit, le SGRS étudie la problématique syrienne dans un contexte géopolitique large, comme en témoigne la création de cette *Joint Cell*, qui traite à la fois les aspects plus nationaux et les ramifications étrangères de la problématique.

---

59 Au sein de cette Division, le département qui s'occupe de la «Sécurité' (l'ancienne Division S) joue également un rôle dans le cadre du suivi du phénomène «extrémisme», mais spécifiquement à la Défense. Il doit détecter les membres du personnel qui, par leur appartenance à des groupements ou des idéologies extrémistes (djihadistes) ou leur rapprochement avec ces groupements, sont susceptibles de représenter un risque de sécurité pour la Défense (voir aussi Chapitre II.3 concernant l'extrémisme au sein de l'armée).

60 Cette circulaire a été remplacée par la Circulaire des ministres de l'Intérieur et de la Justice du 21 août 2015 relative à l'échange d'informations et au suivi des *foreign terrorist fighters* provenant de Belgique. Cette mission n'y figure plus.

II.4.2. LE VOLUME DE TRAVAIL, LE PERSONNEL ET LES MOYENS ENGAGÉS : UNE PREMIÈRE ÉVALUATION

Le Comité a constaté que la crise syrienne avait eu un impact considérable sur le fonctionnement de la VSSE. Les indicateurs quantitatifs relatifs au volume de travail (c'est-à-dire les flux d'informations entrants et sortants ainsi que le nombre de méthodes particulières de renseignement mises en œuvre) montraient un accroissement très net. Mais ce volume de travail n'était pas compensé par un renforcement numérique des services : il était absorbé par une mobilité interne du personnel, par une réorientation de collaborateurs sur la question syrienne ou encore par la prestation d'heures supplémentaires. L'augmentation du volume de travail posait problème. Et pour cause, l'ensemble des matières devant être suivies par la VSSE pouvait s'en trouver négligé. La charge de travail qui reposait sur les collaborateurs directement concernés était lourde. Si le Comité permanent R a pu constater que les services et les personnes concernées effectuaient leurs tâches avec assiduité et enthousiasme, il considérait que cette situation était risquée et précaire. Des solutions structurelles devaient être trouvées. Par ailleurs, le Comité permanent R a attiré l'attention sur une lacune spécifique : des fonctions de cadre vacantes n'étaient pas pourvues de manière systématique. Il convenait d'y remédier.

Comme à la VSSE, le volume de travail a considérablement augmenté au SGRS.[61] La mobilité interne du personnel a permis d'y faire face, du moins partiellement. Le Comité a également constaté que le SGRS avait initié toute une série de projets depuis 2010 (entre autres en matière de CYBERHUMINT, HUMINT, OSINT et SOCMINT) afin d'améliorer sa position d'information sur le terrorisme international. La problématique de la crise syrienne et des *Belgian foreign fighters* en faisait évidemment partie. Le Comité estimait qu'il y avait lieu de surveiller l'état d'avancement de ces projets.

II.4.3. L'INFLUENCE SUR L'ORGANISATION ET SUR LA STRATÉGIE : UNE PREMIÈRE ÉVALUATION

Le Comité permanent R considérait que le dossier syrien était un moment clé, tant pour les services de la VSSE directement concernés que pour le service de renseignement dans son ensemble. Des éléments indiquaient que le dossier syrien servait de catalyseur de changement dans toute l'organisation. Par exemple, une nouvelle stratégie, qui devait se traduire par des modifications

[61] Dans ce premier rapport intermédiaire, le Comité s'est essentiellement limité à un examen du suivi de la problématique syrienne d'un « point de vue national ». En d'autres termes, en ce qui concerne le SGRS, les données ne tenaient pas compte des efforts de la Division Renseignements, qui est surtout active à l'étranger.

structurelles, était en cours de formulation. Il était question d'une stratégie en tant que telle (c'est-à-dire la définition des matières nécessitant plus ou moins d'attention), mais aussi de la transition entre la situation actuelle *(as-is)* et la situation future souhaitée *(to-be)*. Une telle transition va au-delà d'un « simple » glissement de structures et de personnel ; elle touche également au cœur du travail du renseignement, c'est-à-dire à l'élaboration d'une position d'information dans certaines matières. Ce processus prend généralement de nombreuses années et requiert un haut degré de spécialisation. Cela signifie qu'il convient d'adopter une vision à long terme, puisqu'une matière qui semble moins importante aujourd'hui peut devenir une priorité demain.

Pour sa part, le SGRS tentait depuis plusieurs années déjà une approche thématique de la problématique du terrorisme (international). Dans la même optique, en 2010, la capacité d'analyse en matière de terrorisme de la Division Renseignements et de l'ancienne Division *Counter-intelligence* a été réunie en un seul bureau. En 2013, l'examen détaillé du fonctionnement de ce bureau a mis au jour des imperfections. Aussi, en 2014, le SGRS a-t-il procédé à une réorganisation et transformé le bureau en *Joint Cell*. Le Comité permanent R a conclu que le SGRS disposait ainsi d'une structure d'étude et de suivi du radicalisme, du terrorisme et des filières. Il a néanmoins ajouté que cette cellule commune était confrontée à des défis majeurs : une gestion claire, une diversité de bases de données, le non-remplacement de certains membres du personnel…

II.5. LES MEMBRES DU PERSONNEL DES SERVICES DE RENSEIGNEMENT ET LES MÉDIAS SOCIAUX

Ces dernières années, les réseaux sociaux tels que Facebook, LinkedIn et Netlog se sont considérablement développés et comptent un nombre considérable d'utilisateurs dans le monde entier. Depuis lors, les services de réseautage social (SRS) font partie intégrante de la vie quotidienne de très nombreuses personnes.

En novembre 2012, la presse belge a publié des informations selon lesquelles des membres du personnel des services de renseignement belge auraient exposé publiquement leur qualité professionnelle sur ces réseaux sociaux.[62] Ce qui ne serait pas sans risque : selon une source anonyme du monde du renseignement,

62 N. VAN HECKE, *De Standaard,* 26 novembre 2012 ('Belgische spionnen online te vinden') ; X., *7sur7.be*, 26 novembre 2012 ('Des espions belges s'exposent sur le net') ; K. VAN EYKEN, *Het Laatste Nieuws*, 26 novembre 2012 ('Belgische spionnen online te vinden'). Ces informations ont même été reprises dans la presse internationale : C. DEWEY, *The Washington Post*, 26 novembre 2012 ('Belgian intelligence workers outed on Facebook, LinkedIn') ; X., *Voix de la Russie*, 27 novembre 2012 ('Les espions belges se sont déclassifiés sur les réseaux sociaux').

un collaborateur d'un service de renseignement qui divulgue sa fonction s'expose en effet à des manifestations d'hostilité ou à des manœuvres d'approche de la part de services étrangers.

À la demande de la Commission de suivi du Sénat de l'époque, le Comité a ouvert une enquête en décembre 2012. En effet, le Sénat souhaitait recevoir davantage d'informations sur l'ampleur du phénomène, sur les risques qui y sont associés et sur les mesures qui peuvent être prises.[63] L'enquête a été clôturée en avril 2015 et les résultats ont été discutés en juillet 2015 au sein de la nouvelle Commission de suivi de la Chambre. Il est ressorti de ces discussions que les parlementaires souhaitaient obtenir des informations supplémentaires. Aussi le Comité a-t-il mené une enquête complémentaire afin de déterminer si les deux services de renseignement avaient pris des directives contraignantes sur la problématique, quelles actions ils avaient entreprises à l'égard des membres du personnel actifs sur les SRS et ce qu'il était advenu de leur profil. La Commission de suivi souhaitait également savoir s'il était légalement possible d'interdire à des membres du personnel de services de renseignement toute activité sur les SRS, y compris dans la sphère privée. En ce qui concerne ce dernier aspect, le Comité permanent R a recueilli l'avis de la Commission de la protection de la vie privée.[64] L'enquête complémentaire a été clôturée en décembre 2015.

Les résultats des enquêtes initiale et complémentaire sont repris ci-dessous.

II.5.1. L'AMPLEUR DU PHÉNOMÈNE

La VSSE a déclaré que peu après la publication des articles de presse de 2012, elle avait vérifié si des collaborateurs avaient exposé publiquement leur qualité professionnelle sur LinkedIn. Selon la VSSE, aucun cas n'aurait été relevé. Par contre, il n'a pas été possible pour la VSSE de procéder à une telle vérification sur Facebook, faute, à cette époque, d'un accès aux profils des utilisateurs.

Le SGRS a lui aussi déclaré ne pas avoir connaissance de cas où des membres de son personnel auraient divulgué leur profession sans autorisation.[65] Le contrôle portait ici sur quatre services de réseaux sociaux.

En 2014, le Comité a lui-même effectué un contrôle restreint sur LinkedIn. Il a relevé le nom de 17 personnes affichant une qualité de membre d'un des deux services. À la demande du Comité, la VSSE a confirmé que cinq membres actifs

---

63 Le Sénat souhaitait également un examen de la problématique pour le personnel de l'OCAM. Une enquête de contrôle commune a dès lors été ouverte en collaboration avec le Comité permanent P (voir Chapitre II.6).

64 Voir Avis n° 45/2015 du 13 novembre 2015 relatif à la demande d'avis des Comités R et P quant à la possibilité d'interdire aux membres des services de renseignement et de l'OCAM d'avoir une activité, même à titre privé, sur les réseaux sociaux (https://www.privacycommission.be/fr/avis-1?page=2).

65 Pour certaines fonctions, il est évident que la profession est rendue publique (par exemple, le chef de service, les personnes de contact pour les recrutements et les représentants syndicaux).

et deux anciens membres de son service étaient actifs sur LinkedIn et y mentionnaient leur (ancienne) profession.[66, 67] Quatre personnes prétendaient être membres du service, alors qu'il n'en était rien. Quant au SGRS, il s'est avéré que six membres actifs et deux anciens membres étaient actifs sur ce SRS. Cependant, toutes ces personnes ne se présentaient pas explicitement comme membres du SGRS, mais plutôt comme membres de la Défense. Leur fonction pouvait néanmoins être identifiée grâce aux données postées sur le réseau. Ces deux anciens collaborateurs allaient jusqu'à divulguer des données sensibles.[68]

Quant à l' « ampleur du phénomène », le Comité a conclu, d'une part, qu'elle était très limitée et, d'autre part, qu'avec le temps, les services avaient acquis une meilleure vision de ces réseaux. Les deux services n'en ont pas moins avoué leur difficulté de se faire une idée précise du nombre de leurs agents qui sont actifs sur les SRS. Comme indiqué, la VSSE n'a pas pu contrôler le phénomène à l'origine, puisqu'elle ne disposait pas d'un profil sur les réseaux concernés.

II.5.2. LES RISQUES ASSOCIÉS À L'UTILISATION DES SERVICES DE RÉSEAUTAGE SOCIAL

L'utilisation des SRS comporte naturellement des risques « généraux », comme une atteinte à la vie privée ou une éventuelle utilisation abusive de données à caractère personnel. Mais le Sénat souhaitait être informé des risques spécifiques pour les agents concernés et pour le service dont ils font partie.

Il est apparu que ni la VSSE ni le SGRS n'ont analysé les risques spécifiques liés au phénomène.[69] Pourtant, il est évident que de tels risques existent : des informations sensibles ou classifiées peuvent (involontairement) être compromises ; des services étrangers peuvent tenter de recruter des agents belges sur la base d'une analyse de données personnelles ; l'identité Internet peut être reprise et conduire à la publication de fausses informations ; certaines

66 D'autres membres de la VSSE ont également été repérés sur ce réseau, mais sans que leur profession y soit mentionnée.

67 Selon la VSSE, lorsque le profil d'un collaborateur de la VSSE fait directement ou indirectement référence au service, l'intéressé est prié (il n'y est donc pas officiellement contraint) de supprimer la référence visée de son profil. L'incident serait néanmoins repris dans le dossier de sécurité de l'agent concerné.

68 À la demande du Comité, le SGRS a indiqué que *« les profils des membres du personnel trouvés sur les médias sociaux ont été supprimés ou modifiés de manière à ce qu'il ne soit plus possible d'établir le moindre lien avec leur profession »*. Le SGRS n'en avait toutefois pas donné l'ordre officiellement.

69 En 2009, une étude a été réalisée au sein du SGRS sur la protection des données sensibles dans des unités opérationnelles de l'armée. Cette étude a notamment fait apparaître que des militaires en mission échangeaient parfois (involontairement) sur les SRS des informations sensibles liées aux opérations, aux plans militaires, à l'infrastructure, au matériel et au personnel.

informations peuvent être utilisées à des fins de chantage; des agents et leur famille peuvent devenir la cible d'actions violentes…[70]

Sans surprise, l'absence de vision de la problématique au départ (voir ci-dessus) explique notamment que les deux services n'avaient pas pleinement conscience des risques. Pour le Comité, certaines réponses de la VSSE indiquaient une réelle sous-estimation des risques. Par la suite, la direction du service s'est néanmoins montrée disposée à leur accorder l'attention requise. Le Comité a alors constaté une évolution favorable depuis 2014.

II.5.3. LES MESURES PRISES OU SUSCEPTIBLES DE L'ÊTRE

Plusieurs mesures peuvent être prises pour circonscrire ou éliminer les risques décrits ci-dessus. Le Comité a étudié différentes pistes et a interrogé la VSSE et le SGRS à cet égard.

Tout d'abord, il est possible d'envisager d'interdire purement et simplement la présence sur les SRS ou de limiter cette interdiction aux réseaux TIC du service. Une telle interdiction n'a jamais été décrétée ni par la VSSE ni par le SGRS, mais l'utilisation des ressources TIC du service à des fins privées a été réglementée.

Selon la Commission de la protection de la vie privée, l'interdiction d'activités strictement personnelles sur des médias sociaux en dehors du lieu de travail et des heures de bureau serait excessive. Cette interdiction peut donc être imposée sur le lieu de travail et pendant les heures de bureau. L'employeur dispose alors d'un droit de contrôle (qui n'est pas illimité). Les instructions en vigueur doivent évidemment être portées préalablement à la connaissance des agents concernés.

Une autre possibilité consiste à établir des règles concernant les activités sur les SRS dans la sphère privée (et donc ne pas les interdire purement et simplement). La liberté d'expression n'étant pas un droit absolu, il est possible de protéger d'autres intérêts (comme la sûreté de l'État ou la sécurité des militaires). Au moment de l'enquête, la VSSE n'avait pas encore pris de directive spécifique relative à l'utilisation des SRS par ses collaborateurs. Mais les impératifs du secret professionnel et de la discrétion, y compris dans la sphère privée, étaient constamment rappelés au personnel. Les membres du personnel doivent notamment veiller à ne pas faire état, directement ou indirectement, de leur fonction ou de celle d'un collègue sur les médias sociaux. La Commission de la protection de la vie privée a estimé qu'une telle interdiction était justifiée. La VSSE sensibilise également son personnel en ce sens lors de briefings. En mai 2014, la VSSE a annoncé son intention de rédiger une directive spécifique en matière d'utilisation des SRS.

---

70 Certains de ces risques ont été décrits dans la note cadre du 13 mai 2013 relative à l'utilisation des médias sociaux par les membres et services de la Police fédérale. Le Comité permanent R a estimé que ce document pouvait être pris en considération par les services de renseignement.

Au SGRS, il n'y avait pas non plus d'instructions spécifiques concernant l'usage privé des SRS. Mais des dispositions pertinentes régissaient évidemment l'utilisation des SRS à des fins professionnelles. Lors de la clôture de cette enquête de contrôle, le SGRS établissait dans un document interne que la discrétion du personnel était requise en toutes circonstances et faisait explicitement référence à l'utilisation des médias sociaux.

Aucun des services n'a eu recours à une autre mesure (c'est-à-dire l'interdiction générale de révéler son identité et sa qualité professionnelle, quelles que soient les circonstances). La VSSE applique l'obligation générale de discrétion sur l'identité et la qualité de membre du service, sauf dans les contacts avec d'autres instances. Il en va de même au SGRS : dans le cadre de l'utilisation d'Internet et des SRS, il est interdit d'y placer ou d'y échanger des informations qui pourraient établir un lien direct entre l'utilisateur ou un autre membre du SGRS et sa qualité de membre de ce service, sauf si une autorisation explicite a été donnée. Cette directive est régulièrement expliquée lors de briefings de sécurité et lors de formations. Par ailleurs, le SGRS met à la disposition des membres du personnel de la Défense actifs sur les réseaux sociaux des *smartcards* qui reprennent un certain nombre de choses « à faire » et « à ne pas faire ».

Une autre piste consiste à exercer un contrôle (a priori ou a posteriori) sur l'utilisation des TIC par les membres du personnel et sur le contenu de leurs messages. Bien que ce ne soit pas évident du point de vue du respect de la vie privée, la loi offre un certain nombre de possibilités. Par exemple, le « profil ouvert » d'un agent peut être contrôlé dans le cadre d'une enquête de sécurité, mais aussi bien entendu dans le cadre d'une enquête de renseignement. À cet égard, les services de renseignement peuvent d'ailleurs aussi obtenir l'accès aux parties « non publiques » des messages, en recourant à des méthodes particulières de renseignement. Les services rejettent l'idée d'un suivi préventif général du contenu des messages des membres de leur personnel dans la sphère privée, le considérant comme disproportionné et irréalisable.

Enfin, le Comité permanent R a examiné les contre-mesures pouvant être prises en cas d'incidents de sécurité et s'est intéressé aux possibilités de réaction des services dans le cadre de ce genre d'incidents (par exemple, le retrait de l'habilitation de sécurité ou une sanction disciplinaire).

II.5.4. CONCLUSION GÉNÉRALE

En guise de conclusion générale, le Comité a constaté que les deux services de renseignement adoptaient une approche essentiellement préventive à l'égard de la présente problématique, surtout motivés par le souci de ne pas restreindre la liberté d'expression de leurs agents. Cette approche préventive consistait à sensibiliser le personnel aux risques et à leur rappeler régulièrement leurs devoirs en matière de confidentialité et de discrétion. Le Comité a toutefois estimé que

s'en référer à des consignes générales de sécurité ne suffisait pas. Une interdiction absolue de l'utilisation des services de réseautage social n'est pas possible (ce serait contraire aux droits et libertés), mais les mesures spécifiques prises doivent tenir compte des conditions de sécurité particulières des agents de renseignement. Le Comité a formulé diverses recommandations concrètes dans ce cadre (voir IX.2.3).

II.6. LES MEMBRES DU PERSONNEL DE L'OCAM ET LES MÉDIAS SOCIAUX

En 2012, la Commission de suivi du Sénat a demandé qu'une enquête soit réalisée sur la présence éventuelle de membres du personnel des deux services de renseignement sur les sites de réseautage social (SRS) (voir II.5). Et de demander qu'il en soit de même à l'égard des membres du personnel de l'Organe de coordination pour l'analyse de la menace. Cette enquête de contrôle devait être menée conjointement avec le Comité permanent P. Le 20 décembre 2015, les deux Comités ont décidé d'ouvrir une enquête commune sur « *la manière dont l'OCAM gère la publicité que donnent certains membres de son personnel à leur identité et qualité professionnelle sur les réseaux sociaux de l'Internet* ».[71]

Les membres de la Commission de suivi souhaitaient ici aussi obtenir un certain nombre d'informations supplémentaires. Le Comité a dès lors mené une enquête complémentaire afin de vérifier quels résultats le « comité de pilotage » de l'OCAM, tout juste créé, pouvait déjà présenter, et quelle avait été la réaction du service lorsqu'il est apparu que quatre de ses collaborateurs étaient actifs sur les médias sociaux. La Commission de suivi souhaitait également savoir s'il était possible d'interdire légalement à des membres du personnel de l'OCAM d'être actifs sur les services de réseautage social, y compris dans la sphère privée. En ce qui concerne ce dernier aspect, les Comités permanents R et P ont recueilli l'avis de la Commission de la protection de la vie privée.[72]

Les résultats des enquêtes initiale et complémentaire sont repris ci-dessous.

II.6.1. L'AMPLEUR DU PHÉNOMÈNE

L'OCAM a également été avisée par la presse que certains de ses collaborateurs avaient fait apparaître leur nom et leur qualité sur des réseaux sociaux tels que

71 L'enquête a été clôturée le 12 mars 2015.

72 Voir Avis n° 45/2015 du 13 novembre 2015 relatif à la demande d'avis des Comités R et P quant à la possibilité d'interdire aux membres des services de renseignement et de l'OCAM d'avoir une activité, même à titre privé, sur les réseaux sociaux (https://www.privacycommission.be/fr/avis-1?page=2).

LinkedIn et Facebook. Mais l'OCAM avait également obtenu cette information via son propre service IT. Ce service effectuait des coups de sonde réguliers sur Internet pour vérifier quelles informations étaient disponibles sur des membres de l'OCAM. À l'estime de l'OCAM, l'ampleur du phénomène était modérée. En effet, d'une part, il ne concernait que de trois membres actifs et un ancien membre du service, et d'autre part, aucune information sensible n'avait été révélée. En 2015, à la demande des Comités, la direction a déclaré ne pas avoir connaissance de nouveaux cas.

II.6.2. LES RISQUES ASSOCIÉS À L'UTILISATION DES SERVICES DE RÉSEAUTAGE SOCIAL

Selon les Comités permanents R et P, les membres de l'OCAM devraient être particulièrement et attentifs aux possibilités offertes par les sites de réseautage social aux services de renseignement étrangers. En effet, ceux-ci peuvent suivre des personnes de près, par exemple à des fins d'espionnage ou de recrutement d'informateurs.

L'OCAM ne niait pas les risques, mais considérait qu'il fallait en relativiser l'importance. Premièrement, le fait est que tous les analystes de l'OCAM peuvent être connus, puisque leur nom est publié au Moniteur lors de leur nomination. Deuxièmement, l'OCAM estimait qu'il ne remplissait aucune tâche opérationnelle et ne menait pas d'activités inhérentes à des services de renseignement.[73] Enfin, la direction de l'OCAM se fiait au professionnalisme de son personnel et aux formations de sécurité qui lui sont dispensées.

II.6.3. MESURES PRISES OU SUSCEPTIBLES DE L'ÊTRE

La majorité du personnel de l'OCAM est constituée d'agents détachés d'autres services (principalement des services de police et de renseignement), et restent soumis au statut et à la déontologie de leur service d'origine. En outre, l'Arrêté royal du 23 janvier 2007 relatif au personnel de l'OCAM renferme plusieurs dispositions à prendre en considération dans la réglementation et le contrôle éventuel de leur comportement sur les SRS. Par exemple, l'article 37 dispose que l'analyste est tenu d'observer un devoir de discrétion, sur tout ce qui a trait à son activité professionnelle, même dans sa vie privée.

---

73 Les Comités n'ont pas marqué leur accord sur cette assertion. Le travail d'évaluation de l'OCAM repose essentiellement sur le traitement et l'analyse des informations (souvent classifiées) provenant de services de renseignement. Quand bien même l'OCAM n'a pas de compétence propre pour rechercher le renseignement, il est néanmoins chargé de traiter et d'analyser l'information. Il participe ainsi au cycle du renseignement. Ceci expose les agents de l'OCAM aux mêmes obligations de secret professionnel et de discrétion ainsi qu'aux risques de sécurité similaires que ceux des services de renseignement.

De plus, tout membre de l'OCAM est titulaire d'une habilitation de sécurité. Lors de l'octroi ou du renouvellement d'une telle habilitation, une enquête peut également être menée sur les « profils ouverts » sur les sites de réseaux sociaux, c'est-à-dire sur les informations dont l'accès n'a pas été limité par l'intéressé.[74]

Un service de renseignement aurait-il reçu des informations indiquant que le comportement d'un agent de l'OCAM sur les SRS est susceptible de constituer une menace de sécurité, il peut aussi accéder, à l'insu de l'intéressé, à ses comptes « à accès limité » moyennant le recours à une méthode particulière de renseignement.

La version la plus récente des « consignes de sécurité » destinées au personnel accorde une attention spécifique au devoir de discrétion dans le cadre de l'utilisation des médias sociaux. Les membres du personnel ont également reçu plusieurs briefings de sécurité en 2014 et 2015.

Enfin, un « comité de pilotage » a été créé au sein de l'OCAM. Il s'est vu confier quatre missions : (a) inventorier les problèmes éventuels liés à la sécurité ; (b) effectuer une analyse des risques pour chacun de ces problèmes ; (c) déterminer ensuite une priorité d'action ; et enfin (d) proposer des mesures à prendre en termes d'investissements, de consignes et de conscientisation. En 2015, ce comité de pilotage avait terminé l'inventaire des problèmes et avait défini une priorité d'action. La sécurité liée à l'utilisation d'outils TIC au sens large en était un élément essentiel. Un groupe de travail a également été instauré en vue d'élaborer les règles de « bon usage » des médias sociaux. Mais ces initiatives ont été suspendues, la problématique des *foreign terrorist fighters* et les événements de Paris et Bruxelles étant devenus prioritaires.

Comme pour les membres des services de renseignement, la question était de savoir, pour les collaborateurs de l'OCAM, dans quelle mesure des contrôles préventifs de l'utilisation privée ou professionnelle des SRS sont possibles. Les agents de l'OCAM devant être titulaires d'une habilitation de sécurité, leur hiérarchie doit pouvoir s'assurer qu'ils continuent en toutes circonstances à satisfaire aux conditions de sécurité, en particulier lorsque ceux-ci utilisent les TIC mis à leur disposition dans le cadre de leur fonction. Un tel contrôle ne nécessite pas l'accord préalable de l'agent concerné. Dans ce cadre, les Comités R et P considéraient que la hiérarchie de l'OCAM devait être en mesure de vérifier le comportement de ses agents sur les SRS en général.

Dans son avis, la Commission de la protection de la vie privée affirmait que l'interdiction d'activités strictement personnelles sur des médias sociaux en dehors du lieu de travail et des heures de bureau serait excessive. Cette interdiction peut donc être imposée sur le lieu de travail et pendant les heures de bureau. L'employeur dispose alors d'un droit de contrôle (qui n'est pas illimité).

---

74 La consultation des médias sociaux n'est pas explicitement prévue dans la réglementation comme moyen de recueil d'information lors d'une enquête de sécurité. Les Comités sont d'avis qu'elle peut être assimilée à la consultation de sources ouvertes.

Les instructions en vigueur doivent évidemment être portées préalablement à la connaissance des agents concernés.

II.6.4. CONCLUSION GÉNÉRALE

Seule la présence de quatre membres du personnel de l'OCAM ayant été détectée en tant que tels sur les médias sociaux, l'OCAM a d'abord minimisé l'importance du problème en faisant remarquer, à juste titre, que l'on pouvait aisément trouver le nom de tous les analystes de l'OCAM sur Internet, suite à la publication de leur nomination dans le Moniteur. Selon les Comités permanents R et P, l'OCAM paraissait avoir mieux pris conscience du problème et des risques au cours de l'année 2014.

Les Comités étaient d'avis que la création d'un comité de pilotage à l'OCAM, en charge des problèmes de sécurité, constituait un pas important en vue de prendre la problématique à bras-le-corps. Encore faut-il soigneusement définir le rôle de ce comité en la matière, les méthodes de recherche appropriées et leurs limites.

Motivée par le souci de ne pas restreindre la liberté d'expression de ses agents, la direction de l'OCAM a adopté une approche essentiellement préventive à l'égard de l'usage des SRS consistant à sensibiliser son personnel. Son attention est régulièrement attirée sur son devoir de discrétion.

Les Comités ont toutefois estimé que s'en référer à des consignes générales de sécurité ne suffisait pas. Une interdiction absolue de l'utilisation des SRS n'est pas possible (ce serait contraire aux droits et libertés), mais des mesures spécifiques prises doivent tenir compte des conditions de sécurité particulières des agents concernés. La prévention par l'établissement de règles de bonne conduite et de contrôle a posteriori *(Social Media Policy)* s'avère être la voie à suivre. Les Comités ont formulé toute une série de recommandations concrètes en la matière (voir IX.2.4).

II.7. LES CONTACTS INTERNATIONAUX DE L'OCAM

Une des missions de l'Organe de coordination pour l'analyse de la menace consiste à entretenir des contacts avec des « services étrangers ou internationaux homologues ». Début mai 2013, les Comités permanents R et P ont décidé de mener une enquête sur la manière dont l'OCAM remplit cette mission.[75] Dans la période qui a précédé, les Comités ont en effet reçu plusieurs courriers anonymes

[75] « Enquête de contrôle commune sur la manière dont l'OCAM entretient des relations internationales avec des services étrangers ou internationaux homologues en application de l'article 8, 3° de la L.OCAM du 10 juillet 2006 ».

dénonçant les nombreux voyages de service effectués par le directeur de l'OCAM, ainsi que les contacts « douteux » qu'il entretiendrait avec certaines autorités et services de renseignement étrangers.[76] Il tenterait également d'influencer certains dossiers dans un sens favorable à certains pays. Enfin, il aurait discuté, sans aucun mandat, de l'échange d'informations avec un service étranger et de l'accès réciproque à des banques de données.

Le rapport final a été approuvé le 22 juin 2005 et a été discuté peu après au sein de la Commission de suivi de la Chambre. Cette commission a demandé aux Comités de mener une enquête complémentaire sur la présence de deux systèmes de communication à l'OCAM, qui ont été fournis par deux services étrangers. Les Comités ont examiné la sécurité informatique de l'OCAM et la légalité de ces deux systèmes.[77]

II.7.1. TROIS ENQUÊTES SIMILAIRES MENÉES ANTÉRIEUREMENT

Ce n'était pas la première fois que les Comités examinaient les contacts internationaux de l'OCAM.

La première enquête datait de 2009[78] et portait notamment sur les voyages de service du directeur. Les Comités n'ont cependant constaté aucun dysfonctionnement majeur à cet égard.

Dans le courant de l'année 2011, une enquête a été effectuée sur une mission que l'OCAM planifiait en République démocratique du Congo.[79] En menant cette mission, l'OCAM affirmait vouloir se faire une meilleure idée des conditions de sécurité sur place et de la présence éventuelle de groupements radicaux, extrémistes ou terroristes dans ce pays. Les Comités ont toutefois attiré l'attention sur le fait que le législateur n'avait pas habilité l'OCAM à recueillir lui-même des informations sur le terrain, à la place des services d'appui.

La troisième enquête, qui date également de 2011, traitait de la représentation belge à des réunions internationales en matière de terrorisme.[80] Les Comités ont constaté que les services de police et de renseignement belges, ainsi que l'OCAM, participaient régulièrement à des réunions internationales consacrées à la lutte contre le terrorisme et/ou l'extrémisme, mais sans véritable concertation ni coordination. L'enquête a fait apparaître divers problèmes ponctuels.

---

76 Pour cet aspect de l'enquête, les Comités ont également cherché à déterminer ce que les services de renseignement et la Police fédérale savaient des relations établies par l'OCAM avec certains services étrangers, ce que ces services en pensaient et comment ils ont réagi.

77 Le rapport complémentaire a été clôturé le 11 août 2015.

78 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 48.

79 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 33.

80 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 43.

Dans ces trois enquêtes, les Comités permanents R et P ont recommandé que l'OCAM veille toujours à ce que son identité spécifique ne prête pas à confusion à l'égard des instances et des services étrangers avec lesquels il était en contact. L'OCAM n'étant pas un service de renseignement, les Comités estimaient 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. Il a donc été recommandé que l'OCAM fasse preuve d'une extrême prudence dans la préparation et l'exécution de ses missions à l'étranger, et qu'il limite rigoureusement ses voyages d'études. Et enfin, les Comités R et P de plaider pour que le Comité ministériel du renseignement et de la sécurité de l'époque élabore une directive dans les meilleurs délais afin de définir plus précisément la notion de « services homologues » avec lesquels l'OCAM peut entretenir des « contacts spécifiques ».[81]

II.7.2. LE CADRE LÉGAL

Ce sont surtout les articles 8, 9 et 10 L.OCAM qui étaient pertinents dans cette enquête.

Comme indiqué, l'OCAM a pour mission d'entretenir des contacts internationaux spécifiques avec des services étrangers ou internationaux homologues (art. 8, 3° L.OCAM). Il incombe au Conseil national de sécurité de clarifier la signification, ce qui n'était encore le cas lorsque la présente enquête a été clôturée. Les Comités ont souligné que ce ne serait pas évident, compte tenu de la diversité des structures mises en place par les pays pour coordonner l'analyse de la menace terroriste et/ou extrémiste.[82]

L'article 9 L.OCAM constitue la base légale pour la banque de données et les fichiers de travail de l'OCAM. Cette disposition oblige le directeur à prendre des mesures techniques et organisationnelles adéquates afin d'empêcher toute personne non autorisée d'y accéder. Toute interconnexion entre la banque de données de l'OCAM et d'autres systèmes informatiques nationaux ou étrangers est formellement interdite.

Enfin, il reste l'article 10 L.OCAM : cette disposition limite la communication des évaluations de l'OCAM à des services et des autorités belges bien déterminés. Les autorités ou les institutions étrangères ou internationales n'y sont pas mentionnées. Par ailleurs, l'article 8 L.OCAM dispose que les données que l'organe de coordination obtient de l'étranger doivent être transmises aux services belges compétents.

---

81 Ce n'est que récemment qu'une suite a été donnée aux recommandations formulées par les Comités. Le Conseil national de sécurité a pris une directive début 2016. Cette enquête de contrôle ne porte évidemment pas sur cette directive.

82 Voir à cet égard COMITÉ PERMANENT R (éd.), *Fusion Centres Throughout Europe. All-Source Threat Assessments in the Fight Against Terrorism*, Intersentia, Anvers, 2010, 220 p.

II.7.3. LES CONCLUSIONS DES COMITÉS PERMANENTS R ET P

Un premier volet de l'enquête avait pour objet les voyages de service à l'étranger de membres de l'OCAM. Il est ressorti des chiffres communiqués aux Comités que le nombre de missions effectuées à l'étranger n'était pas exagéré.

La fréquence des contacts en Belgique avec certaines autorités et services étrangers n'était pas non plus problématique. Elle démontrait que l'OCAM était accessible, ce qui mérite d'être mentionné.

Les Comités estimaient que l'organisation des contacts avec l'étranger ne procédait pas d'une démarche stratégique claire et réfléchie. Il ne ressortait pas davantage que l'établissement de ces relations était concerté avec d'autres services; celles-ci apparaissaient plutôt comme étant le résultat d'initiatives personnelles prises en fonction d'opportunités et de sollicitations extérieures.

Les Comités ont également constaté une lacune dans les rapports sur les contacts, tant en interne qu'à l'extérieur de l'organisation. La question de la valeur ajoutée, si ce n'est une éventuelle acquisition de connaissances du membre du personnel envoyé en mission, était rarement évidente.

Les contacts de l'OCAM avec des services étrangers et internationaux qui ne sont pas des services «homologues» étaient problématiques, parce qu'ils pouvaient créer une confusion sur la responsabilité des différents services belges.

En outre, il est ressorti de l'enquête que l'OCAM recevait parfois des informations de services étrangers, qu'il ne les transmettait pas systématiquement aux autorités belges compétentes, et que l'OCAM reconnaissait par ailleurs fournir lui aussi des informations à ces services étrangers. Cette manière de procéder est contraire à l'article 8, 3°, alinéa 2 et à l'article 10 L.OCAM.

Sans minimiser les conclusions qui précèdent, les Comités ont souligné qu'au moment où l'enquête a été menée, le Comité ministériel du renseignement et de la sécurité (devenu le Conseil national de sécurité) n'avait toujours pas édicté de directive réglementant ces contacts internationaux, comme le requiert la L.OCAM. Une telle directive devait préciser ce que l'OCAM peut et ne peut pas faire en la matière.[83]

Les Comités permanents R et P partageaient les préoccupations exprimées par les dirigeants des services de renseignement sur la gestion par l'ancien directeur de l'OCAM de ses relations internationales. Les Comités estimaient que le directeur, eu égard aux relations qu'il avait nouées avec plusieurs partenaires étrangers, parfois depuis bien avant sa nomination à ce poste, donnait pour le moins l'impression de manquer de prudence. Il manquait de distance par rapport à certains services dont les activités en Belgique font l'objet

[83] Les Comités ont toutefois ajouté que l'OCAM n'avait jamais pris la moindre initiative à l'égard des ministres compétents pour clarifier la question.

d'une attention particulière de la VSSE et du SGRS, même si, par ailleurs, l'établissement de ces relations officielles a reçu l'aval de ses ministres de tutelle.

De plus, le manque de transparence, de traçabilité et de rapports concernant ces contacts a eu pour conséquence que l'objectivité même de certaines évaluations était mise en doute par les services de renseignement belges. Cette constatation était particulièrement inquiétante.

Les Comités R et P ont également exprimé leur préoccupation particulière quant à la manière dont l'ancien directeur de l'OCAM entretenait certaines relations avec l'étranger. Ces relations étaient perçues comme empiétant sur les compétences de la VSSE et du SGRS, et donc problématiques pour la coopération avec ces services. Cette situation méritait une profonde remise en question.

Les Comités ont à nouveau constaté que l'OCAM restait en défaut de remplir son obligation légale de remettre deux fois par an au Conseil national de sécurité un rapport d'activités sur ses objectifs stratégiques, ses activités et son organisation, ce rapport devant ensuite être transmis aux organes de contrôle.

Quant aux deux systèmes de communication que l'OCAM partageait[84] avec deux services étrangers, les Comités ont mené une enquête complémentaire, comme indiqué ci-dessus. Cette enquête a confirmé et illustré les conclusions précédentes, et ce au niveau des contacts avec des services qui ne sont pas des services homologues et au niveau de l'échange d'informations opérationnelles et de données à caractère personnel. Indépendamment de la nécessité évidente d'un échange international d'informations avec des services étrangers en matière d'extrémisme et de terrorisme, les deux Comités ont dû remarquer que les procédés constatés violaient la lettre et l'esprit de la L.OCAM. En outre, ils ne tenaient aucun compte des compétences et des obligations d'autres autorités et services fédéraux, ce qui pouvait perturber la coopération internationale et les relations mutuelles.

II.8. SUIVI À TORT PAR LES SERVICES DE RENSEIGNEMENT ?

En février 2014, une personne d'origine nord-africaine résidant en Belgique s'est plainte d'être l'objet de surveillances « oppressantes » de la part des services de renseignement. Le plaignant prétendait n'avoir aucune idée des raisons pour lesquelles il aurait attiré l'attention des services de renseignement : il n'a jamais eu de problème dans son pays d'origine, ni dans le pays asiatique où il a travaillé pendant plusieurs années. Il disait ne pas avoir d'antécédents judiciaires ni de lien avec le terrorisme ou le radicalisme.[85]

---

84 Ces systèmes ne sont plus opérationnels.

85 L'enquête a été ouverte le 3 juillet 2014. En février 2015, le rapport final a été envoyé au président de la Commission de suivi, ainsi qu'aux ministres de la Justice et de la Défense.

Aux dires du plaignant, ses problèmes ont commencé en 2011. Il avait alors été retenu pendant six heures dans un aéroport étranger où il s'était arrêté dans le cadre de son travail. Un responsable de la sécurité l'aurait informé ultérieurement que son nom figurait sur une liste de la *Transportation Security Agency* (TSA) américaine. À partir de ce moment-là, il a déclaré faire l'objet d'une surveillance lors de ses déplacements dans ce pays. Il s'est également vu refuser une demande de visa pour un pays tiers. Il a alors été transféré vers le siège belge de la firme.

L'intéressé déclarait avoir été la cible d'opérations de surveillance dès son arrivée en Belgique, en mai 2012, et craindre d'avoir été injustement placé dans le collimateur de divers services de renseignement. Son sentiment était encore renforcé par le traitement particulier auquel il a été soumis à deux reprises à l'aéroport de Zaventem. Ainsi, il est arrivé qu'il soit contrôlé par la Police aéroportuaire, et a même été brièvement retenu, alors qu'il voulait prendre un avion.

Le Comité permanent R a examiné si le plaignant avait effectivement attiré l'attention de la Sûreté de l'État ou du SGRS, et si tel était le cas, quelle étaient la position d'information et quelles étaient les actions menées par les services de renseignement.

II.8.1. LES FAITS

En novembre 2011 – le plaignant n'était pas encore en Belgique à ce moment-là – l'OCAM, le SGRS et la VSSE ont reçu une demande d'information d'un service de renseignement étranger concernant l'intéressé, signalant une sympathie supposée à l'égard d'un prédicateur musulman radical.

Faisant suite à la demande du service étranger, et en l'absence de toute information sur l'intéressé, l'OCAM a demandé à la Police fédérale de procéder à son signalement dans la banque de données générale de la police dans la catégorie « Contexte Information Terroriste », et ce pour une période de six mois.

La VSSE a, de son côté, mené une enquête administrative.[86] L'enquête n'a pas permis de démontrer une quelconque appartenance à des milieux islamistes. Le service partenaire étranger en a été informé.

Étant donné que le plaignant n'apparaissait pas dans sa base de données, et en l'absence de lien direct avec ses missions légales, le SGRS n'a entrepris aucune action dans cette affaire.

Le 28 mai 2012, l'intéressé a atterri à Zaventem.[87] Le lendemain, le service de renseignement étranger a de nouveau transmis des renseignements, cette fois à la

[86] Dans ce cadre, la VSSE a consulté sa propre base de données ainsi que les bases de données existantes (la base de données de la police, le Registre national, l'Office des étrangers…). Et le service de déclarer avoir effectué des recherches sur les réseaux sociaux (Facebook…).

[87] Bien que signalé, il n'a pas été contrôlé lorsqu'il est arrivé pour la première fois en Belgique.

VSSE, à l'OCAM et à la Police fédérale : le service signalait que l'intéressé avait quitté le pays asiatique dans lequel il travaillait. Vu que le document ne contenait pas de nouvelles informations, la VSSE a décidé de ne pas effectuer d'enquête complémentaire. La VSSE a néanmoins demandé une analyse de risques et une évaluation de la menace au service partenaire. Il lui a été répondu qu'une analyse des e-mails de l'intéressé n'avait rien révélé de concluant.

En août 2012 – après un court séjour à l'étranger – l'intéressé a été contrôlé par la Police aéroportuaire à son arrivée à Zaventem.[88] Il a, cette fois-ci, été effectivement interrogé. L'OCAM, le SGRS et la VSSE ont reçu une copie du rapport, dans lequel ne figurait aucun élément significatif.

Toujours en août, l'OCAM a néanmoins réinterrogé les trois services d'appui concernés au sujet de liens présumés de l'intéressé avec les milieux islamistes radicaux. La VSSE a répondu qu'elle ne disposait d'aucun élément complémentaire.

Début 2013, la VSSE a reçu une nouvelle demande d'information, cette fois des services de renseignement du pays asiatique où l'intéressé a vécu. La demande comportait des informations détaillées sur son appartenance supposée à une mouvance islamiste radicale. La VSSE a cette fois ouvert une nouvelle enquête et a notamment fait appel à ses canaux d'information. Le service a donc mené une enquête plus approfondie, tout en respectant le principe de proportionnalité (il n'a pas eu recours à des MRD, par exemple). Toutes les actions entreprises étaient légales.

En mars 2013, la VSSE a transmis le résultat de son enquête au service étranger concerné. Une fois de plus, aucun lien avec un quelconque milieu islamiste radical n'est ressorti. Toutefois, le résultat de cette enquête complémentaire, même négatif, n'a pas été communiqué à l'OCAM. Les informations émanant du pays asiatique sont, elles aussi, restées au sein de la VSSE.

Depuis mars 2013, la VSSE n'a plus reçu de nouvelles informations ou demandes à propos de l'intéressé.

II.8.2. LA PROBLÉMATIQUE DES LISTES D'ORGANISATIONS TERRORISTES

Il existe de sérieux indices établissant un lien entre les problèmes auxquels le plaignant a été confronté à l'étranger et la problématique des listes d'organisations terroristes.[89] L'intéressé aurait par exemple figuré sur la liste de la *Transportation Security Administration* (TSA) américaine. Il est également apparu que le plaignant avait été placé temporairement sur une « liste » belge, à savoir la banque de données générale de la police.

---

88 Ce contrôle a donc eu lieu alors que l'intéressé revenait en Belgique pour la deuxième fois.

89 Voir à ce propos P. DE HERT et K. WEIS, 'Europese terrorismelijsten. Beperkte rechtsbescherming', *Nieuw Juridisch Weekblad*, 2009, 199.

Le Comité attire l'attention sur le fait que les États et les institutions multilatérales utilisent différentes listes dans le cadre de la lutte contre le terrorisme et de la protection de l'aviation civile. L'objectif étant, entre autres, de soumettre les personnes qui sont signalées sur ces listes à des contrôles approfondis, de les interdire de vol ou d'autoriser des signalements aux autorités compétentes. Ce genre de listes se fonde sur la législation nationale et/ou sur des décisions d'organisations internationales (p. ex. les résolutions des Nations Unies ou des directives de l'Union européenne).

Le Comité permanent R ne met certainement pas en doute l'utilité ou la nécessité de telles listes. Loin s'en faut. Les attentats récents démontrent que le partage de renseignements avec d'autres pays est parfois encore insuffisant. Le Comité ne veut pas non plus exclure que dans cette situation concrète, des raisons fondées ou des soupçons existaient ou pouvaient exister concernant le plaignant pour le placer sur une telle liste.

Dans le cas présent, le Comité permanent R a pu constater, dans son domaine de compétences, que les services belges ont agi avec professionnalisme et correction à l'égard du plaignant et des services étrangers.

Du point de vue du citoyen, le placement sur une liste reste problématique. Et pour cause, il n'est pas évident de faire valoir ses droits au regard de mesures de sécurité qui sont souvent prises sur la base de procédures qui se déroulent sans que l'intéressé en soit informé (pas de notification, pas de contestation). Ces procédures, en ce compris leur caractère secret, peuvent être légitimes, pour autant que les raisons et les objectifs qui les sous-tendent le soient également, et que la mise en œuvre des mesures demeure dans des limites acceptables.[90] En effet, il ressort d'exemples concrets que le placement de personnes sur des listes d'individus soupçonnés de terrorisme peut avoir des conséquences disproportionnées.[91] La pratique révèle aussi qu'il n'est pas évident de supprimer des personnes de ce genre de listes.

II.8.3. CONCLUSIONS DE L'ENQUÊTE

Le Comité a souligné que le plaignant n'avait pas fait l'objet d'opérations de surveillance de la part des services belges de renseignement et de sécurité. Ils ne sont pas non plus responsables de son signalement dans le « Contexte Information Terroriste ». Il semble néanmoins très probable qu'il ait été suivi par

90 À propos de telles listes, voir également : COMITÉ PERMANENT R, *Rapport d'activités 2005*, 155-165.

91 Maher ARAR est un citoyen syro-canadien qui, sur la base d'informations canadiennes, était soupçonné de terrorisme par les services de sécurité américains lors de son passage aux États-Unis. Il a même été livré à la Syrie, où il a été torturé. Par la suite, l'intéressé a été blanchi de tout soupçon et a reçu un dédommagement.
Voir http.//ccrjustice.org/ourcases/current-cases/arrar-v.ashcroft.

les services de renseignement du pays asiatique où il a résidé pendant un certain temps.

En outre, le Comité n'a pas trouvé le moindre élément indiquant que la VSSE aurait été « instrumentalisée » par un service partenaire. Il n'y a pas non plus d'indications selon lesquelles des services étrangers auraient entrepris des actions à l'encontre de l'intéressé sur le sol belge.

Les services de renseignement belges ont, dans ce dossier, agi de manière légale, proportionnelle et dans le champ de leurs compétences. Ils ne se sont jamais engagés dans des activités de surveillance telles que décrites par le plaignant. Le Comité a constaté que la VSSE avait travaillé de manière efficace dans la gestion de ce cas.

Enfin, le Comité s'est demandé si et dans quelle mesure les services de renseignement belges, en vertu de la Constitution[92] ou de la CEDH, ont une « obligation positive » à l'égard d'un résident pour le protéger d'accusations éventuellement non fondées émanant de services de renseignement étrangers ou d'autorités étrangères et, le cas échéant, de faire cesser une atteinte à sa vie privée.

II.9. PLAINTE RELATIVE À LA TRANSMISSION D'INFORMATIONS À CARACTÈRE PERSONNEL À UN TIERS PAR UN AGENT DE RENSEIGNEMENT

Début octobre 2014, un particulier a déposé une plainte au Comité permanent R. Selon le plaignant, le contenu d'e-mails personnels qu'il avait envoyés à un membre du ministère de la Défense aurait atterri chez son employeur via le service de renseignement militaire. Peu après, son employeur lui a signifié son licenciement, en se référant explicitement à la transmission par un collaborateur du SGRS d'une copie des e-mails concernés. L'enquête devait établir de quelle manière le SGRS avait traité le dossier, si le service avait respecté la réglementation en vigueur, et si des informations avaient effectivement été transmises à un tiers.[93]

Les e-mails en question étaient arrivés au SGRS par l'intermédiaire d'un membre du ministère de la Défense. Dans ses messages, le plaignant avait effectivement mentionné – en guise de plaisanterie, comme avéré par la suite – qu'il avait transmis un virus informatique. Le SGRS est le service approprié pour

92 Voir, par exemple, l'article 191 de la Constitution : *«Tout étranger qui se trouve sur le territoire de la Belgique jouit de la protection accordée aux personnes et aux biens, sauf les exceptions établies par la loi ».*

93 L'enquête a été clôturée en juin 2015. Le Comité permanent R n'était évidemment pas compétent pour se prononcer sur le motif et la légalité du licenciement de l'intéressé.

examiner ce genre de menace potentielle, cette tâche relevant de ses missions légales.

Outre cette enquête de nature informatique, le recueil de renseignements du SGRS sur le plaignant lui-même a également été effectué dans le cadre de ses compétences, puisqu'il s'agissait d'évaluer la menace éventuelle.

Le résultat de cette enquête technique (qui a démontré le caractère inoffensif de la menace) a été communiqué en termes généraux à l'officier de sécurité de l'entreprise où le plaignant était employé. Cette communication trouve son fondement légal dans l'article 19 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité.[94] Le Comité a toutefois constaté que l'envoi à l'officier de sécurité de l'entreprise de tous les e-mails échangés entre les personnes concernées, sans leur en avoir demandé la permission, ne semblait pas conforme à Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Le SGRS avait également transmis les e-mails à l'Autorité nationale de sécurité (ANS), qui a la compétence de se prononcer sur l'habilitation de sécurité de l'intéressé et de l'entreprise. Bien qu'en l'occurrence, la menace n'était pas sérieuse, le comportement du plaignant pouvait néanmoins apparaître comme constitutif d'un problème potentiel de sécurité. À cet égard, la communication à l'ANS paraissait légitime.

Enfin, le Comité a constaté que le SGRS n'avait pas suffisamment coordonné les différents aspects du problème, ni toujours agi suivant les procédures légales ou réglementaires applicables en cas d'incident de sécurité.

II.10. LA VSSE ET L'APPLICATION DE LA RÉGLEMENTATION SUR LES CONGÉS DE MALADIE

À la mi-2014, un assistant de protection de la VSSE a introduit une plainte. Après une période de congé de maladie, il a été mis en situation de non-activité[95] pour la période complète d'exemption médicale, et a été enjoint de rembourser une somme non négligeable. Cette décision a été motivée par les problèmes de contrôle médical obligatoire qui se sont posés pendant son congé de maladie. De plus, l'intéressé se plaignait d'avoir été contraint d'apurer ses heures supplémentaires avant de reprendre le travail.

---

94 *« Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes ainsi qu'aux personnes qui font l'objet d'une menace visée aux articles 7 et 11 […] »* (art. 19 L.R&S).

95 Art. 62 de l'A.R. du 19 novembre 1998 relatif aux congés et aux absences accordés aux membres du personnel des administrations de l'État.

Le Comité a alors décidé d'ouvrir une enquête de contrôle *« sur la manière dont la VSSE interprète et exécute la réglementation du travail et, plus en particulier, les règles sur les congés de maladie »*.[96]

L'enquête a révélé que la VSSE était bien au courant de la réglementation du travail en vigueur et que des directives internes avaient été prises à l'égard du personnel. Néanmoins, ni la réglementation ni les directives internes n'ont été appliquées dans ce cas-ci.

En ce qui concerne la problématique des heures supplémentaires, le Comité permanent R s'est également référé à son enquête de contrôle sur l'exécution par la VSSE de sa mission légale de protection des personnes.[97] Les problèmes constatés dans ce cadre n'étaient toujours pas résolus au moment où l'enquête relative à la présente plainte a été menée.

Enfin, le Comité a souligné un manque de communication des services administratifs, que ce soit avec les membres du personnel interne qu'avec les services extérieurs de la VSSE.

II.11. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ POSÉS EN 2015 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2015

Cette section énumère et situe brièvement toutes les enquêtes que le Comité permanent R a démarrées en 2015, 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. LA PROTECTION DU POTENTIEL SCIENTIFIQUE ET ÉCONOMIQUE ET LES RÉVÉLATIONS D'EDWARD SNOWDEN

Les révélations d'Edward Snowden ont donné un aperçu du contenu de programmes extrêmement secrets principalement de la *National Security Agency* (NSA) américaine. Elles ont donné lieu à l'ouverture de nombreuses enquêtes (parlementaires, judiciaires et de renseignement) aux quatre coins du monde, y compris en Belgique. Le Comité permanent R a ouvert quatre enquêtes de contrôle qui étaient naturellement étroitement liées.

---

96 Le rapport final a été envoyé en février 2015 au ministre de la Justice et au président de la Commission de suivi.

97 Voir à cet égard : COMITÉ PERMANENT R, *Rapport d'activités 2014* ('II.4. La VSSE et sa mission légale de protection des personnes'), 45-52, particulièrement 51.

Trois de ces quatre enquêtes ont été bouclées en 2014.[98] La dernière enquête de contrôle[99] traite des implications éventuelles de ces programmes étrangers pour la protection du potentiel scientifique et économique du pays. Elle entend vérifier si les services de renseignement belges :

- se sont intéressés à ce phénomène ;
- ont détecté une menace réelle ou éventuelle pour le potentiel scientifique et économique belge ;
- en ont informé les autorités compétentes et ont proposé des mesures de protection ; et
- disposent de moyens suffisants et adéquats pour suivre cette problématique.

Par ailleurs, à la demande de l'ancienne Commission de suivi du Sénat, les conséquences du programme PRISM et/ou d'autres systèmes analogues sur le potentiel scientifique et économique du pays ont été examinées. Le rapport a été clôturé début 2016.

II.11.2. LA PROBLÉMATIQUE DES *FOREIGN FIGHTERS* ET DES PERSONNES PARTIES COMBATTRE EN SYRIE

Depuis 2013, la guerre en Syrie exerce un fort pouvoir d'attraction sur ce que l'on appelle les « *foreign (terrorist) fighters* » du monde entier. Il s'avère que, proportionnellement, de nombreux combattants viennent de Belgique.

Le Comité permanent R a dès lors décidé, en octobre 2014, d'ouvrir une enquête de contrôle sur « *la position d'information des deux services de renseignement (SGRS et VSSE) sur le recrutement, l'envoi, le séjour et le retour en Belgique de jeunes (belges et étrangers résidant en Belgique) qui partent ou sont partis combattre en Syrie ou Irak et sur le transfert de renseignements aux diverses autorités* ». Cette enquête a cherché à répondre aux questions suivantes : quelle est la mission des services de renseignement belges dans ce cadre et quelle ligne à suivre leur a été (est) donnée ? Les services de renseignement belges ont-ils une vue sur les phases de recrutement et de départ ? Peuvent-ils se faire une idée de qui sont ces « combattants syriens » ? Sont-ils au courant des activités de ces combattants sur place ? L'évolution à l'étranger se traduit-elle par d'éventuelles

98 Voir COMITÉ PERMANENT R, *Rapport d'activités 2014*, 7-45 (il s'agit respectivement de 'II.1. Les révélations d'Edward Snowden et la position d'information des services de renseignement belges', 'II.2. Protection de la vie privée et captation massive de données' et 'II.3. L'utilisation dans des affaires pénales d'informations issues d'une captation massive de données par des services étrangers').

99 Enquête de contrôle « *sur l'attention que les services de renseignement belges portent (ou non) aux menaces que peuvent représenter pour le potentiel scientifique et économique de la Belgique des programmes de surveillance électronique sur les systèmes de communication et d'information mis en œuvre à grande échelle par des puissances et/ou des services de renseignement étrangers* ».

menaces en Belgique et, dans l'affirmative, lesquelles ? Qu'en est-il du suivi et de l'approche lors de leur retour en Belgique ? Comment se déroule la collaboration (SGRS, VSSE, OCAM, mais aussi la police) en la matière ? Comment font-ils rapport de leurs activités et à qui ?…

Début 2015, un premier rapport intermédiaire a été rédigé pour la Commission de suivi (à ce propos voir le Chapitre II.4). Le rapport final a été achevé en 2016.

II.11.3. LA VSSE ET LE PROTOCOLE DE COOPÉRATION AVEC LES ÉTABLISSEMENTS PÉNITENTIAIRES

Le 1er octobre 2014, le Comité a ouvert une enquête de contrôle sur la manière dont la VSSE met en application le «*protocole d'accord réglant la coopération entre la Sûreté de l'État et la Direction générale Exécution des Peines et des Mesures*». Cette enquête découle de deux enquêtes de contrôle clôturées précédemment.[100] Elle avait pour objectif d'examiner si l'accord est appliqué efficacement, si la VSSE peut y puiser les informations utiles pour l'exécution de ses missions, et de vérifier si l'échange de données sur des détenus se déroule conformément à la protection des droits que la Constitution et la loi garantissent aux personnes.

Cette enquête a été clôturée en 2016.

II.11.4. LE SUIVI D'UNE MENACE POTENTIELLE À L'ENCONTRE D'UN VISITEUR ÉTRANGER

En mars 2015, un agent des services extérieurs de la VSSE s'est adressé au service d'Enquêtes du Comité permanent R. Il se plaignait de la manière dont les services d'analyse avaient travaillé dans un dossier donné. Il s'agissait plus particulièrement de la manière dont des informations avaient été recueillies et analysées au sujet de la visite imminente en Belgique du médecin congolais, M. Mukwege. L'intéressé est un opposant de longue date au régime congolais actuel. Selon le plaignant, l'OCAM n'a pas non plus reçu la totalité des informations pertinentes pour rédiger une évaluation correcte sur la menace potentielle à l'encontre de l'intéressé.

Cette enquête de contrôle a été bouclée en 2016. Les résultats ont été discutés au sein de la Commission de suivi du Parlement.

---

100 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 22-25 ('II.3. La position d'information et les actions des services de renseignement concernant Lors Doukaev') et *Rapport d'activités 2012*, 28-33 ('II.3. Le suivi éventuel d'un particulier pendant et après sa détention en Belgique').

II.11.5. UNE PLAINTE CONTRE UN COLLÈGUE INDISCRET

En juillet 2015, un officier supérieur du SGRS a introduit une plainte auprès du Comité permanent R. Un collaborateur du SGRS aurait en effet divulgué des données sur sa vie privée et professionnelle dans un espace public, là où le collaborateur et lui habitent. Il craignait même d'éventuelles répercussions sur sa sécurité et celle de sa famille.

Le plaignant s'est adressé à deux reprises à la direction du SGRS, mais a estimé que sa réaction manquait de fermeté. Il a finalement déposé plainte auprès du Comité permanent R. La plainte portait tant sur les indiscrétions présumées que sur la réaction du SGRS.

Le rapport final a été approuvé en 2016.

II.11.6. UNE PLAINTE RELATIVE À UN PAIEMENT DÛ (OU NON)

En avril 2015, un ancien inspecteur de la VSSE a adressé une plainte au Comité permanent R. Il a en effet été contraint de rembourser une somme (modeste) qu'il aurait perçue à tort et qui provenait de la caisse des fonds spéciaux. Après avoir tenté, en vain, de défendre son point de vue auprès de la VSSE, il a décidé de se tourner vers le Comité permanent R. Et d'indiquer que les problèmes qu'il avait rencontrés avec sa hiérarchie directe l'avaient incité à quitter la VSSE.

Aussi le Comité a-t-il décidé d'ouvrir une «*enquête de contrôle suite à la plainte d'un ancien agent de la VSSE relative à la gestion de la caisse de service d'un poste de province*». Cette enquête a également été clôturée en 2016.

II.11.7. UNE INTERVENTION CONTROVERSÉE DE DEUX ASSISTANTS DE PROTECTION ?

En juin 2015, un incident impliquant deux membres du Service Protection des personnes de la VSSE (de l'époque) s'est produit lors d'une mission sur la voie publique. Les assistants de protection étaient chargés d'assurer la sécurité d'un haut dignitaire, lorsque la voiture d'un particulier les a brièvement suivis et a ignoré leurs ordres de se tenir à distance. Lorsque le véhicule de l'intéressé s'est immobilisé, les assistants de protection sont intervenus. Ils auraient fait preuve d'agressivité, l'un d'eux ayant même sorti son arme. C'est ainsi que le conducteur de la voiture a décidé de faire une dénonciation auprès du Comité.

L'enquête sur le déroulement de l'intervention a été bouclée en 2016.

II.11.8. UNE PLAINTE RELATIVE À UNE INTERVENTION DE L'OCAM

En 2015, le Comité permanent R, conjointement avec le Comité permanent P, a ouvert une enquête sur la manière dont l'OCAM avait joué un rôle dans le retrait de la licence d'un pilote de ligne. L'intéressé avait effectivement introduit une plainte, parce que l'OCAM aurait rédigé à tort une évaluation de menace qui pouvait ensuite être utilisée pour lui retirer sa licence de pilote.

La plupart des actes d'enquête ont été achevés en 2015. L'enquête sera finalisée au second semestre 2016.

II.11.9. ÉVALUATIONS INDIVIDUELLES DE LA MENACE PAR L'OCAM

En mars 2015, les Comités permanents R et P ont ouvert une enquête de contrôle sur « *la manière dont l'OCAM détermine le niveau de la menace que représente un individu ou de celle qui le vise, sur les conséquences que la détermination de ce niveau de la menace entraîne sur la répartition des tâches, les mesures à prendre et l'échange d'information entre services concernés, ainsi que sur les conséquences pratiques pour la personne concernée et son suivi* ». Cette enquête a été ouverte à la demande de la Commission de suivi de la Chambre, qui souhaitait obtenir des réponses aux questions suivantes :

- Quels critères l'OCAM applique-t-il pour déterminer le niveau de menace à l'égard d'un individu ?
- Quelle instance arrête les tâches des services concernés dès que le niveau de la menace est connu ?
- Quelles mesures opérationnelles résultent de chaque niveau de la menace et quel service est chargé de la coordination ?
- Comment sont réglés les flux d'informations entre les différents services ?
- Quelles sont les conséquences concrètes pour un individu qui fait l'objet d'un niveau de menace donné ?
- Comment la « classification » de cet individu est-elle suivie par les autorités locales policières et administratives ?

Un rapport intermédiaire a été envoyé à la Commission de suivi en février 2016. Le rapport final est prévu pour le second semestre 2016.

II.11.10. DYSFONCTIONNEMENTS SPÉCIFIQUES AU SEIN DE L'OCAM

Au cours du second semestre 2015, les Comités permanents R et P ont reçu deux lettres anonymes, qui évoquaient des « irrégularités » et des « problèmes structurels graves » au sein de l'OCAM. Par exemple, les experts devraient exécuter des tâches qui incombent statutairement aux analystes. De même, certaines personnes auraient été détachées auprès de l'OCAM en méconnaissance des règles en vigueur.

Un peu plus tard, les Comités ont reçu une nouvelle plainte portant sur le fonctionnement interne de l'OCAM. Le plaignant mentionne notamment la manière dont il a été mis fin à son détachement.

Les Comités ont rassemblé toutes les questions dans une enquête commune. Le rapport final est prévu pour le second semestre 2016.

II.11.11. ENQUÊTE DE CONTRÔLE SUR LA POSITION D'INFORMATION DES DEUX SERVICES DE RENSEIGNEMENT AVANT LES ATTENTATS DE PARIS

Le 13 novembre 2015, plusieurs attentats ont eu lieu à Paris. Des terroristes se sont fait exploser dans le quartier du Stade de France, puis des attaques ont été menées à proximité de terrasses de cafés et restaurants de la capitale française. Au même moment, la salle de concert du Bataclan était le théâtre d'une prise d'otages. Le bilan de ces attentats faisait état 130 morts. Une quatrième attaque était prévue dans le quartier des affaires de La Défense. Ces attentats étaient l'œuvre de *foreign terrorist fighters* de retour de Syrie et étaient pilotés par le groupe terroriste EI.

Des informations indiquant l'existence d'un lien étroit avec la Belgique sont assez vite apparues : plusieurs terroristes provenaient ou résidaient en Belgique, les véhicules utilisés lors des attentats avaient été loués en Belgique, les terroristes avaient des planques en Belgique, les ceintures d'explosifs avaient probablement été assemblées dans un appartement de Schaerbeek…

Le Comité permanent R a presque immédiatement ouvert une enquête de contrôle.[101] Il a toutefois attendu pour procéder aux premiers devoirs d'enquête. En effet, au cours des semaines et des mois agités qui ont suivi les attentats, on ne pouvait pas attendre de la VSSE et du SGRS qu'ils consacrent beaucoup de temps au Comité et à son service d'Enquêtes. L'enquête a été clôturée en 2016.

---

101 *« Enquête de contrôle sur la position d'information des deux services de renseignement sur les individus ou groupes ayant perpétré les attentats de Paris ou liés à ces attentats, avant le vendredi 13 novembre 2015 au soir ».* Début 2016, le Comité a aussi ouvert, conjointement avec le Comité permanent P, une enquête relative à la position d'information de l'OCAM.

CHAPITRE III
LE CONTRÔLE DES MÉTHODES PARTICULIÈRES DE RENSEIGNEMENT

Ce chapitre reprend les chiffres précis relatifs à l'utilisation par la VSSE et le SGRS des méthodes particulières de renseignement et à la manière dont le Comité permanent R exerce sa tâche juridictionnelle. Ce chapitre est basé sur le rapport portant sur l'utilisation des méthodes particulières par les services de renseignement qui est rédigé annuellement pour le Parlement, en exécution de l'article 35 § 2 L.Contrôle.

Le Comité tient au préalable à mentionner l'accord conclu le 16 novembre 2015 entre la Banque nationale de Belgique (BNB) et la VSSE, en vertu duquel cette dernière pourrait, sur simple demande, obtenir l'accès à des données reprises dans le Point de contact central (PCC). Il s'agit d'une banque de données dans laquelle doivent être repris l'identité et les numéros de compte des clients de toutes les institutions bancaires, de change, de crédit et d'épargne. La VSSE estimait qu'une telle consultation constituait une méthode ordinaire (c'est-à-dire la méthode qui est prévue à l'article 14 L.R&S). Mais le Comité n'était pas de cet avis. Bien qu'il voyait dans l'initiative de la VSSE une implication dans la recherche active de canaux d'informations utiles, le Comité a fait référence à l'article 18/15 § 1er, 1° L.R&S. Cet article considérait la demande de listes de comptes bancaires ou de certains instruments financiers (belges ou étrangers, la loi ne le spécifie pas) comme une méthode exceptionnelle. En outre, la loi n'émet aucune réserve sur l'instance qui fournit ces informations. Donc, si la BNB ne devait pas être considérée comme une « banque » ou une « institution financière » au sens de l'article 18/5 § 2 L.R&S, les listes resteraient « protégées » par le mécanisme de la méthode exceptionnelle. Et si la VSSE souhaite recevoir des listes de comptes bancaires via le PCC, elle doit d'abord demander l'autorisation de mettre en œuvre une méthode exceptionnelle. Le ministre de la Justice a indiqué que dans l'attente d'une nouvelle concertation, la VSSE devait appliquer la procédure MRD pour toute demande au PCC.[102]

[102] *Ann. parl., C.R.I,* Chambre, 2015-16, 6 janvier 2016, Q. n° 8170.

III.1. LES CHIFFRES RELATIFS AUX MÉTHODES SPÉCIFIQUES ET EXCEPTIONNELLES

Entre le 1er janvier et le 31 décembre 2015, 1392 autorisations ont été accordées par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement, 1271 pour la VSSE (1143 spécifiques et 128 exceptionnelles) et 121 par le SGRS (87 spécifiques et 34 exceptionnelles).

Le tableau ci-dessous établit une comparaison avec les chiffres des années précédentes.

	SGRS		VSSE		TOTAL
	Méthode spécifique	**Méthode exceptionnelle**	**Méthode spécifique**	**Méthode exceptionnelle**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392

Alors qu'une diminution de 7 % était enregistrée en 2014, le nombre total de méthodes particulières de renseignement a connu une augmentation légèrement supérieure en 2015. L'accroissement se situe exclusivement au niveau des méthodes spécifiques mises en œuvre par la VSSE (de 976 en 2014 à 1143 en 2015). Tant l'ensemble des méthodes particulières mises en œuvre par le SGRS que les méthodes exceptionnelles mises en œuvre par la VSSE ont connu une baisse significative.

Dans ce qui suit, trois rubriques sont établies pour chaque service : des données chiffrées sur les méthodes spécifiques, des données chiffrées sur les méthodes exceptionnelles et des données chiffrées sur les menaces visées par les différentes méthodes ainsi que sur les intérêts à protéger.

III.1.1. LES MÉTHODES RELATIVES AU SGRS

III.1.1.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	14	7	4
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	0	0	0

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	0	0	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	66 méthodes	67 méthodes	55 méthodes
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	15	12	12
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	36	28	16
TOTAL	**131**[103]	**114**	**87**

La tendance à moins utiliser les « observations » et les « localisations », constatée en 2014, s'est confirmée en 2015. On note également une diminution du nombre de « prises de connaissance de données d'identification », tandis que le nombre de « prises de connaissance de données d'appel » est resté stable.[103]

III.1.1.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	1	1	3
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	0	1	0
Création ou recours à une personne morale fictive	0	0	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	0	0	0
Collecte de données concernant des comptes bancaires et des transactions bancaires	5	5	3

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

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
Intrusion dans un système informatique	0	03	3
Écoute, prise de connaissance et enregistrement de communications	17	26	25
TOTAL	**23**[104]	**36**	**34**

En ce qui concerne les méthodes exceptionnelles, il convient de constater que le nombre de mesures d'écoute est resté stable (25 en 2015 contre 26 en 2014), et ce contrairement à l'année 2013 où il avait sensiblement augmenté.

III.1.1.3. Les intérêts et les menaces justifiant le recours aux méthodes particulières[105]

Le SGRS est autorisé à utiliser des méthodes spécifiques et exceptionnelles dans le cadre de trois de ses 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).

NATURE DE LA MISSION	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
Mission de renseignement	111	109	112
Sécurité militaire	15	5	6
Protection de secrets	28	36	4

En ce qui concerne la nature de la mission, on relève un *statu quo* pour la « mission de renseignement » et la « sécurité militaire ». La « protection des secrets » a, quant à elle, enregistré une forte diminution (36 en 2014, à peine 4 en 2015).

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

105 Plusieurs intérêts et menaces peuvent figurer dans une même autorisation.

NATURE DE LA MENACE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
Espionnage	94	123	101
Terrorisme (et processus de radicalisation)	6	7	4
Extrémisme	24	15	13
Ingérence	1	0	4
Organisations criminelles	16	2	0
Autre	13	0	0

En ce qui concerne la nature de la menace, il apparaît que la tendance à moins recourir aux MRD dans le cadre du « terrorisme » et de l'« extrémisme » s'est poursuivie en 2015 (30 en 2013 ; 22 en 2014 et seulement 17 en 2015). Cette tendance peut sembler surprenante au vu de l'augmentation relative de ces menaces en 2015. La menace « espionnage » a elle aussi opéré une courbe rentrante en 2015 (101 contre encore 123 en 2014).

III.1.2. LES MÉTHODES RELATIVES À LA VSSE

III.1.2.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	109	86	86
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	0	0	0
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	0	0	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	613 méthodes	554 méthodes	663
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	136	88	33
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	244	248	361
TOTAL	**1102**	**976**	**1143**

Comme indiqué précédemment, le nombre total d'autorisations relatives à la mise en œuvre de méthodes spécifiques par la VSSE a augmenté. Ainsi, en 2015, un accroissement significatif a été observé pour les « prises de connaissance de données d'identification » (554 en 2014 contre 663 en 2015) et pour les « prises de connaissance de données de localisation » (248 en 2014 contre 361 en 2015). Le nombre de prises de connaissance de données d'appel a encore diminué (de 88 à 33 en 2015). En ce qui concerne les observations, on constate que le nombre de personnes observées a pratiquement doublé, passant de 71 en 2014 à 141 en 2015.

III.1.2.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	6	9	6
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	6	21	8
Création ou recours à une personne morale fictive	0	0	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	6	18	5
Collecte de données concernant des comptes bancaires et des transactions bancaires	11	8	6
Intrusion dans un système informatique	12	18	16
Écoute, prise de connaissance et enregistrement de communications	81	86	87
TOTAL	**122**[106]	**156**	**128**

La diminution du nombre de méthodes exceptionnelles mises en œuvre résulte principalement de la baisse sensible du nombre d' « inspections » (9 en 2015, contre encore 21 en 2014) et du nombre d' « ouvertures de courrier » (18 en 2014 contre 5 seulement en 2015). En revanche, le nombre d' « écoutes de communications » continue d'augmenter légèrement (de 81 en 2012 à 86 en 2013, pour passer à 91 en 2015).

III.1.2.3. Les menaces et les intérêts justifiant le recours aux méthodes particulières

Le tableau suivant reprend les menaces (potentielles) dans le cadre desquelles la VSSE a accordé des autorisations spécifiques et exceptionnelles. Une méthode

106 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste.

peut naturellement viser plusieurs menaces. La VSSE peut utiliser les méthodes spécifiques dans le cadre de toutes les menaces qui entrent dans ses compétences (art. 8 L.R&S). Les méthodes exceptionnelles ne peuvent pas être mises en œuvre 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). La loi définit les diverses notions comme suit :

1. l'espionnage : le recueil ou la livraison d'informations non accessibles au public, et le fait d'entretenir des intelligences de nature à les préparer ou à les faciliter ;
2. le terrorisme : le recours à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d'atteindre ses objectifs par la terreur, l'intimidation ou les menaces ;
   Processus de radicalisation : un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes ;
3. l'extrémisme : les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit ;
4. la prolifération : le trafic ou les transactions relatives aux matériaux, produits, biens ou know-how pouvant contribuer à la production ou au développement de systèmes d'armement non conventionnels ou très avancés. Sont notamment visés dans ce cadre le développement de programmes d'armement nucléaire, chimique et biologique, les systèmes de transmission qui s'y rapportent, ainsi que les personnes, structures ou pays qui y sont impliqués ;
5. les organisations sectaires nuisibles, c'est-à-dire tout groupement à vocation philosophique ou religieuse, ou se prétendant tel, qui, dans son organisation ou sa pratique, se livre à des activités illégales dommageables, nuit aux individus ou à la société ou porte atteinte à la dignité humaine ;
6. l'ingérence : la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins ;
7. les organisations criminelles, c'est-à-dire toute association structurée de plus de deux personnes, établie dans le temps, en vue de commettre de façon concertée des crimes et délits, pour obtenir, directement ou indirectement, des avantages patrimoniaux, en utilisant l'intimidation, la menace, la violence, des manœuvres frauduleuses ou la corruption ou en recourant à des structures commerciales ou autres pour dissimuler ou faciliter la réalisation des infractions. Sont visées dans ce cadre les formes et structures des organisations criminelles qui se rapportent intrinsèquement aux activités visées dans des menaces précédentes ou qui peuvent avoir des conséquences déstabilisantes sur le plan politique ou socio-économique.

En considérant que plusieurs menaces peuvent figurer dans une même autorisation, les chiffres sont les suivants :

NATURE DE LA MENACE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
Espionnage	359	319	253
Terrorisme (et processus de radicalisation)	580	499	812
Extrémisme	246	267	171
Proliferation	15	33	30
Organisations sectaires nuisibles	9	0	0
Ingérence	8	10	10
Organisations criminelles	9	8	0

Les chiffres repris ci-dessus montrent qu'en ce qui concerne la mise en œuvre de MRD, le « terrorisme » a été la priorité absolue de la VSSE en 2015 (de 499 en 2014 à 812 en 2015). On dénombre en revanche moins d'autorisations en matière de menaces liées à l' « extrémisme » (171 contre encore 267 en 2014) et à l'« espionnage » (de 319 en 2014 à 253 en 2015). On note donc un glissement partiel de l'utilisation des moyens MRD disponibles vers la lutte contre le terrorisme.

La compétence de la VSSE n'est pas seulement déterminée par la nature de la menace. Le service n'est autorisé à intervenir que pour la sauvegarde d'intérêts bien déterminés :

- la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, c'est-à-dire :
  a) la sécurité des institutions de l'État et la sauvegarde de la continuité du fonctionnement régulier de l'État de droit, des institutions démocratiques, des principes élémentaires propres à tout État de droit, ainsi que des droits de l'homme et des libertés fondamentales ;
  b) la sécurité et la sauvegarde physique et morale des personnes et la sécurité et la sauvegarde des biens;
- la sûreté extérieure de l'État et les relations internationales : la sauvegarde de l'intégrité du territoire national, de la souveraineté et de l'indépendance de l'État, des intérêts des pays avec lesquels la Belgique poursuit des objectifs communs, ainsi que des relations internationales et autres que la Belgique entretient avec des États étrangers et des institutions internationales ou supranationales;
- la sauvegarde des éléments essentiels du potentiel scientifique et économique.

En considérant que plusieurs menaces peuvent figurer dans une même autorisation, les chiffres sont les suivants pour l'année 2015 :

INTÉRÊTS PROTÉGÉS	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel	1177	1100	1258
La sûreté extérieure de l'État et les relations internationales	1160	1075	1150
La sauvegarde des éléments essentiels du potentiel scientifique et économique	11	10	4

III.2. LES ACTIVITÉS DU COMITÉ PERMANENT R EN SA QUALITÉ D'ORGANE JURIDICTIONNEL ET D'AUTEUR D'AVIS PRÉJUDICIELS

III.2.1. LES CHIFFRES

Cette section reprend les activités du Comité permanent R relatives aux méthodes de renseignement spécifiques et exceptionnelles, avec une attention exclusive portée aux décisions juridictionnelles prises en la matière. Il convient toutefois de souligner au préalable que le Comité soumet *toutes* les autorisations de mise en œuvre de méthodes particulières à une enquête *prima facie*, et ce en vue de décider d'une éventuelle saisine.

En vertu de l'article 43/4 L.R&S, le Comité permanent R peut être saisi de cinq manières :

- 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.

Par ailleurs, 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, le cas échéant, un avis sur la légalité des méthodes spécifiques ou exceptionnelles ayant fourni des renseignements 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. Le Comité n'intervient pas alors *stricto sensu* comme un organe juridictionnel.

TYPE DE SAISINE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015
1. D'initiative	16	13[107]	16
2. Commission Vie Privée	0	0	0
3. Plainte	0	0	0
4. Suspension par la Commission BIM	5	5	11[108]
5. Autorisation du ministre	2	1	0
6. Auteur d'avis préjudiciel	0	0	0
TOTAL	**23**	**19**	**27**

Une fois saisi, le Comité peut prendre plusieurs types de décisions (intermédiaires). Cependant, dans deux cas (voir 1. et 2. ci-après), une décision est prise avant la saisine proprement dite.

1. 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) ;
2. décider de ne pas donner suite à une plainte qui est manifestement non fondée (art. 43/4, alinéa 1er, L.R&S) ;
3. suspendre la méthode contestée dans l'attente d'une décision définitive (art. 43/4, dernier alinéa, L.R&S) ;
4. demander des informations complémentaires à la Commission BIM (43/5 § 1er, alinéa 1er et alinéa 3, L.R&S) ;
5. demander des informations complémentaires au service de renseignement concerné (43/5 § 1er, alinéa 3, L.R&S) ;
6. ordonner une mission d'enquête pour le service d'Enquêtes R (art.43/5 § 2, L.R&S). Dans cette rubrique, il n'y a aucune référence aux multiples informations complémentaires recueillies par le service d'Enquêtes R avant la saisine proprement dite et donc d'une manière plutôt informelle ;
7. procéder à l'audition des membres de la Commission BIM (art. 43/5 § 4, alinéa 1er, L.R&S) ;
8. 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) ;
9. 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) ;

107 Dans deux cas, la décision du Comité n'a été rendue qu'en janvier 2015.

108 Dans un dossier, la saisine a eu lieu en 2015, mais le Comité n'a pris sa décision qu'en 2016.

10. 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) ;
11. 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) ;
12. 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 ;
13. 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 ;
14. constater l'incompétence du Comité permanent R ;
15. déclarer le caractère infondé de l'affaire pendante et permettre la poursuite de la méthode ;
16. délivrer un avis préjudiciel (articles 131*bis*, 189*quater* et 279*bis* CIC).

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 L.R&S). Ce délai a été respecté dans tous les dossiers.

NATURE DE LA DÉCISION	**2013**	DÉCISION FINALE **2013**	**2014**	DÉCISION FINALE **2014**	**2015**	DÉCISION FINALE **2015**
1. Plainte frappée de nullité	0		0		0	
2. Plainte manifestement non fondée	0		0		0	
3. Suspension de la méthode	0		3		2	
4. Information complémentaire de la Commission BIM	0		0		0	
5. Information complémentaire du service de renseignement	0		1		1	

NATURE DE LA DÉCISION	**2013**	DÉCISION FINALE **2013**	**2014**	DÉCISION FINALE **2014**	**2015**	DÉCISION FINALE **2015**
6. Mission d'enquête du Service d'Enquêtes R	50		54		48	
7. Audition membres de la Commission BIM	0		0		2	
8. Audition membres des services de renseignement	0		0		2	
9. Décision relative au secret de l'instruction	0		0		0	
10. Informations sensibles lors de l'audition	0		0		0	
11. Cessation de la méthode	9		3		3	
12. Cessation partielle de la méthode	5		10		13	
13. Levée (partielle) de l'interdiction de la Commission BIM	2	**23**	0	**17**	4	**26**
14. Incompétence	0		0		0	
15. Autorisation légale/ Non- cessation de la méthode/Non-fondement	7		4		6	
16. Avis préjudiciel	0		0		0	

En 2015, le Comité a pris 26 décisions, contre 17 en 2014. Cette augmentation tient au fait que le Comité s'est davantage saisi en 2015 (de 13 à 16 fois), mais surtout que la Commission BIM a procédé plus souvent à la suspension de méthodes (de 5 fois en 2014 à 11 fois en 2015).

Il est par ailleurs intéressant de souligner que le Comité permanent R a entendu pour la première fois des membres de la Commission BIM, et ce dans deux dossiers.

III.2.2. LA JURISPRUDENCE

La substance des décisions finales prises par le Comité permanent R en 2015 est reprise ci-après. Les synthèses sont expurgées des données opérationnelles. Seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue

juridique : le Comité a dû faire preuve de la prudence requise, étant donné que de nombreuses décisions du Comité ont nécessité une classification (sept au niveau « CONFIDENTIEL », cinq au niveau « SECRET » et deux au niveau « TRÈS SECRET »). Dans le présent rapport, le Comité s'est parfois vu contraint de ne pas reprendre explicitement certains éléments juridiques (voir ci-après).

Les décisions ont été regroupées en cinq rubriques :

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

Lorsque cela s'avérait pertinent, certaines décisions ont été reprises dans plusieurs rubriques.

III.2.2.1. Exigences légales (de forme) préalables à la mise en œuvre d'une méthode

III.2.2.1.1. Notification préalable à la Commission BIM

Une méthode spécifique ne peut être effectivement utilisée qu'après la notification de l'autorisation à la Commission BIM (article 18/3 § 1er, alinéa 2 L.R&S). Dans les dossiers 2015/4355, 2015/4356 et 2015/4199, la Commission a été informée de l'autorisation, alors que la mise en œuvre de la méthode avait déjà débuté, ou a été informée tardivement de la prolongation de la méthode. Aussi la Commission a-t-elle suspendu les méthodes pour la partie précédant la notification. Le Comité a chaque fois confirmé ces décisions.

III.2.2.1.2. Projet d'autorisation, avis conforme et autorisation d'une méthode exceptionnelle

Un service de renseignement a soumis un projet d'autorisation en vue de procéder à une mesure d'écoute pendant un mois (dossier 2015/4170). La Commission BIM a rendu un avis conforme. Toutefois, dans l'autorisation finale du dirigeant du service, la mesure d'écoute était autorisée pour 48 heures (et donc plus pour un mois). Bien que ne correspondant pas à l'avis conforme, le Comité a établi « *que cette réduction de temps ne pose pas de problème* ».

Dans le dossier 2015/3713, il était question d'une autre problématique. Le service de renseignement avait l'autorisation de mettre une cible sur écoute pendant deux mois. À l'expiration de ce délai, la méthode n'a pas cessé, mais le service a omis de demander une prolongation. Il s'en est lui-même aperçu après plusieurs jours et en a informé la Commission BIM, qui a suspendu la méthode à

compter de la fin du premier mandat (légal). Sur ce, le Comité a tranché : « *[il] ne peut que constater que la méthode est illégale depuis le [xxx] 2015 à OO H en l'absence de décision de prolongation de la méthode* ».

Dans un troisième dossier (2015/3718), une autorisation était accordée pour mettre sur écoute un GSM bien déterminé appartenant à une cible. Mais le service a également mis sur écoute un second appareil utilisé par l'intéressé. Quand elle l'a constaté, la Commission BIM a procédé à la suspension partielle de la méthode, étant donné qu'aucun projet d'autorisation n'avait été présenté et aucun avis conforme n'avait été obtenu. Selon le Comité, « *Attendu que la Commission BIM, dans sa décision de suspension partielle, a établi, à juste titre, que, pour la partie de la méthode concernée, aucun avis conforme n'a été fourni par la Commission BIM. Qu'elle s'est prononcée à juste titre sur une suspension partielle, pour ce qui concerne le second GSM* » (traduction).

Enfin, dans le dossier 2015/3545, la Commission BIM avait rendu un avis négatif sur un projet d'autorisation. Le dirigeant du service a cependant autorisé la méthode exceptionnelle par erreur. Lorsque cette erreur a été découverte, il a aussitôt été mis fin à la méthode, que le Comité a ensuite aussi déclarée illégale. « *Attendu qu'en l'absence d'avis conforme de la Commission BIM, la méthode exceptionnelle ne peut être mise en œuvre en application de l'article 18/10 § 3 al. 2 et que cette décision de la Commission BIM est sans recours* ».

III.2.2.1.3. Mentions obligatoires dans l'autorisation

Dans quatre dossiers, le Comité permanent R a dû se pencher sur la question de savoir si, dans une autorisation du dirigeant du service, certaines données devaient obligatoirement être reprises. Il s'agissait de la date de la décision, du nom de la cible et de l'article de loi correct relatif à la compétence du service.

Ainsi, l'autorisation pour la mise en œuvre d'une méthode spécifique n'était pas datée (dossier 2015/4065). Le Comité a dès lors jugé que la décision n'était pas nulle, contrairement à ce qui est stipulé à l'article 18/10 § 2, alinéa 1er L.R&S pour les méthodes exceptionnelles.

Par définition, le nom de la cible ne doit pas non plus être mentionné dans la décision (dossiers 2015/4064 et 2015/4065). Le Comité a constaté que la mention de l'identité d'une cible n'est pas requise par la loi et que la cible pouvait être identifiée d'une autre façon, si bien qu'aucun problème ne se posait en l'espèce pour apprécier la légalité, la proportionnalité et la subsidiarité. Et le Comité de souligner que les obligations de secret auxquelles les membres d'un service de renseignement sont soumis, ne peuvent entraver la mission légale de contrôle, telle que décrite à l'article 43/5 §§ 1er et 4 L.R&S.

Dans le dernier dossier (2015/3687), le service de renseignement concerné avait mentionné un article de loi incorrect. Le service souhaitait retrouver, via un moyen technique, où et quand une cible avait utilisé son GSM. Ensuite, les

numéros qu'elle a contactés devaient être identifiés. Le Comité a remarqué que le service « *pour la qualification juridique de la méthode, invoque à tort l'art. 18/4 L.R&S, en combinaison avec l'art. 18/7, § 1er, 1° L.R&S* » (traduction). L'article 18/4 L.R&S ne vise que l'observation de personnes, d'objets, de lieux et d'événements. Le moyen technique utilisé ne l'a été que pour l'obtention d'une identification de numéros de téléphone. Le Comité a estimé que l' « *opération dans son ensemble doit être examinée sous l'angle de la qualification de la méthode* » (traduction), si bien que le service n'aurait dû s'en rapporter qu'à l'article 18/7 § 1er, 1° L.R&S pour les deux parties de la méthode. Mais la méthode n'a pas été déclarée illégale pour autant.

III.2.2.1.4. Procédure d'extrême urgence lors de la réquisition d'un opérateur

Un service de renseignement avait procédé, en extrême urgence, à l'identification et à la localisation de données d'appel d'un appareil déterminé (article 18/7 § 2 et article 18/8 § 2 L.R&S) (dossier 2015/4171). La décision orale requise du dirigeant du service était confirmée par une décision écrite motivée. Cette décision a été portée à la connaissance de la Commission BIM, qui souhaitait obtenir des informations complémentaires sur la durée de la méthode. Mais, rappelant une décision antérieure (dossier 2011/227), le Comité a observé que plusieurs autres éléments manquaient dans la décision : le nom de l'officier de renseignement, la date et l'heure de la réquisition ainsi que la date et l'heure de la confirmation écrite. « *Attendu que l'absence d'information sur les éléments précités ne permet pas au Comité permanent R d'apprécier le respect des conditions posées par l'art. 18/7 § 2 et 18/8 § 2 de la L.R&S pour procéder à une réquisition d'extrême urgence* ». À la demande du Comité, le service concerné a encore pu fournir ces données. La méthode a dès lors été considérée comme légale.

III.2.2.1.5. Légitimité de la procédure d'extrême urgence

Étant donné le caractère très urgent de la mise en œuvre d'une méthode exceptionnelle, le service de renseignement a demandé au président de la Commission BIM s'il était possible, dans ce cas, d'obtenir très rapidement une décision de la Commission dans son ensemble (dossier 2015/3530). Dans la négative, il invoquerait la procédure d'extrême urgence visée à l'article 18/10 § 4 L.R&S. Le président a conseillé d'utiliser cette procédure exceptionnelle parce que, selon lui, il était impossible d'encore réunir la Commission ce jour-là. Par conséquent, il a été décidé de commun accord de ne recueillir que l'avis oral du président. Quelques jours plus tard, le président a confirmé son avis oral et, en exécution de l'article 10 de l'AR du 12 octobre 2010, il a communiqué sa décision aux autres membres de la Commission. Le Comité a constaté que « *le Président de la Commission BIM a estimé qu'il n'était pas possible de réunir la Commission le vendredi après-midi pour des raisons qui lui appartiennent et sur lesquelles le*

Comité permanent R n'a pas à se prononcer ; Attendu néanmoins que le Comité permanent R fait observer que cette décision a été prise un vendredi après-midi pendant les heures habituelles d'ouvertures des locaux, et qu'en cas d'indisponibilité d'un ou de plusieurs membres de la Commission BIM, des membres suppléants sont nommés et peuvent être contactés pour remplacer le ou les membres absents ; Attendu que le Comité permanent R doit, in casu, apprécier si la décision prise par [le service de renseignement] de recourir à la procédure d'extrême urgence est ou non légale ; Attendu en l'espèce que l'urgence de la situation et la gravité de la menace imposaient […] de recourir, sans délai, à la procédure prévue par l'art. 18/10 § 4 ».

La méthode a dès lors été autorisée pour 48 heures. Mais vu l'expiration du délai pendant le week-end et vu la nécessité de poursuivre l'exécution de la méthode, il fallait décider si la méthode devait être prolongée par le biais de la procédure ordinaire ou exceptionnelle (dossier 2015/3531). Le service concerné a donc repris contact avec le président de la Commission BIM. Tant le service que le président étaient au courant qu'une prolongation de la méthode s'imposait et que cela devrait avoir lieu le week-end. Mais le président a choisi de ne pas réunir sa Commission immédiatement ou pendant le week-end. Le Comité a remarqué qu' « *une réunion de la Commission BIM, avant l'échéance des 48 heures, était possible en convoquant les autres membres et/ou leurs suppléants ; Attendu que le Comité permanent R doit apprécier, in casu, si la décision prise par [le service de renseignement] de recourir à la procédure d'extrême urgence est ou non légale ; Attendu que dans des circonstances analogues, le Comité permanent R a déjà décidé qu'en cas d'impossibilité de réunir la Commission BIM – quelles que soient les raisons de cette impossibilité – pour statuer sur une méthode exceptionnelle, [le service de renseignement] pouvait mettre en œuvre une autre procédure prévue par la loi, en l'espèce, avoir recours au ministre [compétent], sans attendre l'écoulement du délai de 4 jours prévu par l'art. 18/10 § 3 de la loi (dossier BIM 2012/1308 – 2012/1309 – 2013/2327 et 2013/2328)* ».

III.2.2.2. Motivation de l'autorisation

Des décisions relatives à la mise en œuvre de méthodes particulières doivent être motivées de manière suffisamment précise. Comme chaque année, le Comité permanent R a dû insister à plusieurs reprises sur cette obligation.

Un service de renseignement souhaitait en apprendre le plus possible sur les contacts belges de plusieurs numéros de GSM étrangers (dossier 2015/4101). Il souhaitait aussi récolter certaines données de localisation et d'identification. Mais ces aspects de la méthode n'étaient pas motivés, si bien qu' « *en l'absence de motivation, les deux méthodes sont illégales* » (dossier 2015/4101).

Dans les dossiers 2015/4150 et 2015/4170, le Comité a également constaté que les méthodes n'étaient pas motivées dans la décision. Aussi a-t-il décidé que les méthodes étaient illégales.

Dans sa décision d'effectuer une observation, le dirigeant du service avait établi dans un paragraphe que la méthode couvrirait une période de deux mois, alors que plus loin dans le texte, il était question d'un délai d'un mois (dossier 2015/4163). Le Comité a en outre constaté qu'auparavant, pour la même cible, une méthode d'un mois seulement était chaque fois présentée. « *Attendu que, donc, aussi vu la contradiction en termes de délais mentionnés dans la décision MRD, le Comité estime que la méthode ne peut être appliquée que pendant un mois* » (traduction). Le Comité a dès lors décidé que la méthode était en partie illégale.

III.2.2.3. Les exigences de proportionnalité et de subsidiarité

Une méthode ne doit pas seulement satisfaire à plusieurs exigences légales, elle doit aussi être en lien avec la menace sous-jacente et ne peut être plus intrusive que nécessaire.

Un service de renseignement voulait procéder à l'identification des moyens de communication d'une personne, à la prise de connaissance de ses données de communication et à la localisation de l'origine et de la destination de ses communications, et ce sur une longue période (15 mois) (dossier 2015/3818). Le service souhaitait notamment vérifier si cet individu « *pourrait être impliqué ou non dans un processus de recrutement par un pays étranger* ». Le Comité a certes jugé que « *la menace potentielle est réelle compte tenu de l'origine du [target] et des pratiques du pays concerné et que les méthodes ordinaires ne permettent pas d'obtenir les informations recherchées* », mais il s'est interrogé sur la proportionnalité : « *la méthode d'identification (article 18/7§ 1-1°) et la méthode de repérage (article 18/8§ 1-1°) permettant d'obtenir les informations utiles mais que la méthode de localisation (article 18/8§ 1-2°) apparait, à ce stade, disproportionnée par rapport à la gravité réelle de la menace décrite, vu le caractère plus intrusive de cette méthode* ».

Dans deux dossiers (2015/3999 et 2015/4000), le service souhaitait, six mois durant, appliquer plusieurs méthodes spécifiques sur une cible dont on savait qu'elle se trouverait quelques jours sur le territoire belge à cette période. Le service spécifiait que les méthodes ne seraient appliquées qu'à ce moment-là. Le Comité a estimé que, vu les éléments concrets du dossier, le délai de six mois n'était pas proportionnel et a jugé que « *la méthode, dans l'état actuel des choses, ne peut être appliquée que durant 1 mois* » (traduction).

Dans le dossier 2015/4154, le service concerné voulait mettre en œuvre trois méthodes spécifiques : le repérage de données d'appel, l'identification et la localisation de chaque numéro belge qui était en contact avec un numéro

étranger. Le Comité a jugé que « *les principes de proportionnalité et de subsidiarité ne sont respectés que si la méthode de localisation se limite à la localisation des numéros de téléphone détectés au moment de la communication avec la cible étrangère. Qu'en effet les numéros identifiés ne peuvent jamais faire l'objet d'une localisation générale, donc aussi en dehors des contacts qu'ils ont avec la cible étrangère* » (traduction). Le Comité a néanmoins constaté que « *la méthode spécifique […] est légale au regard de la précision susmentionnée* » (traduction).

Lorsqu'un service de renseignement a voulu prolonger d'un an l'observation d'un lieu déterminé avec une caméra fixe (la méthode courait alors depuis plusieurs années), la question de la proportionnalité s'est posée (dossier 2015/4199). Le Comité a attiré l'attention sur le fait que « *la Loi R&S ne prévoit pas de procédures particulières pour la prolongation ou le renouvellement d'une méthode spécifique, si ce n'est que la nouvelle décision du chef de service doit répondre aux conditions fixées par l'article 18 § 3 de la loi ; que la loi n'exige pas de conditions plus strictes pour évaluer la proportionnalité et la subsidiarité* ». Étant donné que les images à enregistrer pouvaient fournir des renseignements sur une organisation considérée comme terroriste et parce que le travail de renseignement se déroule nécessairement sur une longue période, le Comité n'avait aucune objection à la prolongation de la méthode. Le Comité a par ailleurs fait remarquer que le travail déjà réalisé avait porté ses fruits. « *Que le Comité a déjà décidé, à plusieurs reprises, que la durée d'un an était raisonnable eu égard aux missions des services de renseignement qui sont entre autre de travailler sur le moyen et le long terme ; que cette nature particulière du travail de renseignement diffère essentiellement du travail policier qui est spécifiquement lié à la recherche des auteurs d'une infraction* ».

Dans les trois derniers dossiers, enfin, le Comité s'est basé sur sa jurisprudence constante, qui établit que dans certains cas, il faut connaître les résultats de méthodes antérieures avant de décider si les méthodes suivantes sont proportionnelles et subsidiaires.

Ainsi, un service de renseignement souhaitait mettre en œuvre une multitude de méthodes spécifiques pour recueillir un maximum de données sur un numéro de GSM déterminé : la prise de connaissance d'appels entrants et sortants ; leur localisation, pour lesquels le service voulait aussi retourner un an en arrière ; l'identification des numéros obtenus si ceux-ci ne pouvaient pas être obtenus par le biais de méthodes ordinaires ; l'historique des utilisateurs du numéro de GSM depuis sa première activation ; vérifier dans quels GSM ce numéro est utilisé et – enfin – vérifier l'identité des utilisateurs de ces appareils. Le Comité a jugé que cette dernière méthode était illégale. Il convenait en premier lieu d'attendre les résultats des autres méthodes (dossier 2015/3842).

La même problématique s'est présentée dans le dossier 2015/4101. Un service de renseignement voulait obtenir une multitude de données sur les contacts belges de plusieurs numéros de GSM étrangers. Pour ce faire, le service devait

d'abord prendre connaissance des données d'appel de ces numéros étrangers pour, sur cette base, filtrer les numéros belges. Mais dans la même décision, la mise en œuvre immédiate de toute une série de méthodes sur les numéros obtenus était souhaitée. La Commission BIM a procédé à une suspension partielle : *« vu qu'au moment de la notification, il n'était pas possible de soumettre les résultats des méthodes qui devaient encore être appliquées à l'examen de la légalité, de la subsidiarité et de la proportionnalité préalable à la mise en œuvre d'une méthode particulière de renseignement »* (traduction). Le Comité a également estimé que le service devait en premier lieu vérifier si et quels numéros belges étaient en contact avec les numéros étrangers et qui en était l'utilisateur. *« Attendu qu'à ce stade, il n'est pas possible de juger de la légalité, de la proportionnalité et de la subsidiarité de toute autre méthode portant sur ces numéros belges qui seront éventuellement identifiés par les méthodes jugées légales ».*

Dans le dernier dossier (2015/4322), le service voulait, dans un premier temps, prendre connaissance de données d'appels d'un GSM déterminé et procéder à l'identification des personnes avec lesquelles la cible était entrée en contact l'année précédente. Mais l'intention était aussi de procéder ensuite à la prise de connaissance de données d'appels d'autres numéros de téléphone de la même cible : le Comité a jugé que cela n'était pas permis. *« Attendu que la troisième méthode sollicitée porte sur un nombre de numéros à ce jour inconnu pour lesquels le service demande le repérage de numéros entrants et sortants et leur localisation ; que même si le titulaire du GSM faisant l'objet de la méthode est connu, il a peut-être utilisé des cartes prépayées anonymes qui devraient faire l'objet d'investigations particulières ou utiliser des cartes qui lui ont été prêtées par d'autres personnes, en lien ou non, avec la personne ciblée ; qu'il n'est pas possible d'apprécier actuellement, à défaut d'identification plus précise, le respect des principes de proportionnalité de subsidiarité pour ces numéros obtenus ».*

III.2.2.4. 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 évidemment pas employer n'importe quelle technique en vue de recueillir des informations auprès de quiconque. La loi pose des limites claires, et ce à différents niveaux : pour quelle menace et pour la protection de quel intérêt une méthode peut-elle être utilisée ? Quels actes peuvent être posés et quels actes ne peuvent pas être posés ? Par qui, pour quelles données ? Combien de temps une technique peut-elle être employée ? Les mesures peuvent-elles être appliquées en dehors de la Belgique ?… Le Comité permanent R a précisé certaines de ces limites dans quelques décisions.

III.2.2.4.1. Menace (sérieuse) déterminée contre un intérêt à protéger bien défini

Un service de renseignement souhaitait appliquer une méthode particulière à l'égard d'une personne susceptible de fournir des informations utiles, mais qui ne représentait pas elle-même une menace (dossier 2015/4064). Le Comité a souligné que, le cas échéant, la loi ne prévoit pas l'utilisation de MRD. Mais il ressortait clairement de la décision qu'il s'agissait d'activités entrant dans les compétences du service. Le Comité a dès lors jugé que ces activités justifiaient la méthode.

Dans le dossier 2015/4320, le Comité a constaté que les méthodes particulières étaient en partie mises en œuvre dans le cadre d'une problématique qui n'entrait pas dans le champ de compétences du service concerné. Le service souhaitait observer une personne déterminée qui était en fuite à ce moment-là, et observer d'autres personnes suspectées de cacher le fugitif. Le Comité a jugé que « *la personne visée en premier lieu par la méthode n'est pas localisée et que de plus cette personne est recherchée activement par les autorités judiciaires pour sa participation à des actes délictueux d'une extrême gravité, qu'en conséquence il n'est pas possible d'observer actuellement la personne et qu'en cas de découverte de celle-ci, il y a lieu pour les services d'en informer les autorités judiciaires en vue de son arrestation ; Attendu qu'à ce stade, il n'existe pas de finalité de renseignement pour cette personne, mais une finalité judiciaire qui d'ailleurs doit primer* ». Ce raisonnement ne valait pas pour les autres personnes : « *la finalité de renseignement est bien présente indépendamment de l'existence ou non de poursuites judiciaires à leur égard ; qu'en effet, il est indispensable pour [le service de renseignement] de mieux connaître et suivre les personnes qui apportent à la personne recherchée un appui logistique quel qu'il soit* ».

III.2.2.4.2. Collaboration de services étrangers

Le Comité avait déjà estimé que les services de renseignement belges devaient aussi collaborer avec des services partenaires étrangers dans le cadre des méthodes particulières, à la condition que le service belge garde le contrôle effectif sur les méthodes mises en œuvre.[109]

Dans le dossier 2015/3823, le Comité a réitéré cette jurisprudence. Un service de renseignement belge a autorisé l'écoute et l'enregistrement de conversations. Le caractère particulier de l'affaire résidait dans le fait que le dispositif d'écoute serait placé par un service de renseignement étranger. Le service étranger ne prendrait connaissance d'éventuelles conversations qu'au moment où la cible se trouverait à l'étranger. Les informations recueillies seraient ensuite partagées

[109] Voir par exemple COMITÉ PERMANENT R, *Rapport d'activités 2013*, 84-85 et *Rapport d'activités 2014*, 87-88.

avec le service belge. Conformément à l'article 13/1 § 2, alinéa 5 L.R&S, la Commission BIM avait accepté que les agents étrangers placent le moyen technique. Le Comité a précisé que «*l'intervention des collègues [étrangers] ne peut que rester limitée à l'aide ou à l'assistance nécessaire et directe, pour autant que cela soit essentiel au succès de la méthode. Que le [service belge] doit, dans le cadre de cette méthode, veiller de manière très stricte à être et à rester maître de l'opération sur le territoire belge. Attendu que le Comité permanent R impose en outre au [service belge] de surveiller aussi de manière stricte la poursuite de la méthode, et plus particulièrement ce qu'il advient des communications enregistrées. Qu'en effet, il apparaît que les conversations seront en premier lieu traitées par le service [étranger] sur [son] territoire, et que ce n'est qu'après qu'elles seront partagées avec le [service belge]. Qu'ici aussi le [service belge] doit être et rester maître de l'opération et respecter les obligations requises en ce qui concerne la transcription des passages pertinents et la destruction ultérieure de l'enregistrement*» (traduction). Étant donné qu'il ressortait des informations obtenues que le service belge pouvait satisfaire à ces exigences, le Comité a constaté la légalité de l'autorisation.

III.2.2.4.3. La Loi MRD et la Convention de Vienne du 18 avril 1961 sur les relations diplomatiques

Le Comité a de nouveau pris une décision (dossier 2015/3805) où il était question de la Convention de Vienne de 1961.[110] Un service de renseignement souhaitait mettre en œuvre une méthode spécifique. Afin de vérifier si la méthode était conforme aux exigences de cette Convention, la Commission BIM a demandé à deux reprises des précisions au service. La Commission n'a toutefois eu qu'une vue insuffisante sur la nature précise de la méthode et a dès lors procédé à une suspension. Le Comité permanent R a estimé que cette suspension se justifiait, puisqu'il était possible, dans ce cas-ci, que la méthode enfreigne la Convention.

III.2.2.5. Les conséquences d'une méthode (mise en œuvre) illégale(ment)

Un service de renseignement souhaitait appliquer une méthode exceptionnelle combinée à quelques méthodes spécifiques. Vu qu'il apparaissait que la méthode exceptionnelle n'avait pas été demandée de manière légale (voir ci-dessus III.2.2.1.2. – dossier 2015/3545), la Commission BIM a également suspendu les méthodes spécifiques «*en raison de leurs liens étroits avec ladite méthode exceptionnelle*». Le Comité permanent R était toutefois d'un autre avis. «*Attendu que le Comité permanent R constate que les méthodes spécifiques ne sont pas liées à ce point à la méthode exceptionnelle, que le sort de celle-ci entraîne automatiquement le sort de celles-là et que [le chef du service] a justifié, à*

110 Voir aussi COMITÉ PERMANENT R, *Rapport d'activités 2014*, 88.

suffisance de droit dans son projet de décision et dans sa décision, la mise en œuvre desdites méthodes spécifiques qui présentent, toujours actuellement, un intérêt pour [le service]».

III.3. CONCLUSIONS

Sur la base des chiffres de l'année d'activités 2015, le Comité a tiré les conclusions générales suivantes :

- alors qu'en 2014, une diminution était enregistrée, en 2015, le nombre de méthodes particulières est revenu à son niveau de 2013. L'augmentation par rapport à 2014 concerne exclusivement les méthodes spécifiques mises en œuvre par la VSSE (de 976 en 2014 à 1143 en 2015). Tant les méthodes particulières utilisées par le SGRS que les méthodes exceptionnelles utilisées par la VSSE ont décru de manière significative;
- l'accroissement des méthodes spécifiques à la VSSE se situe principalement dans le nombre de « prises de connaissance de données d'identification » (de 554 à 663) et de « prises de connaissance de données de localisation » (de 248 à 361). Les « prises de connaissance de données d'appel » ont diminué (de 88 à 33);
- malgré la légère diminution du nombre de méthodes exceptionnelles à la VSSE, il convient de noter une fois encore un léger accroissement du nombre de mesures d'écoute : 81 en 2013, 86 en 2014 et 91 pour 2015;
- en ce qui concerne le SGRS, il apparaît que la tendance à moins recourir aux MRD dans la lutte contre le terrorisme et l'extrémisme se confirme en 2015 (30 en 2013, 22 en 2014 et seulement 17 en 2015). Cela peut surprendre au vu de la relative augmentation de ces menaces en 2015. La mise en œuvre de MRD contre la menace « espionnage » a également opéré une courbe rentrante en 2015 (101 contre 123 en 2014);
- en ce qui concerne la VSSE, le nombre de MRD en matière de « terrorisme » n'est pas seulement en chiffres absolus, mais il a considérablement augmenté par rapport aux autres menaces telles que l' « extrémisme » et l' « espionnage ». On note donc un glissement partiel des moyens MRD disponibles vers la lutte contre le terrorisme;
- en outre, il convient de noter que dans le cadre des méthodes exceptionnelles, la procédure d'extrême urgence est toujours plus utilisée. Dans ce cas, seul l'avis du président de la Commission BIM est sollicité : 11 fois en 2013 ; 19 fois en 2014 et 25 fois en 2015;
- en 2015, le Comité permanent R a rendu 26 décisions, contre 17 en 2014. Cette hausse tient au fait que le Comité s'est davantage saisi en 2015 (de 13 à 16 fois), mais surtout que la Commission BIM a eu plus souvent recours aux suspensions (de 5 fois en 2014 à 11 fois en 2015).

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, dans des conditions très strictes, écouter des communications, en prendre connaissance et les enregistrer (art. 18/17, § 1er L.R&S).

Il convient toutefois d'établir une distinction claire entre les « interceptions MRD » et « *la recherche, 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.* » Cette seconde forme d'écoute est possible depuis longtemps déjà et peut être mise en œuvre 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 alliées lors de missions à l'étranger ainsi que des ressortissants belges établis à l'étranger (art. 11, § 2, 3° et 4°, L.R&S). Ces écoutes sont elles aussi généralement désignées sous l'appellation « interceptions de sécurité », mais elles sont soumises à un tout autre cadre de contrôle.

Ce contrôle externe 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 compétent pour faire cesser les interceptions en cours, lorsqu'il apparaît que les conditions dans lesquelles elles sont réalisées 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 pourront faire l'objet d'interceptions dans le courant de l'année suivante, 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 doit la communiquer au SGRS. Ensuite, le SGRS est tenu de transmettre la liste et l'autorisation ministérielle au Comité permanent R. En 2015, le Comité permanent R a une nouvelle fois[111] dû insister pour obtenir cette liste, qui ne lui a été fournie qu'à la mi-avril 2015.

---

111 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 103 ('IX.3.2. L'envoi à temps des interceptions de sécurité visées').

Par ailleurs, vu les constats qu'il a posés dans la foulée des révélations d'Edward Snowden[112] et vu l'intention déclarée du SGRS d'utiliser la possibilité de mettre des câbles de télécommunication sur écoute, le Comité entendait approfondir ses connaissances sur les activités SIGINT du SGRS et les actualiser sous la forme d'une étude. Au second semestre de 2015, le Comité a mené diverses inspections et visites concrètes et a été briefé à plusieurs reprises.[113] L'étude a été finalisée en 2016 et a été transmise en juillet au ministre de la Défense et au SGRS.

112 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 8-37 ('II.1. Les révélations d'Edward Snowden et la position d'information des services de renseignement belges').

113 En 2015, un avis a également été rendu à propos d'un nouvel accord de coopération international portant sur les informations SIGINT (voir Chapitre V.1.).

CHAPITRE V
AVIS, ÉTUDES ET AUTRES ACTIVITÉS

Les missions du Comité permanent R sont très variées : réalisation d'enquêtes de contrôle ; juridiction en matière de méthodes particulières de données, missions dans le cadre de la compétence d'interception du SGRS, tâches judiciaires remplies par son service d'Enquêtes, rôle dans l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité… Le Comité mène aussi des études. Par ailleurs, il est consulté, fort de son expertise. Il convient enfin de noter qu'en 2015, le Comité a fait l'objet de trois demandes d'avis officiels sur diverses questions.

V.1. AVIS CONCERNANT LA COOPÉRATION INTERNATIONALE EN MATIÈRE DE SIGINT

Début novembre 2015, le ministre de la Défense a demandé l'avis du Comité permanent R à propos de la coopération multilatérale sur les *foreign terrorist fighters* (FTF). Dans le cadre de cette coopération, des données à caractère personnel et des métadonnées sont échangées et des analyses communes sont réalisées.

Vu l'intérêt actuel et la nécessité d'une coopération internationale et d'un échange d'informations les plus larges possibles, et aussi en raison des moyens de collectes limités des services de renseignement belges à l'étranger, le Comité a rendu un avis positif. Mais il n'en a pas moins rappelé les principes suivants :

– la coopération doit se limiter à la problématique des FTF et des *returnees*. Si le SGRS veut coopérer dans d'autres matières, elles doivent naturellement relever de sa compétence. Le Comité a toutefois établi qu'il devait en être informé, et ce en exécution de l'article 33, alinéa 2, L. Contrôle ;
– le Comité permanent R considérait que le SGRS, dans la situation actuelle, était compétent pour suivre la problématique concernée, puisque les FTF et les *returnees* font peser une menace militaire grave et réelle sur « *la protection ou [à] la survie de la population* » (article 11 § 2, 1°, L.R&S). Le Comité estimait toutefois qu'il y avait lieu de déterminer plus clairement et plus largement la compétence du SGRS en matière de terrorisme djihadiste, sur la

base d'un arrêt qui peut être pris en exécution de l'article 11, § 1er, 1° L.R&S[114];

- le Comité a ensuite rappelé avec insistance l'obligation reprise à l'article 20, § 3, L.R&S, par laquelle le Conseil national de sécurité doit prendre les directives nécessaires en matière d'échange d'informations et de coopération. Plus concrètement:
  - il faut préciser quels critères le SGRS doit utiliser lorsqu'il décide de coopérer ou non, même partiellement, avec certains pays et avec leurs services de renseignement respectifs;
  - des critères plus précis doivent être élaborés pour le transfert de données (à caractère personnel) aux pays tiers avec lesquels il existe une coopération (partielle). Il faut de toute manière surveiller l'utilisation que peuvent faire les pays tiers de ces informations, par exemple en les reprenant sur des «listes noires». Dès lors, il faut notamment indiquer clairement quel usage ces pays tiers sont autorisés à faire, et ce pour chaque information communiquée;
  - les exigences de la Loi vie privée doivent être respectées. Le Comité faisait notamment référence à la qualité et à la pertinence des informations transmises. Une indication de la valeur des informations communiquées est un instrument utile à cette fin;
  - il convient de prévoir des garanties renforcées pour le transfert de données vers des pays faisant partie du réseau, qui ne pourraient pas offrir les mêmes garanties en matière de protection des données (articles 21 et 22 Loi vie privée);
- lorsque d'autres services belges (police, autorités judiciaires, VSSE…) veulent, par l'entremise du SGRS, partager des informations en utilisant le réseau de coopération, ils doivent eux-mêmes veiller à ce que ce partage ne sorte pas du cadre de leurs compétences respectives. De plus, les autorités administratives ou judiciaires compétentes doivent indiquer clairement quelles informations peuvent être communiquées, certainement s'il s'agit de données à caractère personnel;
- lorsque le SGRS transmet une *Request for Information* émanant d'un autre service belge vers le réseau de coopération, le SGRS doit toujours veiller à ce que cette question entre également dans le cadre de sa compétence. Par exemple, le SRGS doit tenir compte des limites des possibilités de son «*concours et notamment [de son] assitance technique*» (article 20 L.R&S);
- conformément à ses missions légales, le Comité permanent R exerce un contrôle réel sur tous les aspects de la coopération.

114 Le SGRS est compétent pour «*tout autre intérêt fondamental du pays défini par le Roi sur propostion du Comité minitériel*» (art. 11, § 1er, alina 1er, L.R&S).

Enfin, le Comité a établi qu'il est recommandé de mener une réflexion générale et politique sur le fonctionnement du SGRS en ce qui concerne ses compétences, les possibilités en matière de SIGINT, l'assistance aux autorités judiciaires et la coopération avec les partenaires étrangers.

V.2. AVIS RELATIF À L'OCTROI D'UNE HABILITATION DE SÉCURITÉ AUX MEMBRES DE LA NOUVELLE COMMISSION DE SUIVI

Dès 2014, conformément à la sixième réforme de l'État, le règlement de la Chambre a été adapté en ce sens que l'accompagnement du Comité permanent R et le suivi parlementaire des services de police et de renseignement devaient être assurés par une Commission de suivi de la Chambre des Représentants. La possibilité de consulter des informations classifiées, associée à la détention d'une habilitation de sécurité précédée d'une enquête de sécurité, a de nouveau fait l'objet d'un débat.[115]

À la demande du président de la Commission de suivi, le Comité permanent R a rendu un avis à ce propos, en se basant sur la législation existante. Cet avis reprenait plusieurs avantages et inconvénients des deux cas de figure. Une série d'exemples étrangers étaient également cités.[116]

La Commission a finalement décidé de ne rien changer : ses membres ne souhaitaient ni une habilitation de sécurité ni un accès à des informations classifiées.

La non-communication d'informations secrètes aux parlementaires concernés ne nuit en rien à la qualité du contrôle démocratique.[117] La pratique a montré que la plupart du temps, le Comité permanent R fait rapport de manière significative à la Commission de suivi, sans révéler de secrets.

---

115 Ce sujet avait déjà été abordé : Voir notamment T. VAN PARYS, 'Van parlementaire onderzoekscommissie over Pinksterplan tot Toezichtwet' et H. VAN HEVELE, 'Parlementair toezicht na de Toezichtwet' dans W. VAN LAETHEM et J. VANDERBORGHT, *Regards sur le contrôle. Vingt ans de contrôle sur les services de renseignement*, Intersentia, Anvers, 2013.

116 Pour certains aspects, une comparaison a été établie avec des pays voisins (pour plus de détails, voir '4.5. Access to classified information by parliaments and specialised oversight bodies' in EUROPEAN PARLIAMENT, Directorate-General for Internal Policies, Policy Department Citizens' Rights and Constitutional Affairs, Justice, Freedom and Security, *Parliamentary oversight of security and intelligence agencies in the European Union*, 2011, 117-131).

117 À ce propos : W. VAN LAETHEM, 'Alles onder controle ! Een (ver)nieuw(d)e Kamercommissie die toeziet op de politie- en de inlichtingendiensten', *Vigiles*, 2015/1, 9-16., en particulier 14 et suiv.

V.3. AVIS SUR UNE PROPOSITION DE LOI CONCERNANT LE CONTRÔLE DES ACTIVITÉS DES SERVICES DE RENSEIGNEMENT ÉTRANGERS EN BELGIQUE

En juillet 2015, sur base de l'article 33, alinéa 7, L. Contrôle, la Commission de suivi a demandé un avis au Comité permanent R sur la proposition de loi modifiant la Loi organique des services de renseignement et de sécurité concernant le contrôle des activités des services de renseignement étrangers en Belgique.[118]

Dans son avis[119], le Comité a souligné qu'il souscrivait pleinement à l'esprit de la proposition. En effet, le Comité avait déjà recommandé à plusieurs reprises[120] de procéder à une modification de la loi, par laquelle les services de renseignement belges se verraient attribuer explicitement la compétence de suivre les activités des services de renseignement étrangers sur le territoire belge, indépendamment d'une éventuelle menace d'espionnage, d'ingérence, d'extrémisme… L'idée sous-jacente est que les activités des agents de renseignement étrangers sur le territoire sont potentiellement problématiques.

V.4. SÉANCE ACADÉMIQUE

En 2015, le Comité a de nouveau renoué avec la tradition en organisant, au Sénat, une séance académique dont le thème était 'L'importance de la formation dans le monde du renseignement'. Les orateurs étaient le professeur Philip H.J. Davies, directeur du *Brunel Centre for Intelligence and Security Studies* (Londres), Lucile Dromer-North, directrice de l'Académie du renseignement (France) et le lieutenant général Eddy Testelmans, chef du SGRS.

Dans le cadre de cette séance, les ministres de la Justice et de la Défense ont signé l'acte constitutif officiel de la *Belgian Intelligence Academy* (BIA). Cette académie organise des formations[121] pour les analystes du service de renseignement civil, mais aussi de son pendant militaire, et a pour mission *« d'être le moteur et la référence en matière de formation professionnelle relative aux renseignements civils et militaires, et ainsi être reconnue pour son expertise et ses compétences. Elle a pour mission de dispenser des formations de qualité, communes et structurées, pour le personnel des services de renseignement »* (traduction).

---

118 *Doc. parl.* Chambre, 2014-15, n°54-553/001.

119 *Doc. parl.* Chambre, 2014-15, n°54-553/002.

120 Voir COMITÉ PERMANENT R, *Rapport d'activités 2006*, 128 ; *Rapport d'activités 2008*, 2 ; *Rapport d'activités 2012*, 93 ; *Rapport d'activités 2014*, 3.

121 En 2015, une formation a été dispensée en deux temps ('Formation de base Analyse').

V.5. CONFÉRENCE AU PARLEMENT EUROPÉEN SUR LE CONTRÔLE DÉMOCRATIQUE DES SERVICES DE RENSEIGNEMENT

Si les activités des services de renseignement relèvent effectivement de la compétence des États membres de l'UE, et si l'article 4, alinéa 2, du Traité sur le fonctionnement de l'Union européenne (TFUE) stipule clairement que la sécurité nationale reste la responsabilité exclusive de chaque État membre, des événements récents démontrent qu'une collaboration entre les services de renseignement nationaux (mais aussi entre leurs organes de contrôle) est plus que jamais nécessaire, et ce dans l'ensemble de l'Union. L'élaboration d'une stratégie européenne en matière de sécurité interne démontre également la nécessité d'améliorer la collaboration et l'échange d'informations au niveau national. En outre, bien que la prévention des menaces pour la sécurité, comme les attaques terroristes, demeure une compétence strictement nationale, le suivi requiert une coopération juridique et judiciaire, tel que reconnu explicitement à l'article 83 TFUE.

Dans ce contexte, la Commission libertés civiles, justice et affaires intérieures du Parlement européen a organisé, avec la Chambre des Représentants belge, le Bundestag allemand et le Parlement italien, les 28 et 29 mai 2015, une conférence sur contrôle démocratique des services de renseignement au sein de l'Union européenne.[122] L'objectif de la conférence était de réunir des acteurs nationaux et européens pertinents dans le domaine des services de renseignement et du contrôle exercé sur ceux-ci, afin de discuter des développements récents et de leurs conséquences pour leurs champs de compétences respectifs. Tant le président de la Commission de suivi, Siegfried Bracke, que le président du Comité permanent R, Guy Rapaille, ont pris la parole lors de cette conférence.

V.6. EXPERT DANS DIVERS FORUMS

En 2015, des membres du Comité permanent R et de son personnel ont été consultés à plusieurs reprises en tant qu'experts par des institutions belges et étrangères, publiques et privées :

– le président du Comité permanent R exerce depuis 2011 la présidence du *Belgian Intelligence Studies Centre (BISC)*. Ce centre s'est assigné l'objectif de rapprocher les services de renseignement et de sécurité et le monde académique, et de contribuer à la réflexion en matière de renseignement.[123] En 2015, le BISC a organisé deux journées d'étude : une première intitulée

122 www.europarl.europa.eu/activities/committees/fr/LIBE/home.html.
123 www.intelligencestudies.be.

'Politie en inlichtingenactiviteiten tijdens de Groote Oorlog: parallellen naar vandaag' (juin 2015) et une seconde à l'occasion de plusieurs « anniversaires » : 185 ans de Sûreté de l'État, 100 ans de renseignement militaire, 70 ans du RUSRA, 5 ans du BISC[124] ;

- un représentant du Comité permanent R a participé à un panel de discussion intitulé *'Hoe kostbaar is onze online privacy'*, organisé à l'occasion de la projection du documentaire 'Citizenfour' de Laura Poitras sur les révélations d'Edward Snowden ;
- il a été fait appel à l'expertise du Comité lors d'un séminaire pratique destiné à la police, à la magistrature et au barreau en matière de « screening de personnes », et ce dans le contexte de la Loi relative à la classification et aux habilitations, attestions et avis de sécurité ;
- en novembre 2015, une délégation du Comité permanent R a participé à la deuxième réunion d'experts *'National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies'*, organisée sur initiative du directeur du *Sector of Information Society, Privacy and Data Protection Freedoms and Justice Department* de l'*European Union Agency for Fundamental Rights* (FRA). Celle-ci est chargée de réaliser une étude comparative sur le contrôle démocratique des services de renseignement dans les États membres de l'Union européenne pour le compte du Parlement européen et dans la foulée de la résolution du 12 mars 2014[125] ;
- fin avril 2015, le président et le greffier du Comité permanent R ont accompagné une délégation de la Commission de la Défense nationale à l'occasion de sa visite aux services de renseignement. Au Quartier Reine Elisabeth, la délégation a été reçue par le lieutenant général Eddy Testelmans, ACOS IS, chef du SGRS, et a ensuite été accueillie dans les locaux de la VSSE par l'Administrateur général Jaak Raes ;
- le Comité continue aussi à participer aux réunions du Groupe européen de recherche sur l'éthique du renseignement (GERER). Ce groupe de travail, composé de représentants des services de renseignement (militaires) français, belges et luxembourgeois, le Comité permanent R…), mène une réflexion sur la relation 'éthique – services de renseignement' ;
- en 2015, un représentant du Comité permanent R était présent à plusieurs réunions du 'Groupe de travail Analyse'[126] ;

---

124 Cela était associé à deux publications détaillées (M. COOLS et al (eds.), *1915-2015. Het verhaal van de Belgische militaire inlichtingen- en veiligheidsdienst*, Antwerpen, Maklu, 2015, 672 (avec notamment une contribution du président du Comité permanent R : 'Le SGRS et le Comité permanent R : « une aventure en terre inconnue »', 577-586) et Baron R. COEKELBERGS et al. (eds.), *Gedenkboek Inlichtings- en Actie Agenten*, Antwerpen, Maklu, 2015, 860) ainsi qu'à l'exposition 'Classified' à Bruxelles (du 7 novembre au 5 décembre 2015).

125 European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks* (http://fra.europa.eu).

126 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 95 et *Rapport d'activités 2013*, 94.

- en mars 2015, le président a fait un exposé sur 'Le renseignement, ses défis et son contrôle', à la demande du Département de Sciences Politiques de la Faculté de Droit de l'Université de Liège ;
- en avril 2015, le président du Comité, a participé à une table ronde 'Justice et renseignement : quelle coopération ?', à l'invitation de l'École nationale de la Magistrature française dans le cadre de la formation 'La réponse judiciaire au terrorisme en Europe' ;
- à l'invitation du *Geneva Centre for the Democratic Control of Armed Forces* (DCAF), le greffier du Comité a participé à une conférence sur le contrôle parlementaire des services de renseignement à l'Institut de Défense Nationale tunisien. Cette conférence s'est déroulée dans le cadre d'un cycle annuel intitulé 'L'établissement d'un nouveau service de renseignement pour la Tunisie', financé par le Fonds d'affectation pour l'Afrique du Nord (TFNA) du DCAF ;
- ensuite, le directeur du service d'Enquêtes R a pris la parole au colloque 4Instance ICT-security (septembre 2015), où les compétences « cyber » du service de renseignement étaient exposées ('(Counter) Attack is the best Defence') ;
- enfin, le greffier du Comité permanent R a été invité, en mars 2015, à expliquer le fonctionnement du Comité dans le cadre du module de formation 'Intelligence' du Master en relations internationales et de diplomatie (Université d'Anvers).

V.7. PROTOCOLE DE COOPÉRATION « DROITS DE L'HOMME »

La Belgique ne disposait pas d'une instance publique chargée de vérifier si la législation actuelle et future était conforme aux arrêts de la Cour européenne des droits de l'homme et aux conventions internationales en matière de droits de l'homme. L'absence d'une 'instance publique des droits de l'homme' était considérée comme une lacune majeure.[127]

Diverses réunions préparatoires organisées avec d'autres institutions disposant d'un mandat en matière de droits de l'homme[128] ont abouti, à la

[127] Le Conseil des droits de l'homme des Nations unies l'a constaté en 2001 lors de son « Examen périodique universel (EPU) ». La Belgique sera de nouveau soumise à cet examen en 2016. Diverses instances avaient déjà insisté pour que la Belgique se dote, à l'instar des pays voisins, d'un institut national des droits de l'homme indépendant (voir, par exemple, *Doc. parl.* Chambre 2012-13, 53-2946/001).

[128] Comme l'Unia (l'ancien Centre interfédéral pour l'égalité des chances), le Centre fédéral de la migration, l'Institut pour l'égalité des femmes et des hommes, la Commission vie privée, le Médiateur fédéral, le Conseil supérieur de la Justice, les Comités permanents P et R.

mi-janvier 2015, à un protocole de coopération[129], dans lequel toutes les instances participantes se sont mises d'accord pour échanger leurs pratiques et leurs méthodes, pour examiner des questions communes et pour promouvoir la coopération mutuelle. En attendant la création d'un institut fédéral des droits de l'homme officiel, elles doivent servir de plateforme de concertation entre des instituts exerçant partiellement ou entièrement un mandat d'institution chargée du respect des droits de l'homme et des libertés. En 2015, les activités de cette plateforme ont consisté à organiser des réunions de concertation mensuelles, au cours desquelles ont été discutés tant les problématiques générales (par exemple, le déroulement de l'Examen périodique universel du Conseil des droits de l'homme des Nations unies, mais aussi le fonctionnement de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité), que des cas très concrets.

V.8. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

Dans le prolongement de la visite de travail organisée à Bruxelles (mai 2014) entre un représentant du Comité permanent R et de la *Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten* (CTIVD) des Pays-Bas, l'organe de contrôle néerlandais a organisé une deuxième concertation à la mi-novembre 2014. La réunion a été élargie à des représentants du *Strategic Intelligence Service Supervision* suisse. En octobre 2015, une nouvelle réunion entre organes de contrôle a eu lieu dans ce même cadre à Berne. Cette fois, des délégations suédoise *(Commission on Security and Integrity Protection)*, norvégienne *(Parliamentary Oversight Committee)* et danoise *(Intelligence Oversight Board)* y ont également participé. Cinq thèmes étaient à l'ordre du jour : (la mesure de) l'efficacité, l'accès pour les organes de contrôle à des informations des services de renseignement concernés, une vision sur les opérations en cours et l'échange d'informations entre les services de renseignement et entre les organes de contrôle, ainsi que le contrôle de l'utilisation des données à caractère personnel par les services de renseignement.

Lors de la réunion, il a été décidé d'initier une enquête de contrôle dans tous les pays participants sur la coopération internationale entre les différents services de renseignement en matière de lutte contre les *foreign terrorist fighters*. Par la suite, cette initiative a reçu le soutien explicite du président de la Commission de suivi. L'idée est que chaque organe de contrôle étudie cette thématique de son point de vue et en fonction de sa compétence, mais en s'appuyant sur une même philosophie et certainement une approche commune.

[129] Protocole de coopération du 13 janvier 2015 entre les institutions exerçant partiellement ou entièrement un mandat d'institution chargée du respect des droits de l'homme.

Par ailleurs, en 2015, le Comité permanent R a maintenu des contacts étroits avec la Commission nationale de contrôle des interceptions de sécurité (CNCIS) française et la nouvelle Commission nationale de contrôle des techniques de renseignement (CNCTR). Le président du Comité s'est aussi entretenu avec une délégation de la *Survey Delegation of the House of Councillors* japonaise, dans le cadre de sa '*fact-finding mission to learn about the protection of secrets and parliamentary involvement in these activities*'.

V.9. CONTRÔLE DES FONDS SPÉCIAUX

Au nom de la Chambre des Représentants, la Cour des comptes contrôle l'utilisation des moyens financiers par les services publics. La Cour des comptes est amenée à contrôler la légalité et la légitimité de toutes les dépenses, y compris, en principe, de toutes les dépenses des services de renseignement. Cependant, en raison du caractère sensible de la matière, une partie du budget de la VSSE et du SGRS (à savoir les « fonds spéciaux » avec des dépenses destinées, par exemple, aux opérations et aux informateurs) n'est pas examinée par la Cour des comptes. Pour la VSSE, le contrôle de ces dépenses est effectué par le directeur de la Cellule politique générale du ministre la Justice. Depuis 2006, c'est le chef des Forces armées qui exerce seul le contrôle des fonds spéciaux du SGRS, et ce à raison de quatre fois par an. À la suggestion de la Cour des comptes, ce contrôle se déroule, depuis 2010, en présence du président du Comité permanent R.

V.10. PRÉSENCE DANS LES MÉDIAS

Le Comité permanent R est régulièrement sollicité par la presse écrite et audiovisuelle pour expliquer ses activités ou celles des services de renseignement. Le Comité permanent R a accédé à ces demandes à plusieurs reprises.

Date	Sujet/titre	Forum
13 janvier 2015	'Nos services de renseignement et de sécurité sont-ils à la hauteur ?'	RTBF
18 janvier 2015	'Belgique : en guerre contre les terroristes ?'	RTBF (Mise au point)
18 janvier 2015	'Terreurdreiging : Comité I evalueert Belgisch veiligheidsapparaat'	MO*
18 janvier 2015	'Services de sécurité : un débat sur les mesures prioritaires au Parlement ?'	RTBF
25 janvier 2015	'Le mystère de la toute nouvelle académie pour les espions belges pour lutter contre les terroristes'	RTL

Date	Sujet/titre	Forum
11 mars 2015	'Staatsveiligheid heeft alleen nog tijd voor Syriëstrijders'	De Standaard
11 mars 2015	'Opvolging Syriëstrijders loopt gevaarlijk mank'	De Tijd
11 mars 2015	'Syriëcrisis verstikt Staatsveiligheid'	De Tijd
11 mars 2015	'La crise syrienne étouffe la Sûreté de l'État'	L'Écho
22 avril 2015	'Bescherming staatshoofden en vips in België is een knoeiboel'	Nieuwsblad
25 avril 2015	'Screenings voor kerncentrales en andere hotspots falen'	De Tijd
25 april 2015	'La surveillance des centrales nucléaires présente des failles'	L'Écho
28 avril 2015	'Proximus vraagt uitleg over 'mollen''	De Tijd
6 mai 2015	'Baas geheime dienst geeft foute info over drie aanslagen'	De Tijd
6 mai 2016	'De waarheid komt uitendelijk toch bovendrijven'	MO*
8 mai 2015	'Quand la France prend exemple sur la Belgique du renseignement'	L'Écho
28 mai 2015	'Les services secrets allemands auraient piraté des câbles de communication de Belgacom'	La Libre Belgique
2 juin 2015	'Comité I vraagt controle op lijsten met terrorismeverdachten'	De Tijd
2 juin 2015	'Staatsveiligheid richt blik op gevangenissen'	De Tijd
3 juillet 2015	'Militaire inlichtingendienst gaat datakabels bespioneren'	De Standaard
14 juillet 2015	'Antiterreurorgaan komt in vaarwater van andere inlichtingendiensten'	De Standaard
15 juillet 2015	'Activités de renseignements : l'OCAM sortirait de son rôle'	RTBF
15 juillet 2015	'Antiterreurorgaan OCAD ligt onder vuur wegens overschrijden bevoegdheid'	Knack
31 juillet 2015	'Staatsveiligheid past meer drastische middelen toe'	Het Laatste Nieuws
16 septembre 2015	'Besluit Comité I : 'België heeft niet voor NSA gespioneerd''	Het Laatste Nieuws
16 septembre 2015	'Nos agents n'ont pas épié pour la NSA'	Le Soir
30 septembre 2015	'André Vandoren stopt dit jaar als topman antiterreurdienst OCAD'	De Tijd
30 septembre 2015	'André Vandoren quitte l'OCAM'	Le Soir

Date	Sujet/titre	Forum
23 octobre 2015	'Guy Rapaille : 'Les services sont près d'un point de rupture''	Le Vif
26 octobre 2015	'Sûreté de l'État et Service Général de Renseignement et de Sécurité'	RTBF (Le Forum)
16 novembre 2015	'Drie personen gelinkt aan Parijse aanslagen stonden op lijst van Belgisch antiterreurorgaan'	MO*
17 novembre 2015	'Comité I start onderzoek inlichtingendiensten'	Het Laatste Nieuws
17 novembre 2015	'Nos services de renseignement pas la hauteur ?'	RTBF
17 novembre 2015	'Drie daders stonden op terreurlijst'	De Morgen
17 novembre 2015	'Ging Staatsveiligheid de mist in ?'	De Morgen
17 novembre 2015	'Le Président Guy Rapaille – Journal télévisé en rapport avec l'enquête Syrie'	RTBF
26 novembre 2015	'Tijdelijke commissie monopoliseert in Kamer volledig antiterreurbeleid'	De Standaard
26 novembre 2015	'Zo delen geheime diensten binnen de EU informatie met elkaar'	MO*
26 novembre 2015	'Militaire inlichtingendienst moet alerter zijn voor extremisme in leger'	De Standaard
27 novembre 2015	'La Belgique, miroir de l'Europe'	Le Vif
16 décembre 2015	'Staatsveiligheid en Nationale Bank onder vuur'	De Tijd
16 décembre 2015	'La Sûreté de l'État a désormais accès à nos comptes bancaires'	L'Écho

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.[130] Il s'agit de missions confiées au service d'Enquêtes R par les autorités judiciaires. 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 a élargi cette compétence aux crimes et délits commis par 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'Enquêtes R sont soumis à l'autorité du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a aucune autorité sur eux. Le président du Comité doit cependant veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle, et ce pour une raison évidente : l'organe de contrôle est avant tout à la disposition du Parlement. Cette mission pourrait être mise en péril si les dossiers judiciaires requéraient trop de temps. 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).

Quand le service d'Enquêtes R effectue des enquêtes pénales, le directeur doit remettre un rapport au Comité permanent R au terme de l'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).

---

130 Pour plus de détails, voir : P. NIVELLE, 'Een parlementair controleorgaan met een gerechtelijke opdracht… Over de tweede pet van de Dienst Enquêtes I', dans W. VAN LAETHEM et J. VANDERBORGHT, *Regards sur le contrôle. Vingt ans de contrôle sur les services de renseignement*, Intersentia, Anvers, 2013, 295-305.

En 2015 aussi, le service d'Enquêtes R a réalisé des devoirs d'enquête dans le cadre d'enquêtes judiciaires.

Le premier dossier concernait une enquête menée pour le compte des autorités judiciaires de Liège. Le service d'Enquêtes R a enquêté avec la Police judiciaire fédérale sur l'implication éventuelle d'un membre d'un service de renseignement dans une fraude fiscale et sociale.[131] En 2015, le service d'Enquêtes a participé à une série de perquisitions dans le cadre de cette enquête. Le dossier est toujours en cours.

La seconde enquête judiciaire concernait l'implication possible d'un membre d'un service de renseignement dans des crimes et délits contre la sûreté extérieure de l'État.[132] Ce dossier, ouvert en 2014, a été traité en 2015. Il a été classé sans suite à la fin de l'année.

Le service d'Enquêtes R n'a pas effectué de missions judiciaires dans le cadre d'autres dossiers initiés en 2014.[133]

131 Concernant cette même enquête judiciaire, voir COMITÉ PERMANENT R, *Rapport d'activités 2012*, 80.

132 Il s'agissait d'un dossier relatif à l'usage inapproprié de données classifiées et de données d'un service tiers.

133 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 102.

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. La fonction de greffe est exercée par le greffier du Comité permanent R et par son administration.

L'Organe de recours est compétent pour les contentieux portant sur des décisions dans quatre domaines : les habilitations de sécurité, les attestations de sécurité qui doivent permettre 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 imposent des avis ou des attestations de sécurité pour un secteur, un lieu ou un événement donné.[134]

Ces activités de l'Organe de recours ont un impact direct à la fois sur le budget et 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 son président et son greffier, mais aussi le personnel administratif requis. La préparation, le traitement et le suivi des recours constituent une lourde charge de travail.

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 des deux dernières années sont également repris.

En 2015, le nombre de recours et de décisions a diminué de manière significative par rapport à l'année précédente, passant respectivement de 171 à 130 et de 163 à 137. Cette tendance à la baisse est visible dans le nombre de recours introduits contre des avis de sécurité négatifs, et dans une moindre mesure, contre les refus d'attestations de sécurité relatives à un lieu ou un événement. Force est de constater, en revanche, que le nombre de refus d'octroi

134 Pour plus de détails, voir le *Rapport d'activités 2006* du Comité permanent R (87-115).

d'habilitations de sécurité contre lesquels un recours a été introduit a augmenté, alors qu'il avait encore diminué en 2014 par rapport à 2013. Enfin, il convient de noter que le nombre de recours contre des décisions prises en dehors des délais légaux en matière d'habilitations de sécurité a connu une forte diminution, passant de 15 en 2013 et 2014 à 2 en 2015.

Cependant, derrière ces chiffres en baisse, se cache une charge de travail croissante, tant pour le greffe que pour l'Organe de recours lui-même. En effet, les dossiers à gérer ne cessent de se complexifier en termes de gestion administrative, d'audiences et de décisions.

Ainsi, les dossiers administratifs qui sont transmis par les autorités de sécurité ne sont pas toujours complets, si bien que le greffe doit effectuer des démarches supplémentaires afin d'y remédier. Il en va de même pour l'application de l'article 5 § 3 L. Org.recours : la demande de soustraire certaines pièces à la consultation du requérant est rarement motivée ou émane de la mauvaise instance, ce qui oblige ici aussi le greffe à recueillir des informations complémentaires.

En outre, force est de constater que les audiences durent beaucoup plus longtemps qu'il y a quelques années. Les raisons sont de plusieurs ordres. De plus en plus de requérants se font assister par un avocat qui expose la position de leur client à l'audience. De surcroît, les services de police et de renseignement concernés demandent de plus en plus souvent à être entendus. La complexité de certains dossiers demande un investissement en temps important. Enfin, de nombreux dossiers – et c'est un phénomène nouveau – doivent être repris lors d'une deuxième ou d'une troisième audience, soit parce que le requérant demande un report, soit parce qu'il faut attendre un complément d'informations.

Le processus de décision même requiert lui aussi davantage de temps qu'il y a plusieurs années, et ce pour deux raisons majeures. D'une part, le nombre croissant de questions de procédure (p. ex. le débat sur la recevabilité, la question linguistique, les droits de la défense, l'obligation de motivation…). D'autre part, l'Organe de recours est plus souvent confronté à des dossiers hautement sensibles, qui sont liés à la problématique de la radicalisation et à la menace terroriste actuelle. De tels dossiers nécessitent évidemment un traitement extrêmement minutieux et une motivation adaptée. Du reste, des mesures de sécurité spécifiques doivent parfois être prises.

Tableau 1. Autorités de sécurité concernées

	2013	2014	2015
Autorité nationale de sécurité	98	99	68
Sûreté de l'État	1	0	1
Service général du renseignement et de la sécurité	78	60	47

	2013	2014	2015
Agence fédérale de Contrôle nucléaire	9	8	10
Police fédérale	1	3	3
Police locale	2	1	1
TOTAL	**189**	**171**	**130**

Tableau 2. Nature des décisions contestées

	2013	2014	2015
Habilitations de sécurité			
Confidentiel	5	5	9
Secret	56	43	35
Très secret	5	4	4
Total habilitations de sécurité	66	52	48
Refus	41	25	36
Retrait	5	9	7
Refus et retrait	4	–	–
Habilitation pour une durée limitée	1	2	3
Habilitation pour un niveau inférieur	0	1	0
Pas de décision dans les délais	15	15	2
Pas de décision dans les nouveaux délais	0	0	0
Total habilitations de sécurité	66	52	48
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	**66**	**52**	**48**
Attestations de sécurité documents classifiés			
Refus	0	4	6
Retrait	0	0	0
Pas de décision dans les délais	0	0	0
Attestations de sécurité lieu ou événement			
Refus	15	16	12
Retrait	0	0	1
Pas de décision dans le délai	0	0	0
Avis de sécurité			
Avis négatif	106	99	63
Pas d'avis	2	0	0

	2013	2014	2015
Révocation d'avis positif	0	0	0
Actes normatifs d'une autorité administrative	0	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	**123**	**119**	**82**
TOTAL DÉCISIONS CONTESTÉES	**189**	**171**	**130**

Tableau 3. Nature du requérant

	2013	2014	2015
Fonctionnaire	4	0	4
Militaire	26	17	29
Particulier	159	145	93
Personne morale	0	6	4

Tableau 4. Langue du requérant

	2013	2014	2015
Français	92	92	75
Néerlandais	97	76	54
Allemand	0	0	0
Autre langue	0	0	1

Tableau 5. Nature des décisions interlocutoires prises par l'Organe de recours[135]

	2013	2014	2015
Demande du dossier complet (1)	187	168	130
Demande d'informations complémentaires (2)	12	16	7

135 Le « nombre de décisions interlocutoires » (tableau 5), les « manières dont les requérants font usage de leurs droits de défense » (tableau 6), ou encore la « nature des décisions de l'Organe de recours » (tableau 7) ne correspondent pas nécessairement au nombre de requêtes introduites (voir tableaux 1 à 4). En effet, certains dossiers ont par exemple déjà été ouverts en 2015, alors que la décision n'a été rendue qu'en 2016.

	2013	2014	2015
Audition d'un membre d'une autorité (3)	3	11	7
Décision du président (4)	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (5)	68	78	50
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 de permettre au membre du service de renseignement de garder 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 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 ».

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

	2013	2014	2015
Consultation du dossier par le requérant /l'avocat	103	84	84
Audition du requérant /avocat[136]	138	115	107

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

	2013	2014	2015
Habilitations de sécurité			
Recours irrecevable	2	0	4
Recours sans objet	3	3	3
Recours non fondé	20	12	19

136 Dans le cadre de certains dossiers, le requérant/avocat est auditionné à plusieurs reprises.

	2013	2014	2015
Recours fondé (avec octroi partiel ou complet)	35	14	24
Devoir d'enquête complémentaire par l'autorité	0	0	0
Délai supplémentaire pour l'autorité	14	12	1
Sans suite	–	–	1
Attestations de sécurité documents classifiés			
Recours irrecevable	0	0	0
Recours sans objet	0	0	0
Recours non fondé	0	2	4
Recours fondé (avec octroi)	0	0	2
Attestations de sécurité pour lieux ou événements			
Recours irrecevable	1	0	0
Recours sans objet	0	0	0
Recours non fondé	6	6	8
Recours fondé (avec octroi)	11	8	10
Donne acte de retrait de recours	–	–	2
Avis de sécurité			
Organe de recours non compétent	0	4	0
Recours irrecevable	4	4	6
Recours sans objet	1	4	0
Confirmation de l'avis négatif	25	53	28
Transformation en avis positif	65	41	23
Recours contre des actes normatifs d'une autorité administrative	0	0	0
Donne acte de retrait de recours	–	–	2
TOTAL	**187**	**163**	**137**

CHAPITRE VIII
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

VIII.1. COMPOSITION DU COMITÉ PERMANENT R

La composition du Comité permanent R n'a subi aucune modification en 2015 : la présidence a été assurée par Guy Rapaille (F), avocat général près la cour d'appel de Liège, tandis que les fonctions de conseiller ont été remplies par Gérald Vande Walle (F) et Pieter-Alexander De Brock (N).

Le service d'Enquêtes R n'a lui non plus connu aucun changement. Ce service est composé de cinq commissaires auditeurs et est dirigé par Frank Franceus (N).

Le cadre du personnel administratif du Comité permanent R, placé sous la direction du greffier Wouter De Ridder (N), comptait toujours seize personnes.

VIII.2. RÉUNIONS AVEC LA COMMISSION DE SUIVI

Dans le courant de l'année 2015, six réunions ont eu lieu avec la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent des services de police et du Comité permanent des services de renseignement et de sécurité. Cette commission ne comptait encore que treize membres avec voix délibérative[137], qui ont été désignés comme suit [138] : Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Hendrik Vuye (N-VA), Laurette Onkelinx (PS), André

---

137 À ce propos, voir l'article 149, n°1 du Règlement de la Chambre des Représentants (*« Conformément aux articles 157 et 158, la Chambre désigne en son sein, au début de chaque législature, les membres effectifs de la commission chargée du suivi du Comité permanent P et du Comité permanent R, prévue par l'article 66bis de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'Organe de coordination pour l'analyse de la menace. Il est procédé à autant de nominations qu'il est nécessaire pour que chaque groupe politique compte au moins un membre au sein de la commission. L'article 22 n'est pas d'application »*).

138 En 2016, quatre changements sont intervenus dans la composition de la Commission : Peter De Roover (N-VA), Hans Bonte (sp.a), Gilles Vanden Burre (Ecolo-Groen) et Vanessa Matz (cdH) ont remplacé les Députés Hendrik Vuye, Karin Temmerman, Stefaan Van Hecke et Christian Brotcorne.

Frédéric (PS), Denis Ducarme (MR), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld), Karin Temmerman (sp.a), Stefaan Van Hecke (Ecolo-Groen) et Christian Brotcorne (cdH). Le président de la Chambre Siegfried Bracke (N-VA) assure la présidence des réunions de la Commission.

Lors de sa réunion plénière du 26 mars 2015, la Chambre a approuvé le « Règlement d'ordre intérieur de la Commission visée à l'article 66*bis*, § 1er, alinéa 1er, de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'organe de coordination pour l'analyse de la menace ».[139] Y figure, entre autres, le fait que les membres de la Commission « *prennent les mesures nécessaires afin de garantir le caractère confidentiel des faits, actes et renseignements dont ils ont connaissance en raison de leurs fonctions et sont soumis à une obligation de confidentialité.* » (art. 7).

Lors des réunions de la Commission, diverses enquêtes de contrôle, ainsi que le Rapport d'activités 2014 du Comité permanent R, ont été discutés à huis clos. La Commission a pris « *acte du rapport d'activités 2014 du Comité permanent R et [a] souscrit à ses recommandation* ».[140] En outre, une proposition de loi modifiant la Loi sur les services de renseignement et de sécurité concernant le contrôle des activités des services de renseignement étrangers a été inscrite à l'ordre du jour, et un échange de vues a eu lieu sur l'ouverture d'enquêtes de contrôle suite aux attentats de Paris en 2015.

VIII.3. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

Les articles 52 à 55 L.Contrôle déterminent les cas où le Comité permanent R et le Comité permanent P doivent organiser des réunions communes et la manière dont ils doivent les organiser. La présidence de ces réunions communes est exercée en alternance par les présidents des deux Comités permanents (art. 54 L.Contrôle). Ces réunions poursuivent un double objectif: d'une part, échanger des informations, et d'autre part, discuter des enquêtes de contrôle communes en cours, en l'occurrence les enquêtes portant sur la *Joint Information Box* (II.1), les membres du personnel de l'OCAM et les médias sociaux (II.6), les contacts internationaux de l'OCAM (II.7) ou encore la manière dont l'OCAM détermine le niveau de la menace (II.11.9) et la position d'information de l'OCAM avant les attentats perpétrés à Paris en novembre 2015.[141]

Sept réunions communes ont eu lieu en 2015.

---

139 www.lachambre.be/kvvcr/pdf_sections/publications/reglement/Contrôle des services de police et r – règlement d'ordre intérieur commission de suivi NTC.pdf.

140 *Doc. parl.* Chambre 2014-15, n°54-1340/1 (Rapport d'activités 2014 du Comité permanent R, Rapport fait au nom de la commission spéciale).

141 Cette enquête commune a été initiée en 2016.

VIII.4. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Le budget 2015 du Comité permanent R a été établi à 3,865 millions d'euros[142], soit une hausse de 3 % par rapport au budget 2014 et une dotation identique à celle qui avait été allouée en 2013. Outre les augmentations classiques des frais de fonctionnement, ce budget était également prévu pour absorber les coûts liés à la charge de travail croissante constatée précédemment. Une gestion rationnelle des fonds disponibles et le report du recrutement de deux membres du personnel supplémentaires[143], a généré un boni de 1,082 million d'euros.

Ce bilan positif cache cependant une tout autre réalité sur le plan financier. En effet, la Commission de la Comptabilité de la Chambre a reconfirmé le principe d'affecter *autant que possible* le boni d'un exercice comptable au financement de l'exercice budgétaire suivant, ce qui a pour effet de diminuer les montants octroyés par l'État au titre du financement de la dotation. Il est ressorti des comptes annuels 2014 et 2015 que ces moyens ne couvraient plus les dépenses réelles du Comité. En d'autres termes, cette différence entre les recettes, d'une part, et les dépenses, d'autre part, est compensée par le boni de l'exercice budgétaire précédent.

La décision du Conseil des ministres du 15 octobre 2014 de diminuer de 2 % annuellement, de façon linéaire, le budget des dotations, renforce cette spirale négative, à tel point le bon fonctionnement du Comité pourrait à terme en être affecté.

VIII.5. FORMATION

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

DATE	TITRE	ORGANISATION	LIEU
2014-2015	Hautes études de sécurité et de défense, une opportunité multisectorielle.	IRSD	Bruxelles
16 février 2015	Balancing Counter-Terrorism and Human Rights. Challenges and Opportunities	Global Network for Rights and Development (GNRD)	Genève

142 Loi du 19 décembre 2014 contenant le budget général des dépenses pour l'année budgétaire 2015, *M.B.* 29 décembre 2014.

143 En raison d'autres priorités, la procédure de recrutement n'a pu être lancée qu'en 2016.

DATE	TITRE	ORGANISATION	LIEU
13 mars 2015	Réunion avec M. André Vandoren	ECSA	Bruxelles
12 et 13 mars 2015	Surveillance, Privacy and Transnational Relations in the Digital Era	International Association of Constitutional Responses to Terrorism	Bruxelles
9 et 10 avril 2015	Conférence sur le contrôle démocratique des services de renseignement	DCAF/Institut de la Défense Nationale Tunisien	Tunis
13 avril 2015	Les services spéciaux dans le monde arabo-musulman	Métis	Paris
16 et 17 avril 2015	La réponse judiciaire au terrorisme en Europe	École Nationale de la Magistrature	Paris
28 et 29 mai 2015	Conference on the Democratic Oversight of Intelligence Services in the European Union	European Parliament, Committee on Civil Liberties, Justice and Home Affairs	Bruxelles
25 juin 2015	8ème Conférence de l'Association Francophone des Autorités de Protection des Données Personnelles	AFAPDP	Bruxelles
26 juin 2015	Organisation de la cyber défense face à la menace actuelle	Haut comité français pour la défense civile (HCFDC)	Bruxelles
29 juin 2015	Politie en inlichtingenactiviteiten tijdens de Groote Oorlog : parallellen naar vandaag	BISC	Leeuw-Saint-Pierre
21 septembre 2015	Le renseignement : planification, stratégie et prospective	Métis	Paris
24 septembre 2015	ICT-Security II	4Instance	Bruxelles
30 septembre 2015	L'intelligence stratégique au service du Plan Marshall 4.0 ?	HEC/ULG	Liège
5 octobre 2015	2015 ECSA Diplomatic Security Conference	ECSA	Bruxelles
17 octobre 2015	Quand l'invasion technologique menace nos libertés !	Université de Namur, Faculté de Droit	Namur
23 octobre 2015	Réunion avec M. Wil van Gemert, Vice-Directeur d'Europol	ECSA	Bruxelles
10 novembre 2015	185 ans de Sûreté de l'État, 100 ans de renseignement militaire, 70 ans du RUSRA, 5 ans du BISC : pasts and futures	BISC	Bruxelles

DATE	TITRE	ORGANISATION	LIEU
12 novembre 2015	Questions juridiques actuelles liées à la Défense	Die Keure opleidingscentrum	Bruxelles
13 novembre 2015	Digital Enlightenment Forum. Policy and Strategy Debate. Security, Surveillance and Civil Liberties in Cyber Space	TrustCore.EU	Bruxelles

CHAPITRE IX
RECOMMANDATIONS

À la lumière des enquêtes de contrôle clôturées en 2015, le Comité permanent R formule les recommandations reprises ci-après. 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. ENQUÊTES DE SÉCURITÉ ET MÉDIAS SOCIAUX

Le Comité recommande que des personnes qui font l'objet d'une enquête de sécurité soient expressément informées que la consultation de sources ouvertes – en ce compris les profils publics dans les médias sociaux – est une des méthodes de recueil d'informations qui peut être mise en œuvre dans ce cadre.[144]

IX.1.2. LA LUTTE CONTRE L'EXTRÉMISME AU SEIN DE L'ARMÉE *VERSUS* DROITS FONDAMENTAUX

Pour éviter tout jugement hâtif, le suivi de l'islamisme radical au sein de l'armée requiert un sens critique et une circonspection dans l'analyse des comportements des personnes. Le SGRS doit pouvoir distinguer les comportements relevant d'une pratique religieuse normale, conforme à la

144 À ce propos 'Chapitre II.5. Les membres du personnel des services de renseignement et les médias sociaux' et 'Chapitre II.6. Les membres du personnel de l'OCAM et les médias sociaux'.

liberté de culte reconnue à tout un chacun, d'autres attitudes révélatrices d'une dérive radicale et sectaire.[145]

IX.1.3. EXACTITUDE DES INFORMATIONS ET DROITS DES CITOYENS[146]

Le Comité permanent R recommande aux services, lorsqu'ils demandent des informations à des services étrangers ou lorsqu'ils placent des personnes sur des listes, d'accorder une attention particulière à l'exactitude de leurs renseignements et au bien-fondé juridique de la transmission d'informations, tant au niveau national qu'au niveau international, et ce en vue des conséquences éventuelles pour les intéressés.

Il convient par ailleurs de tenter, dans le futur, de trouver un équilibre entre, d'une part, les exigences collectives et multilatérales de sécurité, et d'autre part les droits des citoyens dont les noms figurent sur ce genre de listes. Cela pourrait se traduire par la conclusion d'accords multilatéraux, sur, par exemple, la création d'une fonction de médiation ou un contrôle externe sur ces bases de données. En effet, actuellement, les instances nationales telles que le Comité permanent R n'ont pas compétence pour contrôler le bien-fondé et la légitimité de telles listes et de leur contenu.

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 LA *JOINT INFORMATION BOX*[147]

Les Comités R et P ont formulé diverses recommandations en vue d'un réexamen approfondi de la *Joint Information Box* (JIB), c'est-à-dire de la liste gérée par l'OCAM reprenant les noms des personnes et des organisations qui jouent un rôle clé dans le processus de radicalisation :

– il convient de clarifier le rôle de chaque service participant. Il en va de même pour l'OCAM, qui en tant que service d'analyse, peut démontrer sa plus-value à l'égard des informations fournies par les services d'appui. L'OCAM

145 Cette recommandation découle de l'enquête de contrôle sur la détection et le suivi des éléments extrémistes au sein du personnel de la Défense (Chapitre II.3).

146 Voir 'Chapitre II.8. 'Suivi à tort par les services de renseignement ?'.

147 Voir 'Chapitre II.1. Enquête de contrôle commune sur la *Joint Information Box* de l'OCAM'.

remplissait de manière trop minimaliste son rôle d'organe d'analyse de la menace dans le cadre de la liste JIB. L'OCAM doit jouer un rôle plus actif dans la coordination de l'analyse. Le service peut évaluer la menace spécifique qui émane de chaque entité en matière de radicalisation ;
- d'autre part, il semble indiqué qu'un autre service (par exemple, la Direction générale du centre de crise) soit désigné pour veiller à la coordination de l'exécution des mesures ;
- l'utilisation de paramètres garantit que la mention dans la liste JIB n'est pas arbitraire. Un système de critères est effectivement requis pour préserver l'objectivité ;
- les Comités permanents R et P soulignent la nécessité de reprendre dans la JIB les informations émanant de services sur le terrain. Les niveaux locaux doivent être en mesure d'introduire leurs constatations dans le système et de recevoir au moins un feedback de la décision de mentionner ou non une entité dans la liste et des mesures à prendre. Il s'avère en effet que les premiers signes de radicalisation sont souvent constatés au niveau local (par exemple, par l'agent de quartier ou l'antenne locale des services de renseignement). Les Comités jugent indispensable un examen approfondi de la manière de mettre en place le flux d'informations le plus adéquat possible, et ce dans le respect des structures existantes ;
- les informations et les analyses doivent être diffusées le plus rapidement et le plus largement possible aux acteurs concernés, et ce en tenant compte évidemment d'une classification éventuelle et du *need to know*. Le cas échéant, certaines personnes (par exemple du niveau régional ou local) doivent disposer d'une habilitation de sécurité ;
- étant donné la diversité et la spécificité des mesures qui doivent ou peuvent être prises à l'égard des vecteurs de radicalisation[148], il convient de confier à des instances ou à des groupes mieux placés, le soin de proposer, d'imposer et de suivre des mesures. L'idée est que les acteurs de la JIB puissent se concentrer sur leur tâche principale, qui est de fournir et d'analyser des renseignements. Le cas échéant, des services autres que les services de sécurité fédéraux doivent être impliqués dans le débat. Et pour cause, la détection, la neutralisation ou la limitation de l'effet « radicalisant » d'une personne ou d'un groupement ne concerne pas que le niveau fédéral.

Les Comités R et P soutiennent tout projet visant à permettre à la JIB de devenir à court terme l'outil par excellence pour identifier et maîtriser autant que possible les vecteurs de toutes les formes de radicalisation dans la société belge. De plus, les Comités ont fait savoir qu'ils vérifieraient ultérieurement la révision annoncée du processus de travail de la JIB.

148 Sont visées les personnes qui ont un effet « radicalisant » sur des tiers.

IX.2.2. RECOMMANDATIONS RELATIVES À LA GESTION ET AU CONTRÔLE DES « FONDS SPECIAUX »[149]

IX.2.2.1. Un cadre juridique

Il convient de procéder à la rédaction d'une disposition légale ou réglementaire définissant de manière claire et précise la gestion des fonds spéciaux. En outre, il est indispensable que les deux services de renseignement soient soumis à des contrôles de même nature, tant internes qu'externes. Cette disposition réglementaire devra notamment déterminer selon quelles procédures les surplus annuels éventuels pourront être conservés par les services concernés. Il y a lieu, par ailleurs, d'impliquer suffisamment les services dans le cycle budgétaire.

IX.2.2.2. Recommandations spécifiques en ce qui concerne les fonds spéciaux et le SGRS

- les montants alloués au SGRS pour ses crédits ordinaires (qui regroupent les frais de personnel, de fonctionnement et d'investissement), ainsi que le montant annuel des fonds spéciaux, doivent pouvoir être identifiables dans la loi budgétaire de la Défense votée chaque année par le Parlement ;
- le SGRS doit repenser l'agencement des sous-caisses, et ce en vertu du principe de finalité de certaines caisses (par exemple, l'autonomie opérationnelle de certaines sections). Dans les autres cas, le Comité estime qu'une centralisation de la gestion des fonds est plus opportune ;
- le SGRS doit établir un cadre normatif et uniforme pour les caisses (« nouvelle formule »). Il s'agit plus précisément de formaliser les procédures de dépenses, afin que le contrôle de la hiérarchie soit efficace et offre une valeur ajoutée. Il convient également d'utiliser la comptabilité de ces fonds comme outil de gestion, en ayant recours à un système informatique uniforme et fiable ;
- en ce qui concerne les dépenses pour lesquelles les critères de « discrétion » et d'« extrême urgence » ne sont pas d'application, le SGRS doit rechercher des modes de financement classiques, en partenariat avec d'autres services de la Défense. Des moyens supplémentaires seront ainsi libérés pour faire face aux dépenses opérationnelles.

Le Comité a attiré l'attention sur le fait qu'une modification de la réglementation ne pouvait en aucun cas mettre en péril les missions du SGRS. Il a souligné que ces fonds sont absolument nécessaires au fonctionnement du SGRS. Les recommandations du Comité ne peuvent avoir pour effet de priver ce service de l'utilisation d'une partie des fonds. Selon le Comité, l'optimalisation de la gestion des fonds du SGRS doit se faire en concertation avec le service. De plus, le

149 Voir 'Chapitre II.2. La gestion, l'utilisation et le contrôle des « fonds spéciaux »'.

Comité a établi que le SGRS doit, d'une part, rechercher un financement alternatif, en partenariat avec d'autres services de la Défense et, d'autre part, sur la base des fonds actuellement disponibles, s'efforcer d'intégrer l'utilisation de ces fonds à sa stratégie de sécurité.

IX.2.2.3. Recommandations spécifiques en ce qui concerne les fonds spéciaux et la VSSE

- la VSSE doit valoriser davantage l'exercice de la fonction de comptable extraordinaire, en rédigeant une description de fonction précise, en formant son personnel à cette fonction et en assurant des formations continues dans ce domaine ;
- la VSSE doit veiller à assurer la continuité de la fonction de comptable extraordinaire, ce qui nécessite, entre autres, la désignation d'un suppléant à la fonction de comptable extraordinaire[150] et la rédaction des procédures de fonctionnement.

IX.2.2.4. Sessions d'information régulières

Le Comité insiste pour que des séances d'information relatives aux modalités d'utilisation des fonds soient régulièrement dispensées à l'ensemble du personnel, tant du SGRS que de la VSSE.

IX.2.3. L'UTILISATION DES MÉDIAS SOCIAUX PAR LES MEMBRES DU PERSONNEL DE LA VSSE ET DU SGRS[151]

Le Comité permanent R recommande que la direction des services de renseignement prenne des initiatives en vue de rendre le cadre normatif (lois, Arrêtés royaux, directives internes, code de déontologie), qui est applicable aux membres des services de renseignement, plus explicite quant à l'attitude générale de loyauté et de prudence attendue de ceux-ci, en particulier sur les réseaux sociaux et quant aux moyens de contrôle susceptibles d'être mis en œuvre à cet effet.

Le Comité avait déjà recommandé[152] 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

150 La désignation, dans l'intervalle, d'un suppléant à la fonction de comptable extraordinaire a rendu cette recommandation obsolète.

151 À ce propos 'Chapitre II.5. Les membres du personnel des services de renseignement et les médias sociaux'.

152 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 113 ('IX.2.8. Un code de déontologie pour les agents de la VSSE').

Sûreté de l'État, ce service élabore un(e) (proposition de) code de déontologie et le soumette à l'approbation du ministre de la Justice. Le Comité recommandait que ce code décrive en quoi consiste le devoir de neutralité et de discrétion des agents de la VSSE. En outre, le Comité demandait 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. Le Comité permanent R réitère cette recommandation, étant d'avis qu'un tel code de déontologie devrait aborder la conduite à tenir par les agents des services de renseignement, aussi bien de la VSSE que du SGRS, dans l'utilisation des médias sociaux.[153]

Le Comité recommande également à la direction des services la prise de dispositions particulières indiquant de quelle manière proactive peuvent être contrôlés l'utilisation des TIC et le comportement des agents sur les SRS, que ce soit à des fins professionnelles ou privées. Ces dispositions devront naturellement tenir compte des principes de finalité, de proportionnalité et de transparence, mais ici aussi, être adaptées à la mission particulière des services.

En outre, une procédure doit être mise en place pour pouvoir, en cas d'incident, évaluer les éventuels dommages pour l'intéressé et, pour le service, réagir de manière appropriée et prendre les mesures correctrices afin d'éviter une répétition d'un tel incident.

Sans préjudice du retrait éventuel de l'habilitation de sécurité, les autorités hiérarchiques doivent envisager l'application de sanctions disciplinaires éventuelles en cas de violation avérée des règles de sécurité et du devoir de discrétion.

Enfin, les services doivent alerter préventivement leurs agents des risques associés à leur présence sur les réseaux sociaux, et pouvoir fixer des recommandations générales ainsi que des mesures de sécurité déterminant les précautions à prendre et les comportements à éviter sur ces réseaux.

IX.2.4. L'UTILISATION DES MÉDIAS SOCIAUX PAR LES MEMBRES DU PERSONNEL DE L'OCAM[154]

En ce qui concerne l'utilisation des services de réseautage social par les membres du personnel de l'OCAM, les Comités R et P formulent les recommandations suivantes :

– il faut poursuivre les efforts que la direction de l'OCAM a déjà entrepris pour appréhender les risques de sécurité suscités par la présence de membres de

153 Le Comité estime à cet égard que les conseils et les consignes contenus dans les chartes d'utilisation des réseaux sociaux telles que proposées par la Police fédérale, le *Belgian Cyber Security Guide* ou les autorités militaires françaises et américaines, peuvent utilement inspirer l'élaboration de ce code de déontologie, tout en prenant en considération les missions particulières dont les membres des services de renseignement sont investis et des conditions de confidentialité et de secret dans lesquelles ceux-ci doivent opérer.

154 À ce propos 'Chapitre II.6. Les membres du personnel de l'OCAM et les médias sociaux'.

son personnel sur les SRS (plus précisément dans le cadre du comité de pilotage) ;
- des initiatives doivent être prises en vue de rendre le cadre normatif de l'OCAM (lois, Arrêtés royaux, directives internes, code de déontologie) plus explicite quant à l'attitude générale de loyauté et de prudence attendue de ses agents sur les réseaux sociaux et quant aux moyens de contrôle susceptibles d'être mis en œuvre à cet effet ;
- l'Autorité nationale de sécurité (ANS) doit avertir explicitement toute personne faisant l'objet d'une enquête de sécurité que la consultation des sources ouvertes, incluant celle des profils publics des médias sociaux, constitue l'une des méthodes de recueil d'information utilisable à cette fin ;
- des règles de « bon usage » destinées aux membres du personnel utilisant ces nouveaux moyens de communication doivent être élaborées ;
- dans le cadre des règles existantes[155], des moyens de recherches ciblés doivent être mis en place afin de vérifier la bonne application de ces règles – toujours susceptibles d'être adaptées à l'évolution des moyens de communication – aussi bien de manière préventive, par sondage, que réactive en cas d'incidents ou d'indices de dysfonctionnement liés à des comportements à risque de membres du personnel sur les médias sociaux ;
- le personnel de l'OCAM doit être informé que l'utilisation des TIC et le comportement des agents sur les sites de réseautage social peuvent être contrôlés de manière proactive. Ces dispositions devront naturellement tenir compte des principes de finalité, de proportionnalité et de transparence, mais ici aussi, être adaptées à la mission particulière des services ;
- une procédure d'évaluation des dommages et de réaction doit être mise en place pour pouvoir pallier et/ou gérer une divulgation intempestive d'informations préjudiciables à l'agent, et par extension à son service. S'inspirant de la méthodologie OPSEC[156], cette procédure devrait également prévoir les mesures correctrices à prendre pour éviter la répétition d'un tel incident et en limiter les conséquences ;
- en cas de violation avérée des règles de sécurité et du devoir de discrétion, les agents de l'OCAM doivent être clairement informés que les mesures suivantes peuvent être prises :

---

155 Plus précisément la CCT n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau (les e-mails, l'usage d'internet, intranet, extranet, les SMS, le chat, les forums de discussion…).

156 OPSEC ou 'Operations Security' est défini comme suit: *'a process that involves the identification and protection of generally unclassified critical information or processes that can be used by a competitor or adversary to gain real information when pieced together. Although the information sought under OPSEC isn't classified, it could give a competitor or other adversary advantage. OPSEC focuses on the identification and protection of information that could give enemies clues or capabilities to put one in a disadvantage'*, dans www.techopedia.com.

a) le retrait éventuel de l'habilitation de sécurité ;
b) l'engagement de poursuites disciplinaires conformément au régime disciplinaire des analystes de l'OCAM ;
c) la fin du détachement de l'agent concerné, et son renvoi à l'autorité du corps d'origine s'il s'agit d'un agent détaché ;

– il convient d'apprécier l'application des principes et des mesures précités aux membres du personnel de l'OCAM, en tenant compte des missions particulières dont ces derniers sont investis dans la communauté du renseignement et des conditions de confidentialité et de secret dans lesquelles ceux-ci doivent opérer.

IX.2.5. LES CONTACTS INTERNATIONAUX DE L'OCAM[157]

En tenant compte des responsabilités politiques et administratives respectives de chaque instance concernée par l'établissement de relations internationales, les Comités permanents R et P formulent les recommandations suivantes :

– les contacts établis par l'OCAM avec des services étrangers homologues (ou non) doivent être transparents et traçables à l'égard des ministres compétents (Intérieur, Justice et Défense nationale), du SPF Affaires étrangères et des services belges de police et de renseignement ;
– le Conseil national de sécurité doit prendre une directive pour assurer les relations internationales spécifiques de l'OCAM avec des services étrangers ou internationaux homologues, et ce conformément à l'article 8, 3° L.OCAM.[158] À cet égard, il paraît nécessaire que la directive précise quels peuvent être les services partenaires stratégiques de l'OCAM, quels types de collaboration peuvent être établis avec ces services et comment déterminer leur caractère « homologue » ou non.[159]

À l'estime des Comités permanents R et P, cette directive devrait à tout le moins contenir les prescriptions suivantes :

– que l'OCAM tienne à jour la liste des services étrangers avec lesquels il entretient ou souhaite entretenir des relations internationales ; que cette liste soit soumise au Conseil national de sécurité et publiée dans les rapports semestriels de l'OCAM ;

---

157 À ce propos : 'Chapitre II.7. Les contacts internationaux de l'OCAM'.

158 L'OCAM et la VSSE ont déjà passé des accords en vue de résoudre des problèmes causés par certains contacts internationaux de l'OCAM. Les Comités estimaient cependant qu'une solution structurelle imposait l'élaboration d'une directive par le Conseil national de sécurité en la matière.

159 La recommandation est entre-temps dépassée, en ce sens que le Conseil national de sécurité a édicté une telle directive courant 2016. Mais la prise en considération par la directive de toutes les prescriptions formulées ci-dessous n'a pas encore été vérifiée.

- qu'à cette fin, les services d'appui et les clients concernés de l'OCAM soient avertis et consultés préalablement à l'établissement de toute relation avec un service étranger, homologue ou non, notamment la VSSE, le SGRS, la Police fédérale, mais aussi le SPF Affaires étrangères. En effet, de telles relations et coopérations, pouvant engager la responsabilité politique du gouvernement et/ou la réputation du pays dans la communauté internationale, nécessitent une évaluation et une couverture politiques. En d'autres termes, les ministres compétents doivent être suffisamment informés, de telle sorte qu'il leur soit toujours possible d'assumer leur responsabilité politique[160];
- que les contacts éventuels que l'OCAM souhaiterait établir avec certains services de renseignement étrangers s'établissent dorénavant par le canal de la VSSE ou du SGRS;
- que les contacts éventuels que l'OCAM souhaiterait établir avec certains services de police étrangers s'établissent dorénavant par le canal du Commissariat général, Direction des relations internationales (CGI) de la Police fédérale;
- que les experts détachés de ces services de police ou de renseignement auprès de l'OCAM soient impliqués dans ces relations;
- que tout établissement d'une relation bilatérale avec un service étranger fasse l'objet d'une analyse préalable de type *Strength, Weaknesses, Opportunities and Threats* (SWOT);
- que chaque collaboration ainsi établie avec un service étranger fasse l'objet d'une évaluation périodique sur la base des critères SWOT;
- qu'à tout le moins, chaque mission effectuée par un membre de l'OCAM à l'étranger fasse l'objet d'un rapport écrit et détaillé sur les contacts établis et sur leur nature; que ces rapports soient communiqués aux services de police ou de renseignement concernés;
- que toute communication d'information à un service tiers soit notée dans un registre ad hoc;
- qu'un relevé des relations internationales établies par l'OCAM et des participations effectuées par des membres de son personnel à des événements à l'étranger soit consigné dans chaque rapport bisannuel que doit établir ce service en application de l'article 10 § 4 L. OCAM;
- que l'OCAM élabore une directive interne visant à déterminer les règles pratiques et de sécurité à suivre lors de déplacements à l'étranger de membres de sa direction et/ou de son personnel dans leur activité professionnelle;
- que l'OCAM utilise les connexions internationales sécurisées des services de renseignement pour correspondre avec des services étrangers;
- que l'OCAM lui-même n'envoie ni ne diffuse plus aucun rapport à des ambassades étrangères.

---

160 Voir également en ce sens une recommandation antérieure: COMITÉ PERMANENT R, *Rapport d'activités 2014*, 117 ('IX.1.3. La nécessité d'une couverture politique des accords de coopération').

D'autre part, les Comités ont jugé souhaitable que tant la VSSE que le SGRS invitent l'OCAM à des concertations avec des services de renseignement étrangers, certainement lorsque celles-ci traitent d'informations relatives à des menaces qui relèvent de la compétence de l'OCAM. En outre, l'OCAM pourrait profiter de l'occasion pour tester des hypothèses, recevoir des informations de première main… Les services concernés pourraient ainsi renforcer leurs liens de confiance réciproque en vue d'une meilleure coopération.

Ces recommandations des Comités R et P sont dans le droit fil de la position commune exprimée à l'époque[161] :

- l'OCAM n'est pas un service de renseignement ;
- il ne lui appartient pas de collecter du renseignement, ni en Belgique, ni à l'étranger, fût-ce pour combler lui-même ce qu'il considèrerait comme des lacunes de la part des services de renseignement ou des services d'appui ;
- il importe que cet organe veille à ne pas entretenir la moindre ambiguïté sur sa mission légale tant dans sa communication que dans ses relations avec d'autres services belges ou étrangers.

IX.2.6. LA LUTTE CONTRE L'EXTRÉMISME AU SEIN DE L'ARMÉE[162]

Le SGRS doit être particulièrement attentif à tout signe de conversion à l'islamisme radical, tant au sein du personnel civil que du personnel militaire de la Défense. Une même vigilance est de mise pour les tendances d'extrême droite et les bandes criminelles de motards, parfois considérées comme moins problématiques dans les unités.

Le Comité recommande donc que le commandement du SGRS donne à ses sections compétentes des instructions claires en ce sens, en leur donnant pour tâche d'identifier des indicateurs non équivoques de radicalisation, ceci en vue de constituer une documentation relative à cette problématique.

Pour ce faire, le SGRS doit veiller à optimaliser tous ses canaux d'informations utiles. Une grande attention doit ainsi être accordée à la qualité des contacts établis avec les différentes unités et d'autres services de la Défense. Les responsables et les chefs de corps d'unités devraient dès lors être sensibilisés à la problématique, notamment par l'organisation régulière de briefings d'information.

Enfin, il est recommandé d'évaluer les canaux et les procédures de communication, tant avec les autorités disciplinaires au sein de la Défense

---

161 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 33-34 ('II.5. Une visite de travail prévue à l'étranger par l'OCAM').

162 Ces recommandations découlent de l'enquête de contrôle sur la détection et le suivi des éléments extrémistes au sein du personnel de la Défense (Chapitre II.3).

qu'avec les services de police et les autorités judiciaires. Le SGRS doit pouvoir être informé en temps utile de toute mesure administrative, sanction ou condamnation prononcée à l'égard d'un membre du personnel de la Défense. Ce type de communication doit être plus systématique pour permettre l'examen ultérieur de mesures à prendre, notamment en matière d'habilitations de sécurité. Si des défaillances devaient être constatées dans les flux d'informations, elles devraient être signalées au ministre afin qu'il puisse y remédier.

IX.2.7. LA RÉVISION DU RÈGLEMENT DE SÉCURITÉ DU SGRS[163]

Le Comité recommande que le SGRS rassemble toutes les dispositions relatives à la sécurité militaire (y compris les directives INFOSEC) dans un document unique (IF5). En 2015, le SGRS a affirmé avoir commencé à y travailler.

IX.2.8. UN RAPPORT CIRCONSTANCIÉ EN CAS D'INCIDENT DE SÉCURITÉ[164]

Le SGRS doit établir un rapport circonstancié pour chaque incident de sécurité, examinant et analysant toutes ses dimensions (techniques *et* comportementales), surtout lorsqu'une des personnes concernées est titulaire d'une habilitation de sécurité. Ce rapport doit être transmis à l'autorité de sécurité compétente.

IX.2.9. LA FINALISATION DU RÈGLEMENT DE TRAVAIL[165]

Le Comité permanent R recommande que la VSSE ne tarde pas à finaliser et à valider son règlement de travail. Ce document devra couvrir au minimum les aspects de durée de travail, de congés de maladie ainsi que les aspects de prévention. Dans le cadre de la prévention, il est recommandé à la VSSE de se doter rapidement d'une structure ad hoc afin d'honorer ses obligations légales. La VSSE devra notamment désigner un conseiller en prévention et créer un réseau de personnes de confiance.

---

163 Voir 'Chapitre II.9. Plainte relative à la transmission d'informations à caractère personnel à un tiers par un agent de renseignement'.

164 Voir 'Chapitre II.9. Plainte relative à la transmission d'informations à caractère personnel à un tiers par un agent de renseignement'.

165 À ce propos : 'Chapitre II.10. La VSSE et l'application de la réglementation sur les congés de maladie'.

IX.2.10. LA TRANSMISSION DE TOUTES LES INFORMATIONS PERTINENTES À L'OCAM[166]

Le Comité permanent R recommande que les services de renseignement transmettent systématiquement à l'OCAM toutes les informations pertinentes ainsi que les résultats d'enquêtes menées dans le cadre de dossiers en cours, et ce même si les résultats ne sont pas probants.

IX.3. RECOMMANDATION RELATIVE À L'EFFICACITÉ DU CONTRÔLE

IX.3.1. LES CONTACTS INTERNATIONAUX DE L'OCAM

Les Comités permanents R et P ont insisté pour que les contacts internationaux établis par l'OCAM avec des services étrangers homologues (ou non) soient transparents pour les deux organes de contrôle et puissent être tracés. En outre, les Comités recommandent que certains éléments de ces contacts soient repris dans les rapports d'activité que l'OCAM doit transmettre aux deux Comités via le Conseil national de sécurité (art. 10, § 4, L.OCAM).

166 Voir 'Chapitre II.8. Suivi à tort par les services de renseignement ?'.

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 2015 AU 31 DÉCEMBRE 2015)

Loi 10 avril 2014 modifiant la 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, *M.B.* 11 février 2015

Loi 20 juillet 2015 contenant le premier ajustement du budget général des dépenses pour l'année budgétaire 2015, *M.B.* 30 juillet 2015

Loi 10 août 2015 modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers en vue d'une meilleure prise en compte des menaces contre la société et la sécurité nationale dans les demandes de protection internationale, *M.B.* 24 août 2015

Loi 10 août 2015 modifiant la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *M.B.* 28 août 2015

Loi 3 septembre 2015 portant assentiment à l'Accord entre les États membres de l'Union européenne, réunis au sein du Conseil, relatif à la protection des informations classifiées échangées dans l'intérêt de l'Union européenne, fait à Bruxelles le 25 mai 2011, *M.B.* 30 novembre 2015, *M.B.* 30 novembre 2015

Loi 14 décembre 2015 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 en ce qui concerne le mandat des membres suppléants du Comité permanent de contrôle des services de police et du Comité permanent de contrôle des services de renseignements, *M.B.* 24 décembre 2015

Extrait de l'arrêt n° 84/2015 du 11 juin 2015, numéros du rôle 5856 et 5859. En cause : les recours en annulation partielle (article 5) ou totale de la loi du 30 juillet 2013 'portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle', introduits respectivement par l'Ordre des barreaux francophones et germanophones et par l'ASBL 'Liga voor Mensenrechten' et l'ASBL 'Ligue des Droits de l'Homme, *M.B.* 11 août 2015

A.R. 19 décembre 2014 portant répartition partielle du crédit provisionnel inscrit au programme 14-53-5 du budget général des dépenses pour l'année budgétaire 2014 et destiné à la compensation salariale et au remboursement aux départements d'origine des indemnités et des coûts afférents au déploiement et au fonctionnement de membres de la Police fédérale, de représentants de la Magistrature et de membres du personnel de la Justice, des Affaires étrangères, des Finances, de l'Intérieur, de l'Organe de Coordination pour l'Analyse de la Menace, de la Défense et d'autres instances publiques chargés de missions à l'étranger, *M.B.* 7 janvier 2015

A.R. 28 janvier 2015 portant création du Conseil national de sécurité, *M.B.* 30 janvier 2015

A.R. 2 juin 2015 portant création du Comité stratégique et du Comité de coordination du renseignement et de la sécurité, *M.B.* 5 juin 2015

A.R. 23 août 2015 portant composition 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, *M.B.* 31 août 2015

A.R. 8 septembre 2015 modifiant divers arrêtés royaux en ce qui concerne la dénomination 'Conseil national de sécurité', *M.B.* 17 septembre 2015

A.R. 27 septembre 2015 modifiant l'arrêté royal du 23 janvier 2007 relatif au personnel de l'Organe de coordination pour l'analyse de la menace, *M.B.* 2 octobre 2015

A.R. 27 septembre 2015 modifiant l'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, *M.B.* 2 octobre 2015

A.R. 2 octobre 2015 portant répartition partielle du crédit provisionnel inscrit au programme 03-41-1 du budget général des dépenses pour l'année budgétaire 2015 et destiné à couvrir des dépenses non structurelles concernant la sécurité, *M.B.* 8 octobre 2015

A.R. 30 octobre 2015 relatif à l'accès direct du Comité permanent de contrôle des services de renseignement et de sécurité et de son Service d'enquêtes aux données et informations de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police, *M.B.* 20 novembre 2015

A.R. 9 décembre 2015 relatif aux tâches spécifiques des membres du collège des procureurs généraux, *M.B.* 28 décembre 2015

A.M. 1er avril 2015 concernant l'exécution d'une vérification de sécurité auprès des membres du personnel de l'entreprise publique autonome Belgocontrol et des tiers, *M.B.* 15 avril 2015

A.M. 29 juin 2015 modifiant l'arrêté ministériel du 5 décembre 2006 portant désignation d'un comité de sélection chargé de l'évaluation des candidatures pour la cellule d'appui de la Sûreté de l'État, *M.B.* 8 juillet 2015

Recrutement – résultat – sélection comparative d'un analyste, néerlandophone. Le nombre de lauréats s'élève à 20, *M.B.* 27 mars 2015

Appel aux candidats 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, *M.B.* 7 avril 2015

Sélection comparative de *Cyber Risk Prevention Specialist* (m/f) (niveau B) francophone pour le Ministère de la Défense, *M.B.* 1er juin 2015

Sélection comparative de *Cyber Risk Prevention Specialisten* (m/f) (niveau B) néerlandophones pour le Ministère de la Défense, *M.B.* 1er juin 2015

Sélection comparative de *Cyber Risk Prevention Experts* (m/f) (niveau A2) francophones pour le Ministère de la Défense, *M.B.* 1er juin 2015

Sélection comparative de *Cyber Risk Prevention Expert* (m/f) (niveau A2) néerlandophone pour le Ministère de la Défense, *M.B.* 1er juin 2015

Sélection comparative de *Cyber Security Experts* (m/f) (niveau A2) francophones pour le Ministère de la Défense, *M.B.* 1er juin 2015

Sélection comparative de *Cyber Security Expert* (m/f) (niveau A2) néerlandophone pour le Ministère de la Défense, *M.B.* 1er juin 2015

Sélection comparative de *Cyber Security Specialist* (m/f) (niveau B) francophone pour le Ministère de la Défense, *M.B.* 1er juin 2015

Sélection comparative de *Cyber Security Specialisten* (m/f) (niveau B) néerlandophones pour le Ministère de la Défense, *M.B.* 1er juin 2015

Appel aux candidats 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, *M.B.* 5 juin 2015

Sélection comparative de Cyber Risk Prevention Specialist, (m/f) (niveau B), néerlandophones, pour le Ministère de la Défense clôturée le 29 septembre 2015, *M.B.* 12 octobre 2015

Sélection comparative de Cyber Security Specialist, (m/f) (niveau B), néerlandophones, pour le Ministère de la Défense clôturée le 29 septembre 2015, *M.B.* 12 octobre 2015

Par arrêté royal du 29 octobre 2015, à la demande de M. Vandoren A., il est mis fin à sa désignation en qualité de directeur de l'Organe de coordination pour l'analyse de la menace, avec entrée en vigueur le 31 décembre 2015 au soir. *M.B.* 6 novembre 2015

Emploi vacant de directeur de l'Organe de coordination pour l'analyse de la menace (Loi du 10 juillet 2006, *M.B.* 20 juillet 2006) – appel aux candidats, *M.B.* 19 novembre 2015

Sélection comparative de gestionnaires de bases de données (m/f) (niveau B), francophones, pour la Sûreté de l'État, *M.B.* 24 novembre 2015

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 2015 AU 31 DÉCEMBRE 2015)

Sénat

Communication du Premier ministre, *Ann. Parl.*, Sénat, 2014-2015, nº 6-8, p. 10

Relevé des lois qui ont posé des difficultés d'application ou d'interprétation pour les cours et tribunaux – RAPPORT 2013-2014, *Doc. parl.*, Sénat, 2014-2015, nº 6-39/2

Chambre des Représentants

Exposé d'orientation politique – Défense et Fonction publique, *Doc. parl.*, Chambre, 2014-2015, nº 54-20/24

Relevé des lois qui ont posé des difficultés d'application ou d'interprétation pour les cours et tribunaux – RAPPORT 2013-2014, *Doc. parl.*, Chambre, 2014-2015, nº 54-435/2

Proposition de loi modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique, *Doc. parl.*, Chambre, 2014-2015, nº 54-553/2

Proposition de loi relative aux traitements automatisés de données à caractère personnel nécessaires aux passeports et titres de voyage belges, *Doc. parl.*, Chambre, 2014-2015, nºs 54-731/2 à 54-731/4

Règlement d'ordre intérieur de la commission visée à l'article 66*bis*, alinéa 1er, de la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignements et de l'organe de coordination pour l'analyse de la menace, *Doc. parl.*, Chambre, 2014-2015, nºs 54-859/1 et 54-859/2

Proposition de résolution visant à organiser une enquête concernant la possibilité d'interdire le financement des mosquées et des instituts islamiques au moyen de fonds internationaux provenant des milieux fondamentalistes musulmans, *Doc. parl.*, Chambre, 2014-2015, nº 54-868/1

Proposition de résolution relative à l'avenir de l'armée belge, *Doc. parl.*, Chambre, 2014-2015, nº 54-908/1

Proposition de résolution relative à la politique européenne de lutte contre le radicalisme et le terrorisme, *Doc. parl.*, Chambre, 2014-2015, nº 54-915/1

Proposition de loi modifiant la loi du 2 juin 1998 portant création d'un Centre d'Information et d'Avis sur les organisations sectaires nuisibles et d'une Cellule administrative de Coordination de la lutte contre les organisations sectaires nuisibles, afin d'étendre son champ d'application aux sectes thérapeutiques, *Doc. parl.*, Chambre, 2014-2015, nº 54-0968/1

Auditions – La Défense belge dans le futur, *Doc. parl.*, Chambre, 2014-2015, nº 54-0975/1

Proposition de résolution relative à l'avenir de la Défense, *Doc. parl.*, Chambre, 2014-2015, nºs 54-988/1, 54-988/2, 54-988/6 en 54-988/7 en *C.R.I.*, Chambre, 2014-2015, 2 avril 2015, PLEN 037, p. 43

Proposition de modification du Règlement de la Chambre des Représentants, visant à garantir le contrôle effectif du commerce des armes au sein de la commission spéciale des achats militaires, *Doc. parl.*, Chambre, 2014-2015, nº 54-0994/1

Le Conseil européen des chefs d'État ou de gouvernement du 12 février 2015 (débriefing), *Doc. parl.*, Chambre, 2014-2015, nº 54-0995/1

Discussion du Plan Justice, *Doc. parl.*, Chambre, 2014-2015, nº 54-1019/1

Commentaires et observations sur les projets d'ajustement du budget de l'État pour l'année budgétaire 2015, *Doc. parl.*, Chambre, 2014-2015, nº 54-1026/2

Projet de loi contenant le premier ajustement du Budget général des dépenses pour l'année budgétaire 2015, *Doc. parl.*, Chambre, 2014-2015, nº 54-1027/1

Projet de loi modifiant la loi du 1er août 1979 concernant les services dans une armée ou une troupe étrangère se trouvant sur le territoire d'un État étranger, *Doc. parl.*, Chambre, 2014-2015, nº 54-1078/1

État des lieux de la sécurité des centrales nucléaires belges, *Doc. parl.*, Chambre, 2014-2015, nº 54-1105/1

Demandes d'urgence de la part du gouvernement : 1. Projet de loi modifiant la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (1187/1) 2. Projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers en vue d'une meilleure prise en compte des menaces contre la société et la sécurité nationale dans les demandes de protection internationale (1197/1) 3. Projet de loi visant à renforcer la lutte contre le terrorisme (1198/1) 4. Projet de loi portant modification de la loi du 16 janvier 2013 portant diverses mesures relatives à la lutte contre la piraterie maritime (1199/1), *C.R.I.*, Chambre, 2015-2016, 1er juillet 2015, PLEN 059, p. 3

Projet de loi portant modification du Code consulaire (1200/1-3) – Projet de loi modifiant la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques (1170/1-6) – Proposition de loi relative au retrait de la carte d'identité, du passeport et des documents de voyage des mineurs qui souhaitent partir combattre à l'étranger (768/1) – Proposition de loi relative au retrait des documents d'identité et des documents de voyage des personnes qui souhaitent partir combattre à l'étranger et y commettre des actes terroristes (797/1) – Projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers en vue d'une meilleure prise en compte des menaces contre la société et la sécurité nationale dans les demandes de protection internationale (1197/1-4) – Projet de loi visant à renforcer la lutte contre le terrorisme (1198/1-4) – Proposition de loi visant à priver les djihadistes de la nationalité belge ainsi que de tout avantage social (658/1) – Proposition de loi prévoyant des sanctions et la déchéance de la nationalité belge pour les Belges qui adhèrent de leur plein gré à certains groupements, associations ou entités djihadistes ou accomplissent des missions pour ceux-ci (781/1) – Proposition de loi modifiant la loi du 1er août 1979 concernant les services dans une armée ou une troupe étrangère se trouvant sur le territoire d'un État étranger, en vue d'interdire le départ de combattants en Syrie ou en Irak (795/1) – Proposition de loi modifiant le Code de la nationalité belge afin d'étendre les possibilités de déchéance de la nationalité (796/1) – Proposition de loi modifiant la loi du 1er août 1979 concernant les services dans une armée ou une troupe étrangère se trouvant sur le territoire d'un État étranger (1078/1), Discussion générale, *C.R.I.*, Chambre, 2015-2016, 15 juillet 2015, PLEN 063, p. 14

Projet de loi modifiant la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes d'étranger et aux documents de séjour et modifiant la loi du 8 août 1983 organisant un Registre national des personnes physiques, *Doc. parl.*, Chambre, 2014-2015, nº 54-1170/7

Projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers en vue d'une meilleure prise en compte des menaces contre la société et la sécurité nationale dans les demandes de protection internationale, *Doc. parl.*, Chambre, 2014-2015, nº 54-1197/5

Projet de loi visant à renforcer la lutte contre le terrorisme (1198/4), *C.R.I.*, Chambre, 2015-2016, 16 juillet 2015, PLEN 065, p. 34

Projet de loi portant modification du Code consulaire, *Doc. parl.*, Chambre, 2014-2015, nº 54-1200/2

Échange de vues avec le ministre des Finances sur le Plan de politique de l'Administration générale des Douanes et Accises, *Doc. parl.*, Chambre, 2014-2015, nº 54-1212/1

Proposition de résolution relative à l'avenir de la Défense belge, *Doc. parl.*, Chambre, 2014-2015, nº 54-1261/1

Projet de loi portant des dispositions diverses Intérieur, *Doc. parl.*, Chambre, 2014-2015, nº 54-1298/1

Projet de loi portant assentiment à l'Accord entre le Royaume de Belgique et le Grand-Duché de Luxembourg concernant l'échange et la protection réciproque des informations classifiées, fait à Luxembourg le 9 février 2012, *Doc. parl.*, Chambre, 2014-2015, nos 54-1299/1 et 54-1299/2

Audition de M. Wim De Clercq, Chief Nuclear Officer d'Electrabel, concernant l'analyse des incidents récents à la centrale de Tihange et le plan d'action en vue d'améliorer la culture de la sécurité dans les centrales, *C.R.I.*, Chambre, 2014-2015, 21 septembre 2015, COM 231, p. 1

Projet de loi modifiant diverses lois en ce qui concerne la dénomination « Conseil national de sécurité », *Doc. parl.*, Chambre, 2014-2015, nos 54-1330/1 à 54-1330/4

Rapport d'activités 2014 du Comité permanent de contrôle des services de renseignement et de sécurité, *Doc. parl.*, Chambre, 2014-2015, nº 54-1340/1

Projet du Budget général des dépenses pour l'année budgétaire 2016, *Doc. parl.*, Chambre, 2015-2016, nº 54-1352/1

Justification du budget général des dépenses pour l'année budgétaire 2016, *Doc. parl.*, Chambre, 2015-2016, nos 54-1353/2, 54-1353/7 et 54-1353/8

Projet de loi modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice, *Doc. parl.*, Chambre, 2015-2016, nos 54-1418/1, 54-1418/2 et 54-1418/4

Note de politique générale – partie Fraude Fiscale du ministre des Finances, *Doc. parl.*, Chambre, 2015-2016, nos 54-1428/2, 54-1428/4, 54-1428/13, 54-1428/19 et 54-1428/22

Communication du gouvernement sur les attentats terroristes, *C.R.I.*, Chambre, 2015-2016, 19 novembre 2015, PLEN 081, p. 2

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 en ce qui concerne le mandat des membres suppléants du Comité permanent de contrôle des services de police et du Comité permanent de contrôle des services de renseignements, *Doc. parl.*, Chambre, 2015-2016, nos 54-1446/1 à 54-1446/4

Cour des comptes, Cour constitutionnelle, Conseil supérieur de la Justice, Comités permanents de contrôle des services de police et de renseignements, Médiateurs fédéraux, Commission pour la protection de la vie privée, Commissions de nomination pour le notariat, Commission BIM et Organe de contrôle de l'information policière – comptes de l'année budgétaire 2014 – ajustements du budget 2015 – propositions budgétaires pour l'année 2016, *Doc. parl.*, Chambre, 2015-2016, nos 54-1497/1 et 54-1497/2

Projet du Budget Général des Dépenses pour l'année budgétaire 2016- Avis sur la section 16 – ministère de la Défense, *Doc. parl.*, Chambre, 2015-2016, nº 54-1352/27

Projet du Budget Général des Dépenses pour l'année budgétaire 2016- Avis sur la section 12 – SPF Justice, *Doc. parl.*, Chambre, 2015-2016, nº 54-1352/37

Comptes de l'année budgétaire 2014 du Comité permanent de contrôle des services de renseignements et de sécurité (1497/1), *C.R.I.*, Chambre, 2015-2016, 17 décembre 2015, PLEN 090, p. 78

Comptes de l'année budgétaire 2014 de la Commission BIM (1497/1), *C.R.I.*, Chambre, 2015-2016, 17 décembre 2015, PLEN 090, p. 80

Propositions budgétaires pour l'année 2016 du Comité permanent de contrôle des services de renseignements et de sécurité (1497/1), *C.R.I.*, Chambre, 2015-2016, 17 décembre 2015, PLEN 090, p. 84

Propositions budgétaires pour l'année 2016 de la Commission BIM (1497/1), *C.R.I.*, Chambre, 2015-2016, 17 décembre 2015, PLEN 090, p. 85

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 2015 AU 31 DÉCEMBRE 2015)

Sénat

Question écrite de J.-J. De Gucht au ministre de l'Intérieur sur le 'wahabisme – écoles radicales – Sûreté de l'État – Défense – collaboration avec les Communautés' (Sénat, 2014-2015, 21 janvier 2015, Q. nº 6-404)

Question écrite de J.-J. De Gucht au ministre de la Justice sur les 'données à caractère personnel traitées par les services de renseignement – loi relative aux archives – délai de conservation' (Sénat, 2014-2015, 13 février 2015, Q. nº 6-441)

Question écrite de Ch. Defraigne au ministre de l'Intérieur sur les 'services de police – zones rurales et grandes villes – OCAM – mesure de sécurité – budget et difficultés opérationnelles' (Sénat, 2014-2015, 17 février 2015, Q. nº 6-451)

Chambre des Représentants

Question de S. Smeyers au secrétaire d'État à l'Asile et la Migration sur 'la réinstallation de réfugiés syriens' (*C.R.I.*, Chambre, 2014-2015, 7 janvier 2015, COM 45, p. 7, Q. nº 776)

Question de J. Fernandez Fernandez au ministre de la Défense sur 'les potentielles missions de police de l'armée' (*C.R.I.*, Chambre, 2014-2015, 7 janvier 2015, COM 46, p. 4, Q. nº 673)

Question de F. Demon au ministre de l'Intérieur sur 'le fonctionnement de la task force locale sur la radicalisation' (*C.R.I.*, Chambre, 2014-2015, 7 janvier 2015, COM 50, p. 38, Q. nº 566)

Question de J.M. Nollet au ministre de l'Intérieur sur 'le redémarrage de Doel 4' (*C.R.I.*, Chambre, 2014-2015, 7 janvier 2015, COM 50, p. 49, Q. nº 629)

Question de J.-M. Nollet au ministre de l'Intérieur sur 'le survol du site de Doel par un drone' (*C.R.I.*, Chambre, 2014-2015, 7 janvier 2015, COM 50, p. 64, Q. nº 1045)

Questions jointes de P. Dewael, V. Matz, L. Onkelinx, K. Temmerman, S. Verherstraeten, H. Vuye, D. Ducarme, M. Almaci, R. Hedebouw, J.-M. Nollet, F. Dewinter, K. Metsu et O. Maingain au premier ministre sur 'l'attaque terroriste au siège de Charlie Hebdo' (*C.R.I.*, Chambre, 2014-2015, 8 janvier 2015, PLEN 26, p. 4, Q. nºs 160 à 172)

Questions jointes de G. Dallemagne et P. Buysrogge au premier ministre sur 'la stratégie belge de cybersécurité' (*C.R.I.*, Chambre, 2014-2015, 13 janvier 2015, COM 51, p. 6, Q. nºs 984 et 1093)

Question de V. Yüksel au ministre de l'Intérieur sur 'le déploiement de l'armée en cas de niveau de la menace 3' (*C.R.I.*, Chambre, 2014-2015, 13 janvier 2015, COM 53, p. 46, Q. nº 1255)

Question de H. Bonte au ministre de l'Intérieur sur 'l'attentat tragique contre la rédaction de Charlie Hebdo et les leçons à en tirer pour la politique de sécurité belge' (*C.R.I.*, Chambre, 2014-2015, 13 janvier 2015, COM 53, p. 48, Q. nº 1256)

Question de S. Smeyers au secrétaire d'État à la Lutte contre la fraude sociale, sur 'le screening des travailleurs dans les entreprises en matière de terrorisme' (*C.R.I.*, Chambre, 2014-2015, 14 janvier 2015, COM 55, p. 15, Q. nº 1340)

Question de R. Bellens au ministre de la Justice sur 'l'échange par la Turquie de combattants de l'EI et d'otages turcs et ses conséquences sur la sécurité nationale' (*C.R.I.*, Chambre, 2014-2015, 14 janvier 2015, COM 55, p. 19, Q. nº 1075)

Questions jointes de H. Bonte, K. Metsu, V. Yüksel, F. Dewinter, S. Smeyers, L. Onkelinx et S. De Wit au ministre de la Justice sur 'la lutte contre le radicalisme dans les prisons' (*C.R.I.*, Chambre, 2014-2015, 14 janvier 2015, COM 55, p. 35, Q. nºs 1278, 1282, 1311, 1333, 1339, 1348 et 1356)

Question de L. Onkelinx au ministre de la Justice sur 'les budgets de la Sûreté de l'État et la lutte contre l'intégrisme et le terrorisme' (*C.R.I.*, Chambre, 2014-2015, 14 janvier 2015, COM 55, p. 48, Q. nº 1347)

Questions jointes de F. Dewinter, H. Bonte, V. Matz, M. Van Hees, B. Hellings et F. Demon au premier ministre sur 'la politique et les mesures concrètes pour lutter contre le terrorisme et le radicalisme' (*C.R.I.*, Chambre, 2014-2015, 15 janvier 2015, PLEN 27, p. 22, Q. nºs 187 à 192)

Question de S. Smeyers au secrétaire d'État à l'Asile sur la 'régularisation médicale' (*Q.R.*, Chambre, 2014-2015, 19 janvier 2015, nº 8, p. 223, Q. nº 21)

Questions jointes de K. Temmerman et S. Crusnière au ministre du Budget sur 'l'utilisation de la provision interdépartementale dans le cadre de la lutte contre le radicalisme et le terrorisme' (*C.R.I.*, Chambre, 2014-2015, 21 janvier 2015, COM 60, p. 18, Q. nºs 1365 et 1403)

Échange de vues et questions jointes d'A. Top, G. Dallemagne, C. Van Cauter, S. De Wit, K. Degroote, J. Fernandez Fernandez, W. Demeyer, F. Demon, M. Wathelet, V. Matz, K. Metsu, P. Buysrogge, W. De Vriendt, S. Van Hecke, O. Maingain, L. Onkelink, V. Yüksel et Ch. Brotcorne au ministre de l'Intérieur sur 'la lutte contre le terrorisme et le radicalisme' (*C.R.I.*, Chambre, 2014-2015, 21 janvier 2015, COM 66, p. 1, Q. nºs 1321, 1364, 1379, 1382, 1447, 1449, 1451, 1452, 1456, 1460, 1461, 1467, 1474, 1475, 1484, 1508, 1513, 1514, 1522, 1523, 1528, 1529, 1530, 1537, 1541 et 1552)

Question de K. Lalieux au ministre de la Justice sur 'les mesures de sécurité au Palais de Justice de Bruxelles' (*C.R.I.*, Chambre, 2014-2015, 28 janvier 2015, COM 70, p. 13, Q. nº 1747)

Question de S. Van Hecke au ministre de la Justice sur 'la déclassification des archives de la Sûreté de l'État' (*C.R.I.*, Chambre, 2014-2015, 28 janvier 2015, COM 70, p. 16, Q. nº 1594)

Question de S. Van Hecke au ministre de la Justice sur 'les 23 analystes supplémentaires à la Sûreté de l'État et le complément des cadres existants' (*C.R.I.*, Chambre, 2014-2015, 28 janvier 2015, COM 70, p. 22, Q. nº 1739)

Question de K. Temmerman au ministre de l'Intérieur sur 'l'octroi de titres de séjour aux imams par la Sûreté de l'État' (*C.R.I.*, Chambre, 2014-2015, 28 janvier 2015, COM 73, p. 19, Q. nº 1535)

Questions jointes de H. Bonte et K. Degroote au premier ministre sur 'la nécessité d'une coordination et d'une collaboration dans la lutte contre le terrorisme et le radicalisme' (*C.R.I.*, Chambre, 2014-2015, 29 janvier 2015, PLEN 29, p. 11, Q. nºs 226 et 227)

Question de S. Van Hecke au premier ministre sur 'les conséquences politiques du piratage dont Belgacom a été victime' (*C.R.I.*, Chambre, 2014-2015, 3 février 2015, COM 77, p. 1, Q. nº 865)

Question de K. Temmerman au ministre de la Justice sur 'l'octroi de titres de séjour aux imams par la Sûreté de l'État' (*C.R.I.*, Chambre, 2014-2015, 4 février 2015, COM 81, p. 3, Q. nº 1840)

Questions jointes de R. Deseyn et G. Dallemagne au Premier ministre sur 'la cybersécurité' (*C.R.I.*, Chambre, 2014-2015, 5 février 2015, PLEN 30, p. 7, Q. nºs 243 et 244)

Question de F. Dewinter au ministre de l'Intérieur sur 'les activités réduites de la police locale en raison du déploiement de ces policiers dans le cadre de la lutte contre le terrorisme ' (*C.R.I.*, Chambre, 2014-2015, 5 février 2015, PLEN 30, p. 23, Q. nº 251)

Question de K. Jadin au ministre de l'Intérieur sur 'le soutien au 'Daech' sur les réseaux sociaux en Belgique' (*Q.R.*, Chambre, 2014-2015, 9 février 2015, nº 011, p. 47, Q. nº 136)

Question de M. Wathelet au ministre de l'Énergie sur 'la protection physique des installations nucléaires et des infrastructures critiques' (*C.R.I.*, Chambre, 2014-2015, 10 février 2015, COM 84, p. 39, Q. nº 1600)

Questions jointes de J. Fernandez Fernandez et S. Pirlot au ministre de la Défense sur 'le budget du SGRS' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 87, p. 31, Q. nºs 1232 et 1833)

Question de M. Wathelet au ministre de l'Intérieur sur 'la protection physique des installations nucléaires et des infrastructures critiques' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 88, p. 1, Q. nº 1601)

Question de V. Matz au ministre de l'Intérieur sur 'les mesures mises en place par l'autorité fédérale pour soutenir les autorités locales dans la lutte contre le radicalisme' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 88, p. 13, Q. nº 1789)

Question de B. Pas au ministre de l'Intérieur sur 'les mesures prises pour protéger la chaîne de télévision kurde ROJ TV' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 88, p. 18, Q. nº 1801)

Question de F. Demon au ministre de l'Intérieur sur 'l'analyse de risques menée par l'OCAM concernant certains événements' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 88, p. 39, Q. nº 1974)

Question de P.-O. Delannois au ministre de l'Intérieur sur 'la réaction sur la fermeture du festival Ramdam' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 88, p. 41, Q. nº 2008)

Question d'E. Kir au ministre de l'Intérieur sur 'le contrôle des imams venus de l'étranger' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 88, p. 59, Q. nº 2108)

Questions jointes de W. Demeyer et N. Ben Hamou au ministre de l'Intérieur sur 'la police de proximité et le niveau 3 de la menace' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 88, p. 61, Q. nºs 2120 et 2187)

Question Ph. Pivin au ministre de l'Intérieur sur 'les impacts sur les zones de police du niveau d'alerte 3' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 88, p. 68, Q. nº 2201)

Question de N. Lanjri au secrétaire d'État sur 'la fraude sociale éventuellement commise par de jeunes Belges partis combattre en Syrie' (*C.R.I.*, Chambre, 2014-2015, 11 février 2015, COM 91, p. 14, Q. nº 84)

Question de H. Bonte au ministre de l'Intérieur sur 'la circulaire du 25 septembre 2014 relative à la gestion de l'information et aux mesures de suivi concernant les 'foreign fighters' qui séjournent en Belgique' (*Q.R.*, Chambre, 2014-2015, 16 février 2015, nº 012, p. 139, Q. nº 127)

Question de P. Buysrogge au Premier ministre sur 'la coopération avec Google et d'autres entreprises internationales actives dans le domaine de l'internet en vue de lutter contre la radicalisation' (*C.R.I.*, Chambre, 2014-2015, 24 février 2015, COM 95, p. 8, Q. nº 1645)

Question de A. Top au ministre de la Défense sur 'le système BINII' (*C.R.I.*, Chambre, 2014-2015, 25 février 2015, COM 96, p. 3, Q. nº 1493)

Question de S. Pirlot au ministre de la Défense sur 'la Belgian Intelligence Academy' (*C.R.I.*, Chambre, 2014-2015, 25 février 2015, COM 96, p. 27, Q. nº 1782)

Question de E. Willaert au secrétaire d'État à la Lutte contre la fraude sociale sur 'le secret professionnel des assistants sociaux' (*C.R.I.*, Chambre, 2014-2015, 25 février 2015, COM 97, p. 14, Q. nº 2240)

Question de L. Onkelinx au ministre de la Justice sur 'le contrôle des imams étrangers' (*C.R.I.*, Chambre, 2014-2015, 25 février 2015, COM 97, p. 16, Q. nº 2099)

Question de S. Lahaye-Battheu au ministre de la Justice sur 'l'avenir du tribunal de Furnes' (*C.R.I.*, Chambre, 2014-2015, 25 février 2015, COM 97, p. 25, Q. nº 2342)

Question de S. Van Hecke au ministre de la Justice sur 'la coopération entre la NSA et les services de renseignements belges' (*C.R.I.*, Chambre, 2014-2015, 25 février 2015, COM 97, p. 43, Q. nº 2256)

Questions jointes de P. Vanvelthoven et W. Demeyer au ministre de l'Intérieur sur 'la protection des membres du gouvernement en vacances' (*C.R.I.*, Chambre, 2014-2015, 25 février 2015, COM 100, p. 49, Q. nº 2295 et 2487)

Questions jointes de P. Dewael et W. Demeyer au ministre de l'Intérieur sur 'les conséquences du maintien du niveau 3 de la menace' (*C.R.I.*, Chambre, 2014-2015, 26 février 2015, PLEN 32, p. 18, Q. nºs 297 et 298)

Question de N. Lijnen au ministre de la Défense sur 'les administrations et services – cyberattaques' (*Q.R.*, Chambre, 2014-2015, 2 mars 2015, n° 014, p. 252, Q. n° 123)

Question de K. Grosemans au ministre de la Défense sur 'l'attrition des candidats militaires' (*Q.R.*, Chambre, 2014-2015, 2 mars 2015, n° 014, p. 258, Q. n° 124)

Question de S. Van Hecke au ministre de la Défense sur 'la mise en œuvre de méthodes MRD à l'étranger' (*Q.R.*, Chambre, 2014-2015, 2 mars 2015, n° 014, p. 262, Q. n° 127)

Question de Ö. Özen au ministre de la Justice sur 'la liste de potentiels combattants djihadistes' (*C.R.I.*, Chambre, 2014-2015, 3 mars 2015, COM 103 p. 21, Q. n° 2602)

Question de Ph. Goffin au ministre de la Justice sur 'les possibilités de collaboration entre la Sûreté de l'État et le Terrorist Screening Center' (*C.R.I.*, Chambre, 2014-2015, 3 mars 2015, COM 103 p. 35, Q. n° 2520)

Question de S. Van Hecke au ministre de la Justice sur 'le piratage de données chez un fabricant de puces électroniques pour cartes SIM et cartes bancaires' (*C.R.I.*, Chambre, 2014-2015, 3 mars 2015, COM 103 p. 34, Q. n° 2612)

Question de R. Hufkens au ministre de l'Intérieur sur 'les jeunes de retour du front syrien' (*Q.R.*, Chambre, 2014-2015, 9 mars 2015, n° 015, p. 68, Q. n° 68)

Question de K. Gabriëls au ministre de la Défense sur le 'SGRS – atteintes à « l'intégrité physique » du personnel civil et des analystes' (*Q.R.*, Chambre, 2014-2015, 9 mars 2015, n° 015, p. 206, Q. n° 131)

Question de R. Hedebouw au ministre de la Défense sur le 'déploiement de l'armée' (*Q.R.*, Chambre, 2014-2015, 9 mars 2015, n° 015, p. 210, Q. n° 134)

Question de J. Fernandez Fernandez au ministre de la Défense sur 'l'évaluation de la présence de « militaires de rue »' (*Q.R.*, Chambre, 2014-2015, 9 mars 2015, n° 015, p. 218, Q. n° 138)

Question de D. Ducarme au secrétaire d'État à l'Asile et la Migration sur 'le contrôle des imams radicaux' (*Q.R.*, Chambre, 2014-2015, 9 mars 2015, n° 015, p. 236, Q. n° 63)

Questions jointes de V. Yüksel, S. Pirlot et G. Dallemagne au ministre de la Défense sur 'la présence de djihadistes au sein de l'armée' (*C.R.I.*, Chambre, 2014-2015, 10 mars 2015, COM 108, p. 35, Q. n^{os} 2383, 2467 et 2856)

Question de V. Yüksel au ministre de la Défense sur le 'vol de matériel appartenant à la Défense à Landen' (*Q.R.*, Chambre, 2014-2015, 16 mars 2015, n° 016, p. 251, Q. n° 149)

Question de M. De Coninck au secrétaire d'État à l'Asile et la Migration sur 'la procédure d'obtention d'un permis de séjour pour les imams' (*Q.R.*, Chambre, 2014-2015, 16 mars 2015, n° 016, p. 255, Q. n° 68)

Question de E. Kir au secrétaire d'État à l'Asile et la Migration sur 'la visite de la délégation belge dans un camp de réfugiés syriens' (*C.R.I.*, Chambre, 2014-2015, 18 mars 2015, COM 118, p. 34, Q. n° 2825)

Questions jointes de A. Top, P. Buysrogge et J. Fernandez Fernandez au ministre de la Défense sur 'la cyberdéfense' (*C.R.I.*, Chambre, 2014-2015, 18 mars 2015, COM 119, p. 10, Q. n^{os} 2722, 2731 et 2867)

Questions jointes de S. Pirlot, A. Top et V. Yüksel au ministre de la Défense sur 'la diminution du niveau de la menace le lundi 9 mars 2015' (*C.R.I.*, Chambre, 2014-2015, 18 mars 2015, COM 119, p. 17, Q. n^{os} 2945, 3083 et 3090)

Question de N. Ben Hamou au ministre de l'Intérieur sur 'l'organisation des missions de police en période de niveau d'alerte augmenté' (*C.R.I.*, Chambre, 2014-2015, 18 mars 2015, COM 124, p. 3, Q. n° 2647)

Question de K. Timmerman au ministre de l'Intérieur sur 'la transparence de notre politique de sécurité' (*C.R.I.*, Chambre, 2014-2015, 18 mars 2015, COM 124, p. 38, Q. nº 2764)

Questions jointes de E. Thiébaut et F. Demon au ministre de l'Intérieur sur 'la diminution du niveau de la menace' (*C.R.I.*, Chambre, 2014-2015, 18 mars 2015, COM 124, p. 46, Q. nºs 2895 et 2982)

Question de J.-M. Nollet au ministre de l'Intérieur sur 'la concertation entre l'AFCN et l'OCAM dans le cadre des survols de nos centrales nucléaires' (*Q.R.*, Chambre, 2014-2015, 23 mars 2015, nº 017, p. 113, Q. nº 93)

Question de K. Jadin au ministre de l'Intérieur sur 'l'élargissement des tâches militaires' (*Q.R.*, Chambre, 2014-2015, 23 mars 2015, nº 017, p. 117, Q. nº 131)

Question de S. De Wit au ministre de la Justice sur 'la volonté de créer dans les prisons des sections distinctes pour les détenus radicalisés' (*C.R.I.*, Chambre, 2014-2015, 25 mars 2015, COM 127, p. 20, Q. nº 3100)

Question de E. Thiébaut au premier ministre sur 'le Centre pour la Cybersécurité Belgique' (*C.R.I.*, Chambre, 2014-2015, 25 mars 2015, COM 130, p. 1, Q. nº 2481)

Question de K. Metsu au ministre de l'Intérieur sur 'le piratage de sites internet par l'EI' (*C.R.I.*, Chambre, 2014-2015, 1er avril 2015, COM 141, p. 1, Q. nº 2868)

Question de V. Yüksel au ministre de l'Intérieur sur 'un schéma pour le niveau de menace et les mesures à prendre' (*C.R.I.*, Chambre, 2014-2015, 1er avril 2015, COM 141, p. 24, Q. nº 3052)

Question de V. Matz au ministre de l'Intérieur sur 'la lutte contre la criminalité économique et financière' (*C.R.I.*, Chambre, 2014-2015, 1er avril 2015, COM 141, p. 43, Q. nº 3199)

Question de Ph. Pivin au ministre de l'Intérieur sur 'les possibles faits de radicalisme dans des entreprises publiques belges' (*C.R.I.*, Chambre, 2014-2015, 1er avril 2015, COM 141, p. 74, Q. nº 3447)

Question de W. De Vriendt au ministre des Affaires étrangères sur 'le déménagement aux Archives de l'État des archives africaines du SPF Affaires étrangères' (*Q.R.*, Chambre, 2014-2015, 7 avril 2015, nº 019, p. 153, Q. nº 120)

Question de Ph. Goffin au ministre de l'Intérieur sur 'l'estimation de la présence de djihadistes belges en Syrie et en Irak' (*Q.R.*, Chambre, 2014-2015, 13 avril 2015, nº 020, p. 29, Q. nº 196)

Question de R. Hedebouw au ministre de l'Intérieur sur 'le contrôle parlementaire de la politique antiterroriste et des services de renseignement' (*Q.R.*, Chambre, 2014-2015, 13 avril 2015, nº 020, p. 31, Q. nº 200)

Question de M. Van Hees au ministre de l'Intérieur sur 'la participation à des conflits étrangers' (*Q.R.*, Chambre, 2014-2015, 13 avril 2015, nº 020, p. 38, Q. nº 207)

Question de F. Demon au ministre de l'Intérieur sur les 'cortèges carnavalesques – sécurité' (*Q.R.*, Chambre, 2014-2015, 13 avril 2015, nº 020, p. 41, Q. nº 212)

Question de P. Luykx au ministre des Affaires étrangères sur 'la lutte contre la menace terroriste en collaboration avec les pays musulmans' (*Q.R.*, Chambre, 2014-2015, 20 avril 2015, nº 021, p. 134, Q. nº 55)

Questions jointes de P. Buysrogge et C. Cassart-Mailleur au ministre de la Défense sur 'l'utilisation de simulations informatiques et de réalité virtuelle à la Défense' (*C.R.I.*, Chambre, 2014-2015, 22 avril 2015, COM 143, p. 23, Q. nºs 3443 et 3791)

Questions jointes de S. Pirlot et G. Dallemagne au ministre de la Défense sur 'les compétences du SGRS en matière de protection du potentiel scientifique et économique' (*C.R.I.*, Chambre, 2014-2015, 22 avril 2015, COM 143, p. 48, Q. nos 3792 et 3819)

Question de K. Temmerman au ministre de l'Intérieur sur 'le renouvellement des badges des travailleurs à l'aéroport de Zaventem' (*C.R.I.*, Chambre, 2014-2015, 22 avril 2015, COM 145, p. 15, Q. no 3440)

Question de V. Matz au ministre de l'Intérieur sur 'la mise en œuvre par le gouvernement de ses 12 mesures relatives à la lutte contre le radicalisme' (*C.R.I.*, Chambre, 2014-2015, 22 avril 2015, COM 146, p. 13, Q. no 3504)

Question de G. Foret au ministre de l'Intérieur sur 'le recours aux techniques de 'predictive profiling' par les forces de l'ordre dans leurs mission de sécurité' (C.R.I., Chambre, 2014-2015, 22 avril 2015, COM 146, p. 35, Q. no 3621)

Question de F. Demon au ministre de l'Intérieur sur 'la Sûreté de l'État et la police fédérale' (*C.R.I.*, Chambre, 2014-2015, 23 avril 2015, PLEN 042, p. 23, Q. no 435)

Questions jointes de P. Buysrogge et Ch. Brotcorne au ministre de la Justice sur 'le fonctionnement de la Sûreté de l'État' (*C.R.I.*, Chambre, 2014-2015, 23 avril 2015, PLEN 042, p. 26, Q. nos 433 et 434)

Question de W. De Vriendt à la secrétaire d'État à la Lutte contre la pauvreté sur 'le déménagement aux Archives de l'État des archives africaines du SPF Affaires étrangères' (*Q.R.*, Chambre, 2014-2015, 27 avril 2015, no 022, p. 165, Q. no 57)

Question de K. Temmerman au ministre de l'Intérieur sur 'la mise en œuvre des douze mesures de lutte contre le radicalisme et le terrorisme' (*Q.R.*, Chambre, 2014-2015, 4 mai 2015, no 023, p. 13, Q. no 257)

Question B. Pas au ministre de l'Intérieur sur les 'frais effectués par le SPF Intérieur pour le compte de la Maison royale' (*Q.R.*, Chambre, 2014-2015, 4 mai 2015, no 023, p. 83, Q. no 110)

Question de F. Demon au ministre de l'Intérieur sur 'les courses cyclistes printanières – corps de police locale – appui de la police fédérale' (*Q.R.*, Chambre, 2014-2015, 4 mai 2015, no 023, p. 127, Q. no 256)

Question de K. Jadin au ministre de l'Intérieur sur 'la politique de renseignement – le Conseil national de sécurité' (*Q.R.*, Chambre, 2014-2015, 4 mai 2015, no 023, p. 136, Q. no 276)

Question de P. Dedecker au ministre des Télécommunications sur 'la révision de la loi sur la rétention de données' (*C.R.I.*, Chambre, 2014-2015, 5 mai 2015, COM 155, p. 1, Q. no 3102)

Question de D. Geerts au ministre des Télécommunications sur 'la multiplication par deux du nombre de cyberincidents en Belgique' (*C.R.I.*, Chambre, 2014-2015, 5 mai 2015, COM 155, p. 12, Q. no 3013)

Questions jointes de O. Maingain et W. Demeyer au ministre de l'Intérieur sur 'le Conseil national de sécurité' (*C.R.I.*, Chambre, 2014-2015, 5 mai 2015, COM 159, p. 6, Q. nos 3907 et 4126)

Question de V. Matz au ministre de l'Intérieur sur 'les menaces terroristes contre des lieux de cultes chrétiens en Belgique' (*C.R.I.*, Chambre, 2014-2015, 6 mai 2015, COM 165, p. 12, Q. no 4119)

Question d'O. Maingain au ministre de l'Intérieur sur 'la lutte contre les cyberattaques' (*C.R.I.*, Chambre, 2014-2015, 6 mai 2015, COM 165, p. 13, Q. nº 3739)

Question de S. Van Hecke au ministre de l'Intérieur sur 'la base juridique du recours à l'armée en cas de niveau 3 de la menace' (*Q.R.*, Chambre, 2014-2015, 11 mai 2015, nº 024, p. 95, Q. nº 242)

Question de F. Demon au ministre de l'Intérieur sur 'les permanences des postes de police' (*Q.R.*, Chambre, 2014-2015, 11 mai 2015, nº 024, p. 99, Q. nº 259)

Question de R. Hedebouw au premier ministre sur 'l'enquête sur l'assassinat de Julien Lahaut ' (*C.R.I.*, Chambre, 2014-2015, 13 mai 2015, PLEN 46, p. 27, Q. nº 490)

Question de F. Schepmans au ministre de la Justice sur 'l'échange de l'information dans le cadre la lutte contre le terrorisme et contre le radicalisme – échelle nationale – groupe de travail' (*Q.R.*, Chambre, 2014-2015, 18 mai 2015, nº 025, p. 117, Q. nº 235)

Question de S. Van Hecke au ministre de la Justice sur 'l'affaire d'espionnage russe' (*Q.R.*, Chambre, 2014-2015, 18 mai 2015, nº 025, p. 120, Q. nº 297)

Question de R. Deseyn à la ministre de l'Énergie sur le 'Service d'inspection de l'infrastructure critique' (*Q.R.*, Chambre, 2014-2015, 18 mai 2015, nº 025, p. 165, Q. nº 49)

Question de J.-M. Nollet au ministre de l'Intérieur sur 'la capacité de nos centrales nucléaires à résister à la chute d'un avion gros porteur' (*C.R.I.*, Chambre, 2014-2015, 27 mai 2015, COM 176, p. 31, Q. nº 4328)

Question de A. Carcaci au ministre de l'Intérieur sur 'le contrôle des frontières' (*C.R.I.*, Chambre, 2014-2015, 21 mai 2015, PLEN 47, p. 13, Q. nº 514)

Question de H. Bonte au ministre de l'Intérieur sur 'des pratiques administratives critiquables dans la lutte contre le radicalisme' (*C.R.I.*, Chambre, 2014-2015, 21 mai 2015, PLEN 47, p. 18, Q. nº 516)

Questions jointes de B. Hellings, J.J. Flahaux et V. Matz au ministre de la Défense sur 'les liens structurels entre le SGRS et la NSA à l'aune des informations erronées sur des attentats prétendument déjoués communiquées par le chef des renseignements militaires' (*C.R.I.*, Chambre, 2014-2015, 27 mai 2015, COM 182, p. 35, Q. nºs 4195, 4259 et 4595)

Questions jointes de W. De Vriendt, V. Yüksel, S. Crusnière et K. Grosemans au ministre de la Défense sur 'le Burundi' (*C.R.I.*, Chambre, 2014-2015, 27 mai 2015, COM 182, p. 28, Q. nºs 4387, 4392, 4511 en 4591)

Question de A. Top au ministre de la Défense sur 'l'étude relative aux services de renseignements' (*C.R.I.*, Chambre, 2014-2015, 27 mai 2015, COM 182, p. 61, Q. nº 4526)

Question de K. Jadin au premier ministre sur 'la politique de renseignement – le Conseil national de sécurité' (*Q.R.*, Chambre, 2014-2015, 2 juin 2015, nº 027, p. 41, Q. nº 30)

Question de K. Metsu au ministre de l'Intérieur sur 'la présence à la police fédérale d'un stagiaire ayant des sympathies pour l'EI' (*Q.R.*, Chambre, 2014-2015, 2 juin 2015, nº 027, p. 123, Q. nº 359)

Question de V. Scourneau au ministre de la Défense sur 'l'engagement dans le cadre du programme de cybersécurité' (*Q.R.*, Chambre, 2014-2015, 2 juin 2015, nº 027, p. 243, Q. nº 221)

Question de D. Ducarme au ministre de l'Intérieur sur 'le groupe NATION et la lutte contre les extrémistes' (*C.R.I.*, Chambre, 2014-2015, 4 juin 2015, PLEN 50, p. 22, Q. nº 559)

Questions jointes de P. Buysrogge, A. Frédéric et B. Hellings au premier ministre sur 'le nouveau piratage de Belgacom par les services de renseignement allemands' (*C.R.I.*, Chambre, 2014-2015, 9 juin 2015, COM 186, p. 17, Q. nos 4802, 4910 et 4915)

Question de K. Grosemans au ministre des Affaires étrangères sur 'les attestations de sécurité délivrées par l'Autorité nationale de sécurité' (*Q.R.*, Chambre, 2014-2015, 9 juin 2015, nº 028, p. 126, Q. nº 171)

Question de S. Van Hecke au ministre de la Défense sur 'la base juridique du recours à l'armée en cas de niveau 3 de la menace' (*Q.R.*, Chambre, 2014-2015, 9 juin 2015, nº 028, p. 257, Q. nº 235)

Question de V. Yüksel au ministre de la Défense sur les 'licenciements pour raisons médicales à l'armée belge' (*Q.R.*, Chambre, 2014-2015, 9 juin 2015, nº 028, p. 264, Q. nº 236)

Question d'A. Top au ministre de la Défense sur 'les mesures de sécurité supplémentaires adoptées à la suite de la divulgation de photos prises dans une autopsie' (*C.R.I.*, Chambre, 2014-2015, 10 juin 2015, COM 189, p. 7, Q. nos 4813)

Question de N. Ben Hamou au ministre de l'Intérieur sur 'la baisse de la criminalité en lien avec la présence militaire en rue' (*C.R.I.*, Chambre, 2014-2015, 10 juin 2015, COM 192, p. 4, Q. nº 4436)

Question de J.-M. Nollet au ministre de l'Intérieur sur 'la capacité de nos centrales nucléaires à résister à la chute d'un avion gros porteur' (*C.R.I.*, Chambre, 2014-2015, 10 juin 2015, COM 192, p. 36, Q. nº 4777)

Question d'A. Top au Premier ministre sur 'l'achat de GSM sécurisés' (*Q.R.*, Chambre, 2014-2015, 15 juin 2015, nº 029, p. 73, Q. nº 32)

Question K. Metsu au ministre de l'Intérieur sur 'l'Imam Van Ael – arrêt des activités publiques' (*Q.R.*, Chambre, 2014-2015, 15 juin 2015, nº 029, p. 99, Q. nº 407)

Question de S. Van Hecke au ministre des Affaires étrangères sur 'l'augmentation du nombre d'espions russes' (*Q.R.*, Chambre, 2014-2015, 15 juin 2015, nº 029, p. 102, Q. nº 167)

Question de R. Deseyn à la ministre de la Mobilité sur le 'Service d'inspection de l'infrastructure critique' (*Q.R.*, Chambre, 2014-2015, 15 juin 2015, nº 029, p. 283, Q. nº 344)

Questions jointes de S. Van Hecke et G. Dallemagne au ministre de la Justice sur 'les activités d'espionnage menées, à la demande de la NSA, par les services de renseignements allemands sur les communications téléphoniques et l'échange de données en provenance de Belgique et vers celle-ci' (*C.R.I.*, Chambre, 2014-2015, 16 juin 2015, COM 193, p. 12, Q. nos 4693 et 4988)

Questions jointes de S. Van Hecke au ministre de la Justice sur 'la catégorisation des informations recueillies par la Sûreté de l'État' (*C.R.I.*, Chambre, 2014-2015, 16 juin 2015, COM 193, p. 23, Q. nos 4806 à 4810)

Question de P. Buysrogge au ministre de la Justice sur 'l'infrastructure de la VSSE' (*Q.R.*, Chambre, 2014-2015, 22 juin 2015, nº 030, p. 106, Q. nº 346)

Question de K. Gabriëls au ministre de la Justice sur 'la transparence à la Sûreté de l'État' (*Q.R.*, Chambre, 2014-2015, 22 juin 2015, nº 030, p. 108, Q. nº 368)

Question de K. Jadin au ministre de la Défense sur 'l'énorme état-major au sein de notre armée.' (*Q.R.*, Chambre, 2014-2015, 22 juin 2015, n° 030, p. 146, Q. n° 250)

Question de J.-M. Nollet au ministre de la Défense sur 'les missions octroyées à Mr André Moyen' (*Q.R.*, Chambre, 2014-2015, 22 juin 2015, n° 030, p. 156, Q. n° 257)

Question de K. Temmerman au ministre de l'Intérieur sur 'la mise en œuvre des douze mesures de lutte contre le radicalisme et le terrorisme' (*Q.R.*, Chambre, 2014-2015, 29 juin 2015, n° 031, p. 212, Q. n° 257)

Question de V. Yüksel au ministre de l'Intérieur sur 'les heures supplémentaires à la police dans le cadre du relèvement du niveau de la menace terroriste' (*Q.R.*, Chambre, 2014-2015, 29 juin 2015, n° 031, p. 213, Q. n° 284)

Question de W. Demeyer au ministre de l'Intérieur sur 'l'opération anti-terroriste menée en divers endroits du royaume ce lundi 8 juin' (*C.R.I.*, Chambre, 2014-2015, 1er juillet 2015, COM 208, p. 1, Q. n° 4970)

Questions jointes de F. Demon et K. Metsu au ministre de l'Intérieur sur 'les conséquences de l'annulation de la loi sur la rétention des données' (*C.R.I.*, Chambre, 2014-2015, 1er juillet 2015, COM 209, p. 30, Q. nos 5100 et 5188)

Question de R. Hufkens au ministre de l'Intérieur sur 'la surveillance d'ambassades et d'institutions internationales par des entreprises privées de gardiennage' (*Q.R.*, Chambre, 2014-2015, 6 juillet 2015, n° 032, p. 116, Q. n° 376)

Question de B. Pas au ministre de l'Intérieur sur 'la campagne électorale du président Erdogan à l'Ethias Arena à Hasselt' (*Q.R.*, Chambre, 2014-2015, 6 juillet 2015, n° 032, p. 117, Q. n° 387)

Question de B. Pas au ministre de la Justice sur la 'Sûreté de l'État – composition actuelle des cadres linguistiques' (*Q.R.*, Chambre, 2014-2015, 6 juillet 2015, n° 032, p. 177, Q. n° 318)

Questions jointes de A. Top, G. Dallemagne et V. Yüksel au ministre de la Justice sur 'la fuite de documents de la Défense' (*C.R.I.*, Chambre, 2014-2015, 8 juillet 2015, COM 219, p. 10, Q. nos 5162, 5373 et 5690)

Question de J. Fernandez Fernandez au ministre de la Défense sur 'le recrutement de 24 spécialistes en cybersécurité' (*C.R.I.*, Chambre, 2014-2015, 8 juillet 2015, COM 219, p. 19, Q. n° 5400)

Question de B. Hellings au ministre de l'Intérieur sur 'l'installation d'unités spéciales d'espionnage dans certaines ambassades américaines dans le monde' (*C.R.I.*, Chambre, 2014-2015, 8 juillet 2015, COM 219, p. 20, Q. n° 5404)

Question de N. Lijnen au ministre des Affaires étrangères sur 'l'opération menée à Alep' (*C.R.I.*, Chambre, 2014-2015, 9 juillet 2015, PLEN 62, p. 38, Q. n° 690)

Question de R. Hedebouw au ministre de l'Intérieur sur 'l'application du protocole d'accord du 17 janvier 2015 sur le déploiement de l'armée' (*Q.R.*, Chambre, 2014-2015, 13 juillet 2015, n° 033, p. 109, Q. n° 199)

Question de D. Ducarme au ministre de l'Intérieur sur 'l'annulation de la conférence du 3 juin 2015 suite à des menaces' (*Q.R.*, Chambre, 2014-2015, 13 juillet 2015, n° 033, p. 139, Q. n° 479)

Question de D. Ducarme au ministre de l'Intérieur sur 'l'Organisation islamiste à Anvers' (*Q.R.*, Chambre, 2014-2015, 13 juillet 2015, n° 033, p. 141, Q. n° 480)

Question de B. Hellings au ministre de l'Intérieur sur 'l'expulsion de ressortissants de l'Union européenne' (*C.R.I.*, Chambre, 2014-2015, 14 juillet 2015, COM 225, p. 10, Q. nº 5569)

Question de K. Metsu au ministre de l'Intérieur sur 'le screening des imams' (*C.R.I.*, Chambre, 2014-2015, 14 juillet 2015, COM 225, p. 13, Q. nº 5595)

Question de K. Metsu au ministre de l'Intérieur sur 'l'expulsion d'imams radicaux' (*C.R.I.*, Chambre, 2014-2015, 14 juillet 2015, COM 225, p. 23, Q. nº 5728)

Question de V. Matz au ministre de l'Intérieur sur 'la demande des syndicats d'annuler le défilé des policiers le 21 juillet 2015' (*C.R.I.*, Chambre, 2014-2015, 16 juillet 2015, PLEN 065, p. 8, Q. nº 700)

Question de F. Dewinter au ministre de la Justice sur les 'combattants de retour de Syrie et/ou membres de l'EI' (*Q.R.*, Chambre, 2014-2015, 22 juillet 2015, nº 034, p. 198, Q. nº 162)

Question de K. Temmerman au Premier ministre sur 'la mise en œuvre des douze mesures de lutte contre le radicalisme et le terrorisme' (*Q.R.*, Chambre, 2014-2015, 27 juillet 2015, nº 035, p. 17, Q. nº 53)

Question de S. Van Hecke au ministre de la Justice sur 'l'augmentation de l'espionnage russe' (*Q.R.*, Chambre, 2014-2015, 27 juillet 2015, nº 035, p. 59, Q. nº 365)

Question de L. Van Biesen au ministre de la Justice sur le 'nouveau système d'évaluation du personnel des services publics fédéraux' (*Q.R.*, Chambre, 2014-2015, 27 juillet 2015, nº 035, p. 63, Q. nº 374)

Question de E. Kir au ministre de l'Intérieur sur 'le plan d'action européen antiterroriste' (*Q.R.*, Chambre, 2014-2015, 3 août 2015, nº 036, p. 68, Q. nº 413)

Question de V. Yüksel au ministre de la Défense sur 'le stockage d'informations numériques' (*Q.R.*, Chambre, 2014-2015, 3 août 2015, nº 036, p. 206, Q. nº 300)

Question de V. Yüksel au ministre de la Défense sur 'les pilotes de la Composante aérienne' (*Q.R.*, Chambre, 2014-2015, 3 août 2015, nº 036, p. 209, Q. nº 302)

Question de V. Yüksel au ministre de la Défense sur 'la Division Sécurité du SGR' (*Q.R.*, Chambre, 2014-2015, 3 août 2015, nº 036, p. 214, Q. nº 303)

Question de V. Yüksel au ministre de la Défense sur 'les militaires qui travaillent pour d'autres ministères' (*Q.R.*, Chambre, 2014-2015, 10 août 2015, nº 037, p. 160, Q. nº 329)

Question de P. Buysrogge au ministre de la Défense sur 'l'infrastructure de la VSSE' (*Q.R.*, Chambre, 2014-2015, 17 août 2015, nº 038, p. 249, Q. nº 333)

Question de R. Deseyn au ministre de l'Intérieur sur le 'Service d'inspection de l'infrastructure critique' (*Q.R.*, Chambre, 2014-2015, 31 août 2015, nº 040, p. 81, Q. nº 297)

Question de G. Gilkinet au ministre de l'Intérieur sur 'l'évolution du nombre de policiers' (*Q.R.*, Chambre, 2014-2015, 31 août 2015, nº 040, p. 114, Q. nº 383)

Question de K. Metsu au ministre de l'Intérieur sur les 'attentats à Lyon, à Sousse et au Koweït' (*Q.R.*, Chambre, 2014-2015, 31 août 2015, nº 040, p. 289, Q. nº 566)

Question de B. Pas au ministre de l'Intérieur sur 'le contrôle exercé par la Commission permanente de contrôle linguistique en matière de respect des cadres linguistiques à la Sûreté de l'État' (*Q.R.*, Chambre, 2014-2015, 31 août 2015, nº 040, p. 301, Q. nº 575)

Question de K. Metsu au ministre de l'Intérieur sur les 'services de renseignement – surveillance' (*Q.R.*, Chambre, 2014-2015, 7 septembre 2015, nº 041, p. 99, Q. nº 619)

Question de R. Deseyn ministre de l'Intérieur sur 'l'espionnage par des diplomates russes' (*Q.R.*, Chambre, 2014-2015, 7 septembre 2015, n° 041, p. 124, Q. n° 269)

Question de B. Pas au ministre de la Justice sur 'la campagne électorale du président Erdogan à l'Ethias Arena à Hasselt' (*Q.R.*, Chambre, 2014-2015, 16 septembre 2015, n° 042, p. 165, Q. n° 357)

Question de B. Pas au ministre de la Justice sur 'la nomination d'administrateurs par le gouvernement fédéral.' (*Q.R.*, Chambre, 2014-2015, 16 septembre 2015, n° 042, p. 182, Q. n° 427)

Question de Ph. Blanchart au ministre de l'Intérieur sur 'les agissements d'anarchistes à Bruxelles' (*Q.R.*, Chambre, 2014-2015, 21 septembre 2015, n° 043, p. 20, Q. n° 405)

Question de Ph. Pivin au ministre de la Justice sur 'les écoles confessionnelles, les matières cultuelles et le contrôle en la matière' (*C.R.I.*, Chambre, 2014-2015, 7 octobre 2015, COM 240, p. 27, Q. n° 6143)

Question de A. Top au ministre de la Justice sur 'la sécurité de l'information' (*C.R.I.*, Chambre, 2014-2015, 7 octobre 2015, COM 240, p. 52, Q. n° 6614)

Question de E. Burton au ministre de l'Intérieur sur 'les caméras ANPR' (*Q.R.*, Chambre, 2015-2016, 9 octobre 2015, n° 046, p. 40, Q. n° 491)

Question de K. Metsu au ministre de l'Intérieur sur 'une unité de police européenne à la recherche de membres de l'EI sur les réseaux sociaux' (*Q.R.*, Chambre, 2015-2016, 9 octobre 2015, n° 046, p. 55, Q. n° 567)

Question de K. Metsu au ministre de l'Intérieur sur les 'allocations perçues par les combattants partis en Syrie' (*Q.R.*, Chambre, 2015-2016, 9 octobre 2015, n° 046, p. 61, Q. n° 594)

Question de K. Degroote au ministre de l'Intérieur sur le 'détachement en dehors de la police intégrée' (*Q.R.*, Chambre, 2015-2016, 9 octobre 2015, n° 046, p. 72, Q. n° 615)

Question de K. Metsu au ministre de la Défense sur 'la radicalisation de militaires' (*Q.R.*, Chambre, 2015-2016, 9 octobre 2015, n° 046, p. 259, Q. n° 375)

Question de J. Penris au ministre de la Défense sur 'les conséquences éventuelles d'actes de trahison commis par des militaires sur la lutte contre l'extrémisme musulman (*Q.R.*, Chambre, 2015-2016, 9 octobre 2015, n° 046, p. 261, Q. n° 377)

Question de R. Deseyn au ministre de la Défense sur 'l'espionnage par des diplomates russes' (*Q.R.*, Chambre, 2015-2016, 19 octobre 2015, n° 047, p. 214, Q. n° 380)

Question de S. De Wit au ministre de la Justice sur 'la solution annoncée par le ministre suite à la suite de l'annulation de la loi sur la conservation des données' (*C.R.I.*, Chambre, 2015-2016, 21 octobre 2015, COM 250, p. 28, Q. n° 5823)

Question de S. Van Hecke au ministre de la Justice sur 'le rôle joué par la Sûreté de l'État lors de la visite d'État du président Erdogan' (*C.R.I.*, Chambre, 2015-2016, 21 octobre 2015, COM 250, p. 47, Q. n° 6817)

Questions jointes de B. Hellings et A. Top au ministre de la Défense sur 'les velléités du chef des renseignements militaires de mettre sous surveillance généralisée les échanges numériques transitant par fibre optique en Belgique' (*C.R.I.*, Chambre, 2015-2016, 28 octobre 2015, COM 256, p. 4, Q. n^{os} 5720 et 5863)

Question de S. Pirlot au ministre de la Défense sur 'la stratégie du SGRS en matière de lutte contre le terrorisme' (*C.R.I.*, Chambre, 2015-2016, 28 octobre 2015, COM 256, p. 21, Q. n° 5950)

Questions jointes de P. Dedecker, Ö. Özen, Ph. Goffin et D. Geerts au secrétaire d'État à la Lutte contre la fraude sociale sur 'la position du gouvernement en ce qui concerne la protection des données personnelles des Européens aux États-Unis' (*C.R.I.*, Chambre, 2015-2016, 28 octobre 2015, COM 257, p. 4, Q. n^{os} 6455, 6480, 6635 et 7116)

Question d'O. Maingain au ministre de la Justice sur 'la lutte contre la montée du radicalisme en milieu carcéral' (*C.R.I.*, Chambre, 2015-2016, 28 octobre 2015, COM 259, p. 6, Q. n° 6777)

Question de W. Demeyer au ministre de l'Intérieur sur 'la circulaire relative à l'échange d'informations et au suivi des 'foreign terrorist fighters' en provenance de Belgique' (*C.R.I.*, Chambre, 2015-2016, 28 octobre 2015, COM 259, p. 19, Q. n° 7029)

Question de K. Jadin au ministre de l'Intérieur sur 'le recensement des armes' (*C.R.I.*, Chambre, 2015-2016, 28 octobre 2015, COM 261, p. 30, Q. n° 6003)

Question de Ph. Pivin au ministre de l'Intérieur sur 'les actions de protection des infrastructures aéronautiques et fluviales belges contre les menaces terroristes' (*C.R.I.*, Chambre, 2015-2016, 28 octobre 2015, COM 261, p. 41, Q. n° 6142)

Question de A. Top au ministre de l'Intérieur sur 'la visite de travail du ministre en Afrique du Nord' (*C.R.I.*, Chambre, 2015-2016, 28 octobre 2015, COM 261, p. 57, Q. n° 6531)

Question de B. Pas au ministre de l'Intérieur sur 'la foire musulmane' (*C.R.I.*, Chambre, 2015-2016, 29 octobre 2015, PLEN 079, p. 29, Q. n° 760)

Question de E. Kir au ministre de l'Intérieur sur 'l'évaluation de la menace terroriste en Belgique suite aux attentats en France et en Tunisie du 26 juin 2015' (*Q.R.*, Chambre, 2015-2016, 9 novembre 2015, n° 049, p. 93, Q. n° 722)

Question de F. Schepmans au ministre de la Justice sur les 'perquisitions menées dans le milieu du djihadisme tchétchène' (*Q.R.*, Chambre, 2015-2016, 9 novembre 2015, n° 049, p. 132, Q. n° 410)

Question de B. Pas au ministre de la Justice sur 'les rémunérations ou indemnités supplémantaires perçues par les délégués syndicaux dans les comités de gestion et autres conseils/commissions' (*Q.R.*, Chambre, 2015-2016, 9 novembre 2015, n° 049, p. 140, Q. n° 536)

Question de S. Lahaye-Battheu au ministre des Finances sur les 'condamnations pour infraction au Code de la route – confiscations de véhicules' (*Q.R.*, Chambre, 2015-2016, 9 novembre 2015, n° 049, p. 198, Q. n° 223)

Question de F. Demon au ministre de la Défense sur 'la mise en ligne des plans de bâtiments publics' (*Q.R.*, Chambre, 2015-2016, 9 novembre 2015, n° 049, p. 358, Q. n° 389)

Question de F. Dewinter au ministre de l'Intérieur sur 'les mesures prises par le gouvernement pour contrecarrer l'infiltration d'éventuels militants de l'EI mêlés au flux des demandeurs d'asile' (*C.R.I.*, Chambre, 2015-2016, 12 novembre 2015, PLEN 080, p. 37, Q. n° 793)

Communication du ministre de la Défense, échange de vues et questions jointes de S. Pirlot, B. Hellings, G. Dallemagne, V. Yüksel, A. Top, W. De Vriendt et K. Grosemans sur 'la nouvelle mission du Léopold I^{er}'(*C.R.I.*, Chambre, 2015-2016, 18 novembre 2015, COM 270, p. 1, Q. n^{os} 7356, 7361, 7462, 7478, 7480, 7481, 7493, 7463 et 7479)

Question de B. Vermeulen au Premier ministre sur 'la protection des infrastructures critiques' (*C.R.I.*, Chambre, 2015-2016, 24 novembre 2015, COM 274, p. 10, Q. nº 7616)

Questions jointes d'A. Top, S. Pirlot et G. Dallemagne au ministre de la Défense sur 'la participation belge à l'opération MINUSMA en 2016' (*C.R.I.*, Chambre, 2015-2016, 25 novembre 2015, COM 277, p. 25, Q. nºs 6417, 7571 et 7632)

Question d'A. Top au ministre de la Défense sur 'la fuite de documents contenant des informations sensibles' (*C.R.I.*, Chambre, 2015-2016, 25 novembre 2015, COM 277, p. 30, Q. nº 6420)

Questions jointes de S. Pirlot, A. Top, G. Dallemagne et K. Jadin au ministre de la Défense sur 'le coût du déploiement des militaires dans les rues' (*C.R.I.*, Chambre, 2015-2016, 25 novembre 2015, COM 277, p. 40, Q. nºs 6546, 6684, 6977, 7128, 7611 et 7631)

Questions jointes de W. De Vriendt, A. Top, G. Dallemagne et S. Pirlot au ministre de la Défense sur 'le plan stratégique de la Défense' (*C.R.I.*, Chambre, 2015-2016, 25 novembre 2015, COM 277, p. 58, Q. nºs 7252, 7313, 7464 et 7567)

Question de K. Metsu au ministre de l'Intérieur sur 'la présence des terroristes dans les centres d'accueil belges' (*C.R.I.*, Chambre, 2015-2016, 25 novembre 2015, COM 278, p. 1, Q. nº 7650)

Question de K. Metsu au ministre de l'Intérieur sur 'la task force sur la radicalisation' (*C.R.I.*, Chambre, 2015-2016, 25 novembre 2015, COM 278, p. 4, Q. nº 7652)

Questions jointes de L. Onkelinx, R. Hedebouw, P. Dewael, F. Dewinter, M. Kitir, G. Dallemagne, O. Maingain, S. Verherstraeten, K. Metsu, D. Ducarme, et J.-M. Nollet au Premier ministre sur 'le terrorisme' (*Q.R.*, Chambre, 2015-2016, 26 novembre 2015, nº 083, p. 1, Q. nºs 816 à 826)

Question de Ph. Pivin au ministre de l'Intérieur sur les 'combattants belges partis faire le « djihad »' (*Q.R.*, Chambre, 2015-2016, 29 novembre 2015, nº 048, p. 111, Q. nº 400)

Question S. Pirlot au ministre de la Justice sur 'la collaboration entre la Sûreté et le SGRS en matière de lutte contre le terrorisme' (*Q.R.*, Chambre, 2015-2016, 29 novembre 2015, nº 048, p. 252, Q. nº 599)

Question de K. Metsu au ministre de la Défense sur les 'services de renseignement – surveillance' (*Q.R.*, Chambre, 2015-2016, 29 novembre 2015, nº 048, p. 322, Q. nº 384)

Question de F. Schepmans au ministre de l'Intérieur sur 'les perquisitions menées dans le milieu du djihadisme tchétchène' (*Q.R.*, Chambre, 2015-2016, 30 novembre 2015, nº 052, p. 77, Q. nº 719)

Question de S. Van Hecke au ministre de l'Intérieur sur 'la visite d'État du président Erdogan – contrôle des armes de l'équipe de sécurité' (*Q.R.*, Chambre, 2015-2016, 30 novembre 2015, nº 052, p. 99, Q. nº 794)

Échange de vues avec le ministre de l'Intérieur et le ministre de la Justice sur la lutte contre le terrorisme et le radicalisme et questions jointes d'O. Maingain,

W. Demeyer, E. Thiébaut, K. Jadin, K. Metsu, E. Kir, N. Ben Hamou, G. Vanden Burre, V. Matz, F. Demon, S. Van Hecke, K. Van Vaerenbergh, Ph. Pivin, A. Top, Ph. Blanchart, J.-M. Nollet, G. Dallemagne, Ph. Goffin, H. Bonte, F. Schepmans, I. De Coninck, D. Ducarme et S. De Wit sur 'la circulaire relative au suivi des 'foreign terrorist fighters' en provenance de la Belgique' (*C.R.I.*, Chambre, 2015-2016, 2 décembre 2015, COM 285, 1, Q. nºs 6645, 7029, 7208, 7384, 7610, 7466, 7487, 7488,

7518, 7519, 7527, 7530, 7547, 7566, 7568, 7573, 7607, 7620, 7640, 7641, 7655, 7702, 7707, 7722, 7730, 7740, 7751, 7761, 7762, 7763, 7764, 7766, 7770, 7771, 7776, 7777, 7778, 7780, 7781, 7782, 7788, 7789, 7790, 7791, 7806 et 7807)

Questions jointes de K. Jadin et G. Dallemagne au ministre de la Défense sur 'le rapprochement entre SGRS et Sûreté de l'État' (*C.R.I.*, Chambre, 2015-2016, 9 décembre 2015, COM 288, p. 1, Q. n^{os} 7385 et 7461)

Questions jointes de A. Top, R. Hufkens et V. Yüksel au ministre de la Défense sur 'la bombe incendiaire à la caserne de Heverlee' (*C.R.I.*, Chambre, 2015-2016, 9 décembre 2015, COM 288, p. 16, Q. n^{os} 7795, 7799 et 7888)

Question de V. Yüksel au ministre de la Défense sur 'le rapport du Comité R sur la radicalisation au sein de la Défense' (*C.R.I.*, Chambre, 2015-2016, 9 décembre 2015, COM 288, p. 20, Q. n^{o} 7887)

Question de R. Hufkens au ministre de la Défense sur 'la divulgation d'informations sensibles par des canaux 'open source'' (*C.R.I.*, Chambre, 2015-2016, 9 décembre 2015, COM 288, p. 26, Q. n^{o} 7925)

Question de F. Dewinterau ministre de l'Intérieur sur 'le bail emphytéotique et l'éventuelle fermeture de la Grande Mosquée saoudienne du Cinquantenaire de Bruxelles' (*C.R.I.*, Chambre, 2015-2016, 10 décembre 2015, PLEN 085, p. 8, Q. n^{o} 867)

Question de Ph. Goffin au ministre de la Justice sur 'les contacts du présumé terroriste Salah Abdeslam à la prison de Namur' (*C.R.I.*, Chambre, 2015-2016, 10 décembre 2015, PLEN 085, p. 12, Q. n^{o} 870)

Questions jointes d'Ö. Özlen, V. Matz, G. Vanden Burre, O. Maingain, D. Ducarme, H. Bonte et C. Van Cauter au ministre de la Justice sur 'l'enquête autour de Salah Abdeslam' (*C.R.I.*, Chambre, 2015-2016, 17 décembre 2015, PLEN 090, p. 161, Q. n^{os} 885 à 891)

Question de S. Van Hecke au ministre de la Justice sur 'le protocole d'accord entre la Banque nationale et la Sûreté de l'État' (*C.R.I.*, Chambre, 2015-2016, 6 janvier 2016, COM 301, p. 3, Q. n^{o} 8170)

ACTIVITEITENVERSLAG 2015
RAPPORT D'ACTIVITÉS 2015

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).

Reeds 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.
10) W. Van Laethem en J. Vanderborght (eds), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, 2013, 565 p.
11) Vast Comité I, *Activiteitenverslag 2012*, 2013, 115 p.
12) Vast Comité I, *Activiteitenverslag 2013*, 2014, 210 p.
13) Vast Comité I, *Activiteitenverslag 2014*, 2015, 135 p.
14) Vast Comité I, *Activiteitenverslag 2015*, 2016, 132 p.

ACTIVITEITENVERSLAG 2015

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

intersentia
Antwerpen – Cambridge

Voorliggend *Activiteitenverslag 2015* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 16 september 2016.

(*getekend*)
Guy Rapaille, voorzitter
Gérald Vande Walle, raadsheer
Pieter-Alexander De Brock, raadsheer
Wouter De Ridder, griffier

Activiteitenverslag 2015
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

ISBN 978-94-000-0782-6
D/2016/7849/167
NUR 823

INHOUD

LIJST MET AFKORTINGEN

ADCC	Algemene Directie Crisiscentrum
ADIV	Algemene Dienst inlichting en veiligheid van de Krijgsmacht
AGG	Antiterroristische Gemengde Groep
ANG	Algemene Nationale Gegevensbank
BIA	*Belgian Intelligence Academy*
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
BISC	*Belgian Intelligence Studies Centre*
BS	Belgisch Staatsblad
CAP	Centraal Aanspreekpunt
CCB	Centrum voor Cybersecurity België
CNCIS	*Commission nationale de contrôle des interceptions de sécurité* (Frankrijk)
CNCTR	*Commission nationale de contrôle des techniques de renseignement* (Frankrijk)
COC	Controleorgaan voor politionele informatie
CRIV	Compte Rendu Intégral – Integraal Verslag
CTIVD	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (Nederland)
DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
EVRM	Europees Verdrag voor de Rechten van de Mens
FOD	Federale overheidsdienst
FRA	*European Union Agency for Fundamental Rights*
FTF	*Foreign terrorist fighters*
Parl. St.	Parlementaire Stukken van Kamer en Senaat
Hand.	Handelingen
HUMINT	*Human intelligence*
ICT	Informatie- en communicatietechnologie
IS	Islamitische Staat

ISIS	Islamitische Staat in Irak en Syrië
JIB	*Joint information box*
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
KUIAD	Koninklijke Unie der Inlichtings- en Actiediensten
M.B.	Ministerieel besluit
MCIV	Ministerieel Comité voor inlichting en veiligheid
NBB	Nationale Bank van België
NSA	*National Security Agency*
NTF	Nationale Task Force
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open sources intelligence*
Privacycommissie	Commissie voor de bescherming van de persoonlijke levenssfeer
SIGINT	*Signals intelligence*
SND	Sociale netwerkdiensten
SNS	Sociale netwerksites
SOCMINT	*Social media intelligence*
Sv.	Wetboek van Strafvordering
Sw.	Strafwetboek
TSA	*Transportation Security Agency*
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
VWEU	Verdrag betreffende de werking van de Europese Unie
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 coördinatie-orgaan voor de dreigingsanalyse

WOORD VOORAF

Begin januari 2015 vallen in het hoofdkantoor van het Franse satirische weekblad 'Charlie Hebdo' tijdens een schietpartij twaalf dodelijke slachtoffers. Nagenoeg gelijktijdig speelt er zich een gijzeling af in een supermarkt in Parijs. Hierbij komen nog eens vijf mensen om het leven. De daders zijn geradicaliseerde moslims die banden hebben met IS.

Amper enkele dagen later vindt in Verviers een grote antiterrorisme-actie plaats. Daarbij worden twee teruggekeerde Syriëstrijders gedood en raakt een derde gewond. Sindsdien volgden de (pogingen tot) terroristische aanslagen in Europa en de rest van de wereld elkaar op. Op 14 en 15 februari zijn er schietpartijen in het centrum van de Deense hoofdstad waarbij meerdere slachtoffers vallen. Twee maanden later wordt in Frankrijk een man gearresteerd omdat hij aanslagen plande tegen kerken in Parijs. Op 26 juni wordt in het Franse Isère een werkgever onthoofd en op 21 augustus verijdelen enkele alerte militairen een aanslag op de Thalys. Andere aanslagen vinden buiten Europa plaats. Daarbij wordt onder meer Tunesië hard getroffen.

Op 13 november 2015 gebeuren in Parijs meerdere aanslagen. Het aantal dodelijke slachtoffers loopt op tot 130. De gruweldaden zijn het werk van teruggekeerde *foreign terrorist fighters*. Vrij vlug na de aanslagen dook er informatie op die wees op het bestaan van een nauwe band met België.

De terreurdreiging houdt België tot de laatste seconde van 2015 in haar greep. Het eindejaarsvuurwerk wordt voor de tweede keer in een paar jaar tijd afgelast[1] en het dreigingsniveau wordt opgetrokken tot niveau 4. Dit bleek evenwel maar de voorbode van wat nog moest komen: Brussel, Istanbul, Nice, München…

De golf van aanslagen heeft de agenda van het Vast Comité I natuurlijk sterk bepaald. Er werden onderzoeken gestart naar de informatiepositie van de inlichtingendiensten en het OCAD voorafgaand aan de terreurdaden in Parijs en in Zaventem en Brussel.

Maar het Comité was reeds lang voordien gestart met een aantal toezichtonderzoeken die bepaalde aspecten van de opvolging van het radicaal islamisme belichtten. Een eerste onderzoek in deze materie werd zelfs opgestart voor de aanslagen van 9/11. Maar vanaf 2012 opende het Comité vele specifieke onderzoeken over deze problematiek. Zo onderzocht het Comité de opvolging van het extremisme binnen het leger, met daarin aandacht voor de radicale

1 VAST COMITÉ I, *Activiteitenverslag 2008*, 9-22 ('II.1. Het terreuralarm rond de jaarwisseling').

islam. En in 2014 werden onderzoeken geopend naar de *Joint Information Box* van het OCAD (dit is een lijst met radicaliserende personen en groeperingen), naar de informatie-uitwisseling tussen de VSSE en het gevangeniswezen (waarbij de focus lag op inlichtingen over extremisten en terroristen) alsook naar de informatiepositie van de inlichtingendiensten over de problematiek van de '*foreign terrorist fighters*' en de mislukte aanslag op de Thalys. De resultaten van een aantal van die onderzoeken vindt u terug in dit jaarverslag.

Diezelfde aanslagen hebben uiteraard ook de agenda bepaald van de Belgische regering die talloze initiatieven nam. Een aantal van die initiatieven hebben een directe impact op de werking van het Vast Comité I. Zo kreeg het recent de opdracht om – samen met het Controleorgaan voor politionele informatie (COC) – de nieuwe dynamische databank '*foreign terrorist fighters*' te controleren. En ook in het kader van de aankomende *Passenger Name Record*-regeling is een nieuwe toezichttaak voor het Comité in het vooruitzicht gesteld. Hetzelfde geldt voor de controle op buitenlandse intercepties door de ADIV die mogelijk zal uitgebreid worden. Er ligt namelijk een grondige herziening van de Inlichtingenwet van 30 november 1998 voor. Ten slotte valt niet uit sluiten dat het aantal dossiers voor het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen sterk zal stijgen. Er worden immers steeds meer (én strengere) veiligheidsscreenings uitgevoerd.

In de strijd tegen het barbaarse terrorisme waarin onze maatschappij vandaag verzeild is geraakt, moet elke actor van de veiligheidsketen zijn verantwoordelijkheid opnemen en 'een tandje bijsteken'. Zo ook het Vast Comité I dat, waar mogelijk, voorstellen zal blijven formuleren om de efficiëntie van de inlichtingen- en veiligheidsdiensten te verhogen en het respect voor fundamentele rechten en vrijheden en de rechtsstaat te garanderen.

Guy Rapaille,
Voorzitter van het Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

1 juni 2016

HOOFDSTUK I
DE OPVOLGING VAN DE AANBEVELINGEN VAN HET VAST COMITÉ I

Het Vast Comité I formuleert jaarlijks ten behoeve van de wetgever en de uitvoerende macht aanbevelingen 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 zijn ondersteunende diensten. De aanbevelingen die het Comité in 2015 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 aandacht gevestigd op aanbevelingen die het Comité essentieel acht, maar die vooralsnog niet werden geïmplementeerd.

I.1. INITIATIEVEN EN REALISATIES IN DE LIJN VAN DE DIVERSE AANBEVELINGEN

I.1.1. HET OCAD EN RICHTLIJNEN INZAKE DE SAMENWERKING MET BUITENLANDSE DIENSTEN

Het Coördinatieorgaan voor de dreigingsanalyse heeft, onder meer, de opdracht om met gelijkaardige buitenlandse of internationale diensten specifieke internationale contacten te onderhouden (art. 8, 3° W.OCAD). De Vaste Comités I en P drongen er op aan dat ter zake een richtlijn zou worden uitgevaardigd.[2] Het is de taak van de Nationale Veiligheidsraad om te bepalen wat het begrip 'gelijkaardige diensten' waarmee het OCAD 'specifieke contacten' mag onderhouden, inhoudt. Begin 2016 werd door de Nationale Veiligheidsraad een dergelijke richtlijn uitgevaardigd.

[2] VAST COMITÉ I, *Activiteitenverslag 2011*, 111 ('IX.2.4.8. De 'buitenlandopdracht' van het OCAD') en 'IX.2.5. De internationale relaties van het OCAD' van onderhavig verslag.

I.1.2. POLITIEKE STURING DOOR DE NATIONALE VEILIGHEIDSRAAD

Het toenmalige Ministerieel Comité voor inlichting en veiligheid (MCIV) werd opgericht als politiek sturend orgaan van het inlichtingenwerk. Het had onder meer als taak bij wijze van richtlijnen de algemene politiek inzake inlichtingen te bepalen en de prioriteiten van beide inlichtingendiensten vast te leggen. Het MCIV werd in 2015 omgevormd tot de Nationale Veiligheidsraad. Deze wordt bijgestaan door een Strategisch Comité voor inlichting en veiligheid en een Coördinatiecomité.[3]

Het Comité achtte het wenselijk dat de nieuwe Nationale Veiligheidsraad – mede op aangeven van de twee inlichtingendiensten – zijn sturende rol zou opnemen.[4] Mede onder impuls van de aanslagen in 2015, werd het vergaderritme sterk opgedreven en werden diverse ontwerp-richtlijnen besproken in de schoot van de Raad en zijn uitvoerende comités. De sturing uitte zich verder ook in de oprichting van een aantal thema-gebonden platformen waarin verschillende aspecten van het (inlichtingen-)beleid worden voorbereid. Zo werden bijvoorbeeld in 2015 de voorbereidingen getroffen voor de ontwikkeling van een 'nationaal inlichtingen(stuur)plan'.

I.1.3. PERMANENTE VORMING VAN HET PERSONEEL

Het belang van vorming en opleiding vormt uiteraard een belangrijk onderdeel van een goede organisatie. Tijdens de audit naar de werking van de Veiligheid van de Staat werd echter vastgesteld dat de '*intenties werden bemoeilijkt om de analisten een specifieke vorming te geven, aangepast aan de noden van de VSSE op het vlak van de analyse*'.[5] De officiële oprichting in 2015 van de *Belgian Intelligence Academy* (BIA) geeft uitvoering aan deze nood.

I.1.4. VOLDOENDE GEKWALIFICEERDE PERSONEELSLEDEN INZAKE *CYBERSECURITY*, *ICT-SECURITY* EN *CYBERINTELLIGENCE*

Het Vast Comité I stelde bij de inlichtingendiensten een ernstig tekort vast aan gekwalificeerd personeel om de opdracht inzake informatieveiligheid uit te oefe-

---

3 Zie J. VANDERBORGHT, 'De Trinitas 'Nationale Veiligheidsraad', 'Strategisch Comité' en 'Coördinatiecomité voor inlichting en veiligheid'', *Vigiles. Tijdschrift voor politierecht*, 2016, 1, 57-68.

4 VAST COMITÉ I, *Activiteitenverslag 2014*, 114 ('IX.1.4. De nood aan politieke sturing door de Nationale Veiligheidsraad').

5 VAST COMITÉ I, *Activiteitenverslag 2009*, 17.

nen. Het beval aan de diensten eindelijk de middelen te verschaffen die moeten toelaten het benodigde personeel te rekruteren.[6]

Halfweg 2015 verschenen vacatures voor de aanwerving van 24 *cyber security* en *risk prevention experts* om het *Cyber Security Operations Center* bij de ADIV te versterken.

I.1.5. DE AANWERVING VAN EEN PREVENTIEADVISEUR BIJ DE VSSE

Midden 2016 werd een preventieadviseur aangesteld binnen de VSSE. Immers, in het kader van het welzijn op het werk wordt bepaald dat elke entiteit met 200 tot 1.000 werknemers een interne dienst voor preventie en bescherming op het werk in het leven roept.[7] Bij de VSSE was die functie officieel vacant sinds maart 2013. In 2015 deed de VSSE nog beroep op de preventiedienst van de FOD Justitie (die elke week een gedurende één dag een preventieadviseur ter beschikking stelde).

I.1.6. RICHTLIJNEN AANGAANDE HET WERKEN MET HUMINT

Het Vast Comité I moest in het verleden vaststellen dat de richtlijnen met betrekking tot de informantenwerking verspreid lagen over diverse documenten. Dit was des te meer problematisch nu de informantenwerking slechts een zeer summiere wettelijke basis heeft (art. 18 W.I&V). Alhoewel het Comité meerdere malen gepleit heeft voor een nadere wettelijke regeling ter zake, werd vooralsnog geen dergelijk wetgevend initiatief genomen. Om die redenen beval het Comité aan dat de VSSE haar interne richtlijnen en *best practices* met betrekking tot de informantenwerking verder zou ontwikkelen en uitschrijven in duidelijke dienstnota's.[8] In 2011 werd hieraan reeds grotendeels tegemoet gekomen door de realisatie van de *'Instructies over het werken met menselijke bronnen'* en een dienstnota over *'de evaluatie van de informatie aangeleverd door menselijke bronnen'*.[9] Eind januari 2014 verspreidde de VSSE opnieuw een gedetailleerde nota over het omgaan met menselijke bronnen. In januari 2015 verscheen de omstandige dienstnota *'Instruc-*

---

6 VAST COMITÉ I, *Activiteitenverslag 2011*, 109 ('IX.2.3. Aanbevelingen met betrekking tot de informatieveiligheid', in het bijzonder 'IX.2.3.3. Voldoende gekwalificeerde personeelsleden').

7 Koninklijk besluit van 27 maart 1998 betreffende de Interne Dienst voor preventie en bescherming op het Werk. Inzake de aanbeveling tot aanstellen van een preventieadviseur, zie 'IX.2.9. Finaliseren van het arbeidsreglement' van dit activiteitenverslag.

8 VAST COMITÉ I, *Activiteitenverslag 2009*, 84 ('VIII.2.2. Een duidelijke, allesomvattende richtlijn inzake de informantenwerking').

9 VAST COMITÉ I, *Activiteitenverslag 2011*, 3.

tions relatives au traitement des sources humaines', waarin onder meer rekening werd gehouden met de door het Comité geformuleerde aanbevelingen.

Het Comité herhaalt evenwel dat de verplichting om richtlijnen uit te vaardigen inzake de werking met menselijke bronnen rust op de Nationale Veiligheidsraad (art. 18 W.I&V).

I.1.7. AANWIJZING VAN EEN PLAATSVERVANGEND BUITENGEWOON REKENPLICHTIGE

Verwijzend naar de aanbevelingen[10] van het Comité in het kader van zijn toezichtonderzoek naar het beheer, het gebruik en de controle van 'speciale fondsen'[11], werd door de VSSE een plaatsvervangend buitengewoon rekenplichtige aangewezen.

I.1.8. ALTERNATIEVEN VOOR DE AANWENDING VAN 'SPECIALE FONDSEN'

Het Comité stelde in zijn aanbevelingen[12] dat de ADIV voor bepaalde uitgaven waarvoor de speciale fondsen niet zijn bedoeld, op zoek moet gaan naar alternatieve financiering in samenwerking met andere diensten van Defensie. In 2015 kon de ADIV reeds voor een aanzienlijke bedrag materialen aankopen zonder daarbij te putten uit de 'speciale fondsen'.

I.1.9. KENNISOVERDRACHT WAARBORGEN

In het kader van de audit bij de VSSE, werd het waarborgen van de continuïteit in leidinggevende functies bestudeerd. Er kon worden vastgesteld dat de *tool* voor de kennisoverdracht tussen een uittredend personeelslid en diens opvolger beperkt bleef tot een taakomschrijving. Een globale reflectie over het optimaal organiseren van het behoud en het doorgeven van kennis vond nog niet plaats. Er werd dan ook aanbevolen in deze stappen te ondernemen.[13] In 2015 stelde de Dienst vorming en ontwikkeling een methode van kennisoverdracht ter beschikking van alle personeelsleden van de VSSE.

---

10 Zie 'IX.2.2. Aanbevelingen inzake het beheer van en de controle op de speciale fondsen' van dit verslag.

11 Zie 'II.2. Het beheer, het gebruik en de controle van de 'speciale fondsen''.

12 Zie 'IX.2.2. Aanbevelingen inzake het beheer van en de controle op de speciale fondsen' van dit verslag.

13 VAST COMITÉ I, *Activiteitenverslag 2009*, 83.

I.2. EEN HERNEMING VAN EERDERE AANBEVELINGEN

Artikel 35, 3° W.Toezicht geeft het Vast Comité I de opdracht verslag te doen aan het Parlement '*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*'. In dit kader herneemt het Comité jaarlijks een of meerdere aanbevelingen die het essentieel acht vanuit zijn dubbele finaliteit: de efficiënte werking van de diensten en het waarborgen van fundamentele rechten.

I.2.1. NADERE REGELS VOOR INTERNATIONALE GEGEVENSUITWISSELING EN SAMENWERKING

Het Vast Comité I blijft met klem herhalen dat er uitvoering moet worden gegeven aan de verplichtingen gesteld in de artikelen 19 en 20 W.I&V om de informatie-uitwisseling en de samenwerking van de Belgische inlichtingendiensten met andere – ook buitenlandse – overheden nader te regelen.[14] Zeker gelet op de noodzakelijke verregaande internationale samenwerking in de strijd tegen het terrorisme, is het gebrek aan dergelijke regeling niet langer aanvaardbaar. Het Comité vraagt nadrukkelijk aandacht voor deze delicate materie, in het bijzonder vanwege de Nationale Veiligheidsraad.

I.2.2. NADERE REGELS VOOR GEGEVENSUITWISSELING EN SAMENWERKING MET DE POLITIEDIENSTEN

Wat de nationale samenwerking betreft, beval het Comité eerder[15] 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 blijvende tekortkoming in ons veiligheidssysteem. Het Vast Comité I brengt dit, gezien het grote belang, opnieuw in herinnering.[16]

---

14 VAST COMITÉ I, *Activiteitenverslag 2010*, 3-4 en *Activiteitenverslag 2011*, 5-6. Deze aanbeveling werd ook steeds onderschreven door de Begeleidingscommissies. Hierover uitvoerig: VAST COMITÉ I, *Activiteitenverslag 2013*, 4-5 en *Activiteitenverslag 2014*, 5-6.

15 VAST COMITÉ I, *Activiteitenverslag 2011*, 112-113.

16 VAST COMITÉ I, *Activiteitenverslag 2006*, 135; *Activiteitenverslag 2007*, 77 en *Activiteitenverslag 2009*, 86.

I.2.3. INFORMATIEHUISHOUDING BIJ DE ADIV

Het Vast Comité I wil de aandacht vestigen op de aanslepende tekortkomingen in de informatiehuishouding van de ADIV. Reeds in november 2005 werden problemen gesignaleerd naar aanleiding van een toezichtonderzoek naar de wijze waarop de militaire inlichtingendienst de ingewonnen informatie beheert en exploiteert.[17] De ADIV kondigde aan dat de structuur van de dienst ingrijpend zou gewijzigd worden teneinde aan deze problematiek tegemoet te komen. Mede om die reden werd het thema 'informatiehuishouding' mee opgenomen in de in 2010 opgestarte audit. Daarin constateerde het Comité dat de inlichtingenwerkzaamheden niet (meer) voldoende werden ondersteund door ICT en wees het op evidente risico's die dit met zich brengt.[18] Diverse onderzoekverrichtingen die het Comité in 2014 en 2015 stelde in het kader van belangrijke onderzoeken[19], toonden echter opnieuw aan dat de manier waarop de informatie bij de ADIV wordt opgeslagen en beheerd, problematisch is. Het Comité beveelt dan ook met aandrang aan dat er dringend werk zou gemaakt worden van de uitbouw van de databanken van de ADIV (*input* van gegevens, eenduidige en algemene rubricering van gegevens, toegangsrechten vanuit verschillende divisies, informatisering van de papieren collecties, uitwerken van performante zoeksystemen…).

17 VAST COMITÉ I, *Activiteitenverslag 2008*, 77 ('II.11.2. Informatiehuishouding bij de militaire inlichtingendienst').

18 VAST COMITÉ I, *Activiteitenverslag 2011*, 12-13 ('II.1.5.2. Informatiehuishouding' en 'IX.2.1.3. Aanbevelingen inzake informatiestromen en ICT').

19 Onder meer naar de '*foreign terrorist fighters*' (II.11.2) en naar de aanslagen in Parijs (II.11.11).

HOOFDSTUK II
DE TOEZICHTONDERZOEKEN

In 2015 finaliseerde het Vast Comité I negen onderzoeksrapporten. Daarenboven stelde het op vraag van de Begeleidingscommissie twee aanvullende onderzoeksverslagen op en, op eigen initiatief, één tussentijds verslag.

Van de negen gefinaliseerde toezichtonderzoeken waren er twee geïnitieerd op eigen initiatief, twee op gezamenlijk initiatief van de Vaste Comités I en P (het betrof namelijk aspecten van de werking van het OCAD), drie na klacht en twee op verzoek van de parlementaire Begeleidingscommissie.

In wat volgt, worden de negen eindverslagen en het tussentijdse verslag (II.1 tot II.10) verkort weergegeven.

Daarna volgt een opsomming en een korte situering van de nog lopende onderzoeken (II.11). Onder deze laatste rubriek staan ook de acht in 2015 geopende toezichtonderzoeken vermeld. Van deze nieuwe onderzoeken werden er zes opgestart naar aanleiding van een klacht, één ambtshalve door het Comité en één op verzoek van de Begeleidingscommissie.

In totaal ontving het Comité in 2015 22 klachten of aangiften. Na verificatie van een aantal objectieve gegevens wees het Comité 14 van deze klachten of aangiften af omdat ze kennelijk niet gegrond waren (art. 34 W.Toezicht) of omdat het Comité onbevoegd was om de opgeworpen vraag te behandelen. In die laatste gevallen werden de klagers zo mogelijk doorverwezen naar de bevoegde instanties. De overige acht klachten uit 2015 gaven aanleiding tot het openen van zeven onderscheiden toezichtonderzoeken.

II.1. GEMEENSCHAPPELIJK TOEZICHTONDERZOEK NAAR DE *JOINT INFORMATION BOX* VAN HET OCAD

In september 2012 maakte een persbericht melding van het feit dat er zich problemen voordeden met de zogenaamde *Joint Information Box* (JIB).[20] Dit was een door het OCAD beheerde lijst met namen van personen en organisaties die een

[20] K. CLERIX, 'Sharia4Belgium helpt strijd tegen radicalisering', *MO* Magazine*, september 2012.

sleutelrol speelden in het radicaliseringsproces en ten aanzien van wie bepaalde administratieve of gerechtelijke maatregelen konden genomen worden. Het ging dus niet om een lijst met geradicaliseerde personen, maar wel radicaliserende personen of groepen. Wie op de lijst kwam, werd vanaf 2006 bepaald door de Nationale Task Force (NTF) die vertegenwoordigers groepeert van verschillende diensten die betrokken zijn bij de strijd tegen de radicalisering. Volgens het persbericht werd er binnen de NTF niet steeds voldoende samengewerkt bij het opstellen en actualiseren van de JIB. De Vaste Comités I en P openden hierop een toezichtonderzoek om na te gaan of dit instrument op een doelmatige en doeltreffende wijze bijdroeg tot de identificatie en de bekendheid van radicaliserende elementen bij alle betrokken overheden.[21] De Comités richtten zich daarbij op de JIB zoals die operationeel was vanaf 2009 tot 2014.[22]

II.1.1. HET ONTSTAAN VAN DE JIB

De JIB werd voor het eerst opgesteld in 2005. Het was een van de resultaten van het Actieplan Radicalisme (Plan R) uit 2004 waarin een overzicht werd geboden van de radicalisering binnen de Belgische samenleving en van de administratieve en gerechtelijke mogelijkheden om de problematiek aan te pakken. Aangezien het Actieplan gericht was op alle vormen van radicalisme (moslimextremisme, extreemlinks, extreemrechts en dierenrechtenactivisme) gold dit ook voor de JIB. In het Actieplan Radicalisme werden diverse 'assen' of kanalen onderscheiden die gebruikt worden om te radicaliseren: radio, televisie, gevangenissen, culturele centra … Het bestaan van die assen, zal ook doorwerken in de JIB.

Het opstellen van de JIB gebeurde aanvankelijk zonder concrete werkafspraken.[23] De lijst werd eerst korte tijd beheerd door de VSSE en nadien door de Antiterroristische Gemengde Groep (AGG). In 2006 gaat de AGG over in het OCAD; het coördinatieorgaan neemt vanaf dan het beheer over.

Wanneer in 2006 de Nationale Task Force wordt opgericht, krijgt deze als taak '*in te staan voor de coördinatie en opvolging van de inlichtingenvergaring met als doel de analyse van deze inlichtingen en het al of niet bepalen van de opname in de JIB.*' Maar het is wachten tot 2009 vooraleer er echte afspraken worden gemaakt.

---

21 Het onderzoek werd geopend op 13 november 2012 en gefinaliseerd in april 2015.

22 In de loop van het onderzoek gaf het OCAD te kennen dat zij de JIB-werking zou bijsturen. Een werkgroep binnen het OCAD formuleerde in dit kader diverse voorstellen. Het toezichtonderzoek werd echter afgesloten vooraleer de voorgenomen wijzigingen werden geïmplementeerd. Wel stelden de Vaste Comités I en P vast dat er een duidelijke intentie bestond om over een nieuw werkproces na te denken. Aan één van de door de Comités gesignaleerde tekortkomingen (een afwezigheid van een duidelijk omschreven finaliteit van de JIB) werd alvast gepoogd om tegemoet te komen. Voor het overige leverde het OCAD in haar reactie destijds geen andere elementen aan die de bevindingen van de Comités in vraag stelden.

23 Wel zou de nota tot oprichting van de JIB een aantal inhoudelijke en functionele werkingsmodaliteiten hebben vastgesteld.

Tot dan trachtten de diensten de materies, vermeld in het initiële Plan R, op te volgen, evenwel zonder duidelijke richtlijnen. Zij ondervonden daarbij tal van problemen.

II.1.2. DE WERKING VAN DE JIB VANAF 2009 TOT 2014

In 2009 kwamen de vertegenwoordigers van de betrokken diensten tot een formeel akkoord over de werking van de JIB. Wel werd geen eenduidige visie omtrent de doeleinden ervan verwoord. Dit werd door de meeste actoren als een belangrijk punt van kritiek naar voor gebracht en kon verklaren waarom er een verschil in visie bestond over de reikwijdte van de op te nemen personen of entiteiten.[24] Ook werd aangehaald dat de onderlinge verhouding met andere lijsten (zoals de actieplannen van de inlichtingendiensten, de lijst 'op te volgen groeperingen' en later de lijst 'Syrië-strijders') niet steeds even duidelijk was.

Sinds 2009 werd de opname of schrapping van een entiteit op of van de lijst onderworpen aan een duidelijke procedure waarbij strikte criteria (de zogenaamde 'parameters'[25]) werden gehanteerd én een waarbij consensus vereist was van alle betrokken diensten.[26] Dit alles zorgde ervoor dat de medewerking aan de JIB uitdraaide op een vrij formalistische activiteit die veel tijd in beslag nam.

De JIB zou werken rond de volgende zeven assen: 'Ideologen en predikers', 'Culturele centra en VZW's', 'Propagandacentra', 'Internet en web', 'Radio en televisie', 'Groeperingen' en 'Gevangenissen'. De leden van de NTF werden formeel aangeduid: het OCAD, de VSSE, de ADIV, de Federale en Lokale Politie, de Cel Antiterrorisme van de FOD Buitenlandse Zaken, de Algemene Directie Crisiscentrum (ADCC) en het Federaal Parket. Sommige van deze diensten werden als 'piloot' aangeduid van een of meerdere assen.[27]

Van elke entiteit die op de lijst terecht kwam, werd door het OCAD een fiche opgesteld met daarin alle[28] relevante informatie én de te nemen maatregelen. Wat betreft het aanleveren van informatie, wees het OCAD op markante verschillen. Zo was de bijdrage van de VSSE in de beginperiode beperkt. Wat betreft de te nemen maatregelen ten aanzien van een entiteit, viel bij de participanten te note-

---

24 Er circuleerden dan ook twee meningen: zij die de JIB beperkt wilden houden en zij die veel sneller entiteiten wilden toevoegen.

25 'Het oproepen tot gebruik van geweld' was bijvoorbeeld een parameter. De lijst van parameters was een poging om een noodzakelijke objectivering door te voeren, dit om een ondoordachte opname van een entiteit te verhinderen. Een entiteit moest beantwoorden aan minstens twee parameters.

26 Indien er na debat geen consensus werd bereikt over een voorstel tot opname, werd het toenmalige College voor inlichting en veiligheid hiervan op de hoogte gebracht.

27 Zo was de VSSE 'piloot' van vijf assen.

28 Opmerkelijk was dat voor sommige entiteiten veel informatie was opgenomen en voor andere zeer weinig.

ren dat hierover vaak een ernstig debat ontbrak. Sommige diensten stelden ook dat het hun taak noch expertise was om maatregelen voor te stellen.

Het opstellen en bewaren van de fiches kwam toe aan het OCAD.[29] Deze dienst zag het evenwel niet als zijn taak om de aangeleverde informatie te verrijken door analyses op te stellen of bijkomende informatie op te vragen. Het vulde zijn bijdrage vrij minimalistisch in, en dit ondanks zijn wettelijke opdracht om dreigingsanalyses op te stellen inzake extremisme.[30]

De diensten die hun medewerking verleenden aan de JIB konden de lijst en de opgenomen informatie niet rechtstreeks raadplegen. Zij krijgen aanvankelijk om de zes maanden (en nadien iets frequenter) via het OCAD uitgeprinte fiches of een CD-rom met de stand van zaken.

II.1.3. DE INHOUD VAN DE JIB IN 2014

De Vaste Comités I en P onderwierpen de inhoud van de JIB-lijst in september 2014 aan een controle. De lijst bevatte op dat ogenblik de namen van slechts 97 'entiteiten', waarvan ongeveer twee derde personen en één derde groeperingen.[31]

Het overgrote deel van de entiteiten was gelinkt aan de as 'Propagandacentra', gevolgd door de as 'Internet en web'.

Wat betreft de 'te nemen maatregelen' ten aanzien van de opgelijste personen, bleek dat ze allen geseind waren in het Schengen Informatie Systeem.[32] Veertien onder hen stonden ook geseind in de Algemene Nationale Gegevensbank (ANG); twee personen stonden in die ANG specifiek aangemerkt op het vlak van contraterrorisme. Voor het overige vermeldde de lijst amper 'te nemen maatregelen'. Het was voor de Comités ook niet steeds duidelijk op welke wijze de te nemen maatregelen het radicaliserend karakter van een persoon mee zouden kunnen inperken.

Dezelfde vaststellingen golden voor de in de lijst opgenomen groeperingen. Er was in hoofdzaak sprake van één maatregel, namelijk de 'opname op de lijst van te volgen groeperingen'. Deze lijst wordt beheerd door de Federale Politie onder verantwoordelijkheid van de minister van Binnenlandse Zaken. Het doel van deze lijst bestaat erin dat deze entiteiten met een bijzondere aandacht (moeten kunnen) worden gevolgd. Net zoals bij de personen, was het aantal vermelde

---

29 Het bewaren van de JIB-gegevens door het OCAD is wettelijk verankerd op basis van art. 9, §§ 1 en 2 W.OCAD.

30 Zie art. 8 W.OCAD.

31 Het was de Comités bovendien opgevallen dat bepaalde namen, waarvan redelijkerwijs kon worden aangenomen dat ze in de JIB thuishoorden, niet vermeld waren op de lijst terwijl andere namen dan weer niet leken te beantwoorden aan de finaliteit van de lijst.

32 Deze seiningen hebben tot doel de grensoverschrijdende verplaatsingen van een persoon binnen de Schengenzone te kunnen opvolgen. De meeste personen waren echter reeds geseind op het moment dat zij in de JIB werden opgenomen.

'andere maatregelen' ten aanzien van groeperingen beperkt. Ook hier was de meerwaarde van de JIB op het vlak van de strijd tegen radicalisering volgens de Comités zeer beperkt.

II.1.4. ALGEMENE CONCLUSIES VAN DE VASTE COMITÉS I EN P

De Comités stelden vast dat de samenwerking tussen de diverse diensten aan de JIB belangrijke positieve effecten kan ressorteren. Zo worden de diensten aangezet om elkaar op regelmatige en gestructureerde wijze te ontmoeten en operationele informatie uit te wisselen in het domein van de radicalisering. Ook worden zij aangezet om concrete gemeenschappelijke resultaten voor te leggen, te weten een lijst van radicaliserende elementen en daaraan gekoppelde maatregelen. De Comités waren echter van oordeel dat de wijze waarop de *Joint Information Box* ondanks twaalf jaar werking functioneerde, daartoe nog weinig had bijgedragen. De JIB bood evenmin veel meerwaarde in de strijd tegen de radicalisering.

De diensten zelf ervoeren de werking als tijdrovend en complex en de inspanningen en opbrengsten niet in verhouding. Dit had verschillende aanwijsbare oorzaken.

Vooreerst was er te veel onduidelijkheid over de exacte finaliteit van de lijst. De Comités waren van oordeel dat een lijst met personen en groeperingen die een radicaliserend effect hebben op hun omgeving en die het voorwerp dienen uit te maken van gecoördineerde administratieve, politionele en gerechtelijke maatregelen, waardevol is en dit zowel voor de veiligheidsdiensten als voor beleidsmakers. Deze finaliteit dient eenduidig te worden geformuleerd en gecommuniceerd aan alle betrokken actoren (weze het op federaal, gemeenschaps- of lokaal niveau). In functie van deze finaliteit dienen geobjectiveerde criteria te worden vastgesteld die de opname of schrapping op deze lijst regelen.

Ten tweede stelden de Comités vast dat de maatregelen die in de schoot van de JIB werden uitgewerkt ten aanzien van de gekende vectoren van radicalisering, marginaal waren. Het zoeken naar gepaste maatregelen bleef te veel achterwege. Maar de Comités wezen er ook op dat de diensten die deel uitmaakten van de JIB-werking niet steeds goed geplaatst zijn om desgevallend een breed scala aan maatregelen voor te stellen; hetzij omdat ze niet steeds de optimale kennis hebben over de mogelijke maatregelen, hetzij omdat zij mogelijk niet verantwoordelijk zijn voor de implementatie ervan.

II.2. HET BEHEER, HET GEBRUIK EN DE CONTROLE VAN DE 'SPECIALE FONDSEN'

In 2011-2012 werden door de gerechtelijke overheden twee strafonderzoeken opgestart naar het eventuele misbruik door inlichtingenagenten van gelden bestemd voor de vergoeding van informanten.[33] De Dienst Enquêtes I werd vanuit zijn gerechtelijke opdracht ingeschakeld in beide onderzoeken.[34] Gezien de elementen waarover het Vast Comité I kon beschikken op mogelijke structurele problemen wezen, werd begin september 2012 beslist een thematisch onderzoek te openen naar de wijze van beheer, besteding en controle van de fondsen bestemd voor de vergoeding van informanten van de VSSE en de ADIV.[35]

Gelet op de lopende strafonderzoeken, werd het toezichtonderzoek echter meteen opgeschort. Eind maart 2014 werd het onderzoek heropgestart. Het uitgebreide eindverslag werd goedgekeurd in juni 2015.

II.2.1. VOORWERP VAN HET ONDERZOEK

Zoals elke overheidsdienst, krijgen ook de inlichtingendiensten overheidsgeld toegekend voor de uitoefening van hun wettelijke opdrachten. De normale regel bij de besteding van die gelden is dat er volledige transparantie en controle moet zijn. Maar aangezien bepaalde taken van de VSSE en de ADIV onvoorzienbaar zijn of geheim moeten blijven, ontsnapt een deel van hun budget aan die 'normale regel'. Dat deel is beter gekend als de 'speciale fondsen'. Hoewel het bedrag van die fondsen dus deel uitmaakt van het budget dat aan de diensten wordt toegewezen, gelden er bijzondere regels voor het beheer, het gebruik en de controle ervan.[36]

Bij het begrip 'speciale fondsen' – dat overigens niet wettelijke gedefinieerd is – wordt in eerste instantie vaak gedacht aan gelden die bestemd zijn voor de vergoeding van informanten. Maar deze fondsen worden ook aangewend voor

---

33 Het eerste, dat in 2011 werd geopend, had betrekking op eventuele financiële malversaties door inlichtingenagenten van de ADIV. Dit onderzoek werd afgerond in 2013: de zaak werd geseponeerd. Het tweede onderzoek werd geopend in 2012 en had betrekking op eventuele financiële malversaties door een lid van de VSSE. De Dienst Enquêtes I rondde zijn onderzoek in dit dossier af in februari 2014.

34 VAST COMITÉ I, *Activiteitenverslag 2013*, 97-98 ('Hoofdstuk VI. De opsporings- en gerechtelijke onderzoeken').

35 In 1994 voerde het Vast Comité I reeds een toezichtonderzoek naar de budgetten van de Veiligheid van de Staat en de ADIV (Zie VAST COMITÉ I, *Activiteitenverslag 1995*, 105-109). Het onderzoek beperkte zich toen tot een beschrijving van het gebruik van de fondsen, de betrokken bedragen, het beheer en de controleprocedures.

36 Ook qua budgettaire planning wijken de 'speciale fondsen' af van die van de andere begrotingsrubrieken van overheidsdiensten omdat de bestemming van de fondsen niet moet worden gemotiveerd of beschreven op het ogenblik van de planning.

andere doeleinden. Het Comité besloot dan ook die andere aspecten mee op te nemen in het onderzoek.

In tegenstelling tot andere landen[37], bestaat er in België geen instantie die specifiek is belast met de controle op de speciale fondsen. In principe valt deze controle op de goede besteding van dit deel van de overheidsgelden dan ook onder de bevoegdheid van het Rekenhof. Maar gelet op het bijzondere en geheime karakter ervan, is deze controle niet echt effectief.[38] Er bestaan nochtans specifieke redenen die pleiten voor een degelijke controle op de besteding van die fondsen.[39]

Het Comité onderzocht onder meer welke de 'speciale fondsen' zijn, om welke bedragen het gaat en hoe ze worden verdeeld. Het controleerde ook de wijze waarop de middelen werden aangewend en hoe de wisselwerking verloopt tussen deze 'speciale fondsen' en de 'normale' budgetten. Ten slotte werd het reglementaire kader bestudeerd en onderzocht welke controlemechanismen er bestaan, en dit zowel intern (binnen de diensten) als extern (Rekenhof, Inspectie van Financiën, Vast Comité I…).

II.2.2. HET WETTELIJK KADER

Er bestaat geen wet, Koninklijk of ministerieel besluit, ministeriële omzendbrief of richtlijn[40] die de fondsen definieert en regels vastlegt voor het gebruik ervan en de controle erop. Op wettelijk vlak is er dus een leemte.

---

37 Bijvoorbeeld in Frankrijk, waar de '*Commission parlementaire de vérification des fonds spéciaux*' met deze opdracht werd belast.

38 De controle van de besteding van de speciale fondsen van de VSSE gebeurt door de directeur algemeen beleid van de minister van Justitie. Sinds 2006 wordt de controle van de speciale fondsen van de ADIV alleen uitgevoerd door het hoofd van de Krijgsmacht en dit vier maal per jaar. Op suggestie van het Rekenhof gebeurt dit sinds 2010 in aanwezigheid van de voorzitter van het Vast Comité I (VAST COMITÉ I, *Activiteitenverslag 2013, 95* en *Activiteitenverslag 2014*, 96).

39 *'There are four main reasons why external oversight of intelligence service finance is important:*
- *the principles of democratic governance require the allocation and use of public funds to be closely scrutinized;*
- *financial records can provide insights into the behaviour and performance of intelligence services;*
- *intelligence service secrecy limits the ability of the public to scrutinize service activity;*
- *the nature of intelligence work creates a variety of financial risks, including the risk of the misuse of public funds.'*

in A. WILLS, 'Financial Oversight in Intelligence Services', in *Overseeing Intelligence Services – a toolkit,* H. BORN en A. WILLS (eds.), DCAF, 2012 (www.dcaf.ch), 151-180.

40 Artikel 18 W.I&V bepaalt dat de diensten, in de uitoefening van hun opdrachten, gebruik mogen maken van menselijke bronnen *'overeenkomstig de richtlijnen van het Ministerieel Comité* (nu Nationale Veiligheidsraad)'. Deze richtlijnen zouden meer bepaald betrekking moeten hebben op het beheer en het doel van de speciale fondsen. Dergelijke richtlijnen ontbreken momenteel.

Wel hebben de twee diensten zelf richtlijnen uitgevaardigd over het gebruik van de fondsen. Alhoewel het Comité dit als positief beoordeelde, volstaan deze richtlijnen niet om een passend gebruik van de fondsen te garanderen. Meer fundamenteel was het Comité van mening dat het niet de taak van de diensten is om zelf te beslissen over de bestemming en het gebruik van de fondsen en over de controleprocedures. Uiteraard met dien verstande dat de diensten wel autonomie moeten genieten in het operationeel gebruik van de fondsen.

Het Comité kon vaststellen dat de personeelsleden van beide inlichtingendiensten die betrokken zijn bij het beheer van de fondsen op de hoogte zijn van deze interne richtlijnen. Dit gold echter niet noodzakelijkerwijs voor de agenten op het terrein, die slechts nu en dan gebruik maken van de speciale fondsen.

II.2.3. VASTSTELLINGEN TEN AANZIEN VAN DE ADIV

Anders dan voor de VSSE, worden de speciale fondsen die aan de ADIV worden toegekend, niet gedetailleerd in de jaarlijkse Begrotingswet die door het Parlement wordt gestemd. Maar ook het globale werkingsbudget van de ADIV (personeels-, werkings- en investeringskosten) is er niet in opgenomen. Alleen het globale Defensiebudget wordt vermeld. De bedragen die de ADIV uiteindelijk ontvangt voor zijn gewone kredieten en de 'speciale fondsen', worden toegekend door de Algemene Directie Budget en Financiën van Defensie.

Het Vast Comité I is van oordeel dat de transparantie van diensten gebaat is bij de publicatie van zowel het globale ADIV-budget als dat van de speciale fondsen, zonder daarbij details te geven over operaties, targets, gehanteerde methoden…[41] Het Comité wijst er op dat de publicatie van het bedrag van de aan de VSSE toegekende fondsen de geheime aard van haar activiteiten nooit in het gedrang heeft gebracht. De bekendmaking van deze cijfers moet het Parlement toelaten zijn rol van 'financieel controleur' beter op te nemen.

Zoals boven vermeld, heeft de ADIV diverse interne richtlijnen opgesteld voor het beheer van de fondsen. De basisrichtlijn geeft op duidelijke wijze aan onder welke voorwaarden de fondsen kunnen worden aangewend. Daarnaast bestaan er ook specifieke richtlijnen voor het gebruik van gelden uit zogenaamde 'subkassen'.[42] Sommige van die richtlijnen – zoals deze van de secties HUMINT – zijn uiterst gedetailleerd; voor andere 'subkassen' ontbreekt een dergelijke regeling. Wat betreft de organisatie van die laatste 'subkassen', heeft het Comité tekortkomingen vastgesteld. Tevens was het Comité niet overtuigd van de meerwaarde van de werking met 'subkassen'. Het gaf aanleiding tot verwarring en vergrootte aanzienlijk het risico op niet-conform gebruik van de toegekende fondsen. Zo

41 Zie in dezelfde zin: A. WILLS, *l.c.* 156 e.v.

42 De 'centrale kas' van de ADIV is onderverdeeld in een twintigtal 'subkassen' voor specifieke uitgaven.

kon het Comité vaststellen dat sommige uitgaven niet beantwoordden aan de vereiste criteria (bijvoorbeeld de vertrouwelijke of geheime aard van de opdracht en de hoogdringendheid als gevolg waarvan de gewone aankoopprocedure niet kon worden gevolgd). Andere uitgaven dienden dan weer te worden gedragen door andere budgetten en niet door de 'subkassen' (bijvoorbeeld de betaling van reglementair vastgestelde vergoedingen voor het burgerpersoneel van de ADIV). Wel heeft het Comité vastgesteld dat sommige secties van de ADIV (bijvoorbeeld de secties HUMINT of secties in operationele zones) over autonomie moeten beschikken om hun opdrachten uit te oefenen. Hiervoor is de terbeschikkingstelling van fondsen in contanten een absolute noodzaak. Maar voor de andere 'subkassen' was het Comité evenwel voorstander van een centralisatie van het beheer.

Het Comité stelde vast de ADIV de boekhouding betreffende het beheer van de fondsen ten tijde van het onderzoek niet als een beheerinstrument gebruikte. Met andere woorden, de boekhoudkundige gegevens dienden niet voor een doeltreffender en efficiënter beheer van de dienst.

Verder stelde het Comité vast dat de vormvoorwaarden van de uitgaveprocedures niet waren vastgelegd. De uitgaven waren onvoldoende gedocumenteerd zodat bij latere controles moeilijk kon worden vastgesteld of ze beantwoordden aan de richtlijnen. Daartoe is het immers noodzakelijk om de bestaansreden van de uitgave te kennen, welke instantie de beslissing tot aankoop heeft genomen en welke instantie de gegrondheid van de uitgave kan bevestigen.

Nog wat de 'subkassen' betreft, bleken de informatiseringsprogramma's om de boekhouding te voeren bewerkingen *a posteriori* toe te laten. Het Comité beval aan om ervoor te zorgen dat een ingevoerde boeking niet meer kon worden gewijzigd. Het Comité stelde ook vast dat voor sommige kassen een eigen boekhoudkundig systeem was ontwikkeld, dat niet compatibel was met dat van de centrale kas.

Een laatste vaststelling van het Comité had betrekking op de uitbetaling van menselijke bronnen. Zij ondertekenden geen ontvangstbewijzen voor de vergoedingen die ze ontvingen. De bronnen van de VSSE doen dit wel.

II.2.4. VASTSTELLINGEN TEN AANZIEN VAN DE VSSE

Zoals gezegd, is het bedrag van de speciale fondsen die aan de VSSE worden toegekend, zichtbaar in de begroting van deze dienst. Het staat vermeldt onder de rubriek 'beveiligingsmaatregelen' en bedroeg in 2013 ongeveer anderhalf miljoen euro. Wat betreft het beheer van dit budget, heeft de VSSE heldere en precieze richtlijnen voor haar personeel uitgewerkt.

Sinds 2014 maakt de VSSE gebruik van een 'elektronische kas'; dit is een informaticaprogramma dat dient om de boekhouding van de fondsen te voeren. Het is een efficiënt systeem omdat het de buitengewoon rekenplichtige toelaat om de boekhouding van de kassen door de secties permanent en rechtstreeks te contro-

leren. Het programma registreert de boekingen in *real-time* en kan naderhand niet meer worden gewijzigd, hetgeen een belangrijk element vormt om mogelijke fraude tegen te gaan.

De buitengewoon rekenplichtige heeft een belangrijke functie binnen de VSSE. Hij beheert de fondsen en controleert dagelijks het gebruik ervan. Het Comité moest evenwel vaststellen dat de fondsen niet optimaal werden beheerd tijdens de afwezigheid van de buitengewoon rekenplichtige. Het Comité was dan ook van oordeel dat het van wezenlijk belang is om de continuïteit van deze functie te garanderen. Zo moet in zijn vervanging worden voorzien bij zijn afwezigheid (hetgeen niet het geval was op het ogenblik van het onderzoek). Vanuit dezelfde bekommernis van continuïteit, oordeelde het Comité dat het noodzakelijk is om de werkingsprocedures van de buitengewoon rekenplichtige te beschrijven.

Ten slotte bleek uit het onderzoek dat de VSSE over een beperkt 'werkkapitaal' in contanten beschikte. Deze 'erfenis uit het verleden' was naar alle waarschijnlijkheid opgebouwd door jaarlijks een deel van de overschotten op de speciale fondsen over te boeken. Het Comité meende dat het bestaan van een dergelijk kapitaal een probleem kon vormen op het vlak van de wettelijkheid. Enerzijds omdat het jaarlijks overschot van de fondsen dat wordt bewaard om dit 'werkkapitaal' te verhogen werd geboekt als een uitgave. Anderzijds omdat de VSSE, zonder enige vorm van externe controle, elk jaar zelf bepaalde welk deel van dat overschot werd bijgehouden. Het Comité achtte het noodzakelijk om samen met de bevoegde instanties (FOD Justitie en Rekenhof) de wettelijkheid van dit 'werkkapitaal' te analyseren. Tevens zou moeten worden vastgelegd volgens welke procedures en controles de VSSE eventuele jaarlijkse overschotten van de fondsen kan bijhouden.

II.3. DE OPSPORING EN OPVOLGING VAN EXTREMISTISCHE ELEMENTEN BIJ HET PERSONEEL VAN DEFENSIE

In de loop van 2011-12 gaf de ADIV verschillende briefings aan het Vast Comité I over de problematiek van militairen die banden hebben met extreemrechts en met criminele motorbendes. In diezelfde periode verschenen er ook persartikels[43] over de aanwezigheid van extremistische, zelfs jihadistische militanten bij de Belgische Krijgsmacht. Het Vast Comité I besloot in juni 2012 dan ook om een toezichtonderzoek te openen naar de aanpak van deze problematiek door de ADIV.[44] Het Comité benaderde de thematiek vanuit vijf vragen.

---

43 P. HUYBERECHTS, *Het Nieuwsblad*, 22 november 2012 ('Leger vreest infiltratie door moslim-extremisten'); A. LALLEMAND, *Le Soir*, 22 november 2012 ('Des islamistes dans l'armée: 'L'Etat doit mieux se protéger').

44 Het eindverslag van het onderzoek werd goedgekeurd in november 2015.

II.3.1. WELKE REGELS GELDEN VOOR HET PERSONEEL VAN DEFENSIE WAT BETREFT DE FUNDAMENTELE VRIJHEDEN?

Elke militair en alle burgerlijke personeelsleden van Defensie genieten zoals eenieder de grondwettelijke rechten, meer bepaald de vrijheid van meningsuiting, van vereniging en van religie.[45] Verschillende bepalingen betreffende het statuut van het militair en burgerlijk personeel schrijven wel voor dat zij de Grondwet en de wetten moeten naleven en de morele en materiële belangen van de Staat moeten verdedigen. Specifieke nadruk wordt gelegd op de gevaren van lidmaatschap van een 'organisatie met een twijfelachtige reputatie'. 'Extremisme' op zich is dus niet verboden, maar bepaalde daden of uitingen van een extremistisch gedachtengoed, zowel binnen als buiten de professionele context, kunnen worden bestraft omdat ze in tegenspraak zijn met het tuchtstatuut, de deontologie en de militaire reglementen.

II.3.2. WAT IS DE BEVOEGDHEID VAN DE ADIV IN DEZE MATERIE?

De opvolging van extremistische activiteiten werd door de wetgever expliciet toegewezen aan de VSSE (artt. 7 en 8, 1°, c° W I.&V). Dat verhindert echter niet dat de ADIV op legitieme wijze extremisme bij militairen of burgerlijk personeel van Defensie zou opvolgen, althans voor zover zij een mogelijke dreiging vormen voor het departement of zijn werking. De ADIV is immers bevoegd voor alle dreigingen tegen de belangen die zij dient te verdedigen. Dit toezicht past dus binnen de wettelijke opdrachten van de ADIV, te weten het verzamelen van inlichtingen over activiteiten die het vervullen van de opdrachten van de Krijgsmacht kunnen bedreigen of het zorgen voor het behoud van de militaire veiligheid van het personeel en de installaties, of nog, het beschermen van militaire geheimen (art. 11 W.I&V).

De ADIV is daarnaast belast met het uitvoeren van veiligheidsonderzoeken met het oog op de toekenning van veiligheidsmachtigingen aan het personeel van Defensie én met het uitvoeren van veiligheidsverificaties op kandidaat-militairen.[46] Ook deze bevoegdheden zijn van belang in de strijd tegen het extremisme binnen Defensie (zie verder).

---

45 Zo was de ADIV bijvoorbeeld van oordeel dat het salafisme – in de zin van een strikte interpretatie van de islam – valt onder de vrijheid van godsdienst. Pas op het ogenblik dat een gelovige de rechten en plichten, erkend in internationale verdragen, in de Grondwet en in de nationale wetten verwerpt, kan er sprake zijn van extremisme en radicalisme.

46 Art. 9, eerste lid, 9° van de Wet van 28 februari 2007 tot vaststelling van het statuut van de militairen van het actief kader van de Krijgsmacht.

II.3.3. WIE BESCHOUWT DE ADIV ALS EXTREMISTISCH?

De ADIV heeft in zijn Inlichtingenstuurplan vier extremistische bewegingen geïdentificeerd die ze opspoort en opvolgt binnen Defensie: de radicale islam, extreemrechts, criminele motorbendes[47] en extreemlinks/ecopacifisme. Alleen de eerste drie bewegingen worden prioritair en in gelijke mate opgevolgd.

Uit de cijfers van de ADIV over de opvolging van deze drie fenomenen in het recente verleden, is gebleken dat er een vrij beperkt aantal individuen[48, 49] bij betrokken is of, in een uitzonderlijk geval, een kleine groep van personen. Bij de enkele in de media geciteerde gevallen ging het voornamelijk om oud-militairen die na hun legerdienst in de belangstelling zijn gekomen omwille van hun extremistische uitlatingen en/of omdat ze, gedreven door radicaal islamistische overtuigingen, in Syrië gingen vechten. Bij het afsluiten van het onderzoek was er echter geen enkel geval bekend van een militair in actieve dienst die een dergelijke stap zou hebben gezet. Er werden wél reeds militairen in actieve dienst strafrechtelijk veroordeeld voor hun lidmaatschap aan een extreemrechtse, terroristische groepering.[50] Tevens werd een beperkt aantal personen opgevolgd wegens extremistische overtuigingen (overigens geïnspireerd door verschillende ideologieën), maar er was daarbij geen enkel ernstig feit vastgesteld.

Het Comité oordeelde dat de omvang van de problematiek van extremisme binnen de Krijgsmacht in het algemeen vrij beperkt bleef en niet groter is dan het extremisme bij gelijkaardige bevolkings- en leeftijdscategorieën binnen de burgerlijke samenleving. Wel benadrukte het Comité dat het fenomeen niet mocht onderschat worden gezien de opdrachten die aan militairen worden toevertrouwd en de mogelijkheden waarover ze beschikken.

---

47 Strikt genomen valt het lidmaatschap van criminele motorbendes niet onder de wettelijke omschrijving van 'extremisme'. Dit neemt niet weg dat de ADIV deze materie kan opvolgen: dergelijke clubs hebben interesse voor de ervaring en technische kennis van militair personeel en voor het feit dat ze toegang hebben tot bewapening en ander militair materiaal. In die zin kunnen ze een bedreiging vormen voor de door de ADIV te verdedigen belangen (zie II.3.2).

48 In het kader van de radicale islam hebben in de periode 2010-12 een dertigtal personen de aandacht getrokken van de ADIV. Drie onder hen stonden onder verscherpt toezicht wegens het actief bedrijven van religieus proselitisme binnen de Krijgsmacht. In 2013-'14 werden eveneens een dertigtal gevallen onderzocht. Dertien militairen werden in meerdere of mindere mate opgevolgd. In 2015 alleen werd een vijftigtal gevallen onderzocht. Vier personen bleken actief betrokken bij de radicale islam.

49 Wat betreft militairen met extreemrechtse banden, waren volgende cijfers beschikbaar: in 2006-'07 hadden 76 actieve militairen vermoedelijk banden met een extreemrechtse beweging. Tussen 2010 en 2012 werd geen enkel nieuw geval vastgesteld. In 2013 en 2014 onderzocht de dienst twee gevallen.

50 In 2014 werden veertien leden van de neo-nazigroepering *Bloed, Bodem, Eer en Trouw,* waaronder zich elf militairen bevonden, veroordeeld voor racisme en negationisme. Een aantal beklaagden werd ook schuldig bevonden aan terrorisme, bendevorming en illegaal wapenbezit.

II.3.4. OP WELKE MANIER VOLGT DE ADIV EXTREMISTISCHE ELEMENTEN BINNEN DEFENSIE OP?

Extremistische militairen worden op verschillende manieren opgespoord en opgevolgd.

Vooreerst is er de veiligheidsverificatie waaraan elke kandidaat-militair onderworpen wordt. Deze screening, die gebeurt door de ADIV, heeft blijkens de voorbereidende werken bij de wet tot doel om kandidaten met een extremistisch en/of gerechtelijk verleden uit de selectie te weren.

Eens aangeworven, worden veel militairen én leden van het burgerpersoneel (met name zij die een veiligheidsmachtiging behoeven) onderworpen aan een veiligheidsonderzoek. Ook dit onderzoek – dat diepgaander is dan de verificatie en minstens om de vijf jaar herhaald dient te worden – kan extremisme aan het licht brengen. De ontdekking van omstandigheden die de betrouwbaarheid van een persoon kunnen aantasten (zoals extremistische connecties), kan leiden tot de weigering of intrekking van een veiligheidsmachtiging.

Buiten de context van veiligheidsverificaties en -onderzoeken, doet de ADIV een beroep op de eenheden, hun korpschefs en de dienstverantwoordelijken om verdachte handelingen te detecteren en te melden.[51] De resultaten van deze informatiebronnen variëren naargelang de kwaliteit van de persoonlijke contacten die de onderzoekers van de ADIV hebben opgebouwd met de eenheidscommandanten. Zo heeft het Comité moeten vaststellen dat in de praktijk relevante feiten en veiligheidsincidenten vaak pas onder de aandacht van de ADIV worden gebracht op het moment dat de betrokkene aan een nieuw veiligheidsonderzoek wordt onderworpen en dus niet op het moment dat de feiten of incidenten zich voordoen. Onderzoek van meerdere concrete gevallen heeft ook aangetoond dat het nuttig zou zijn mochten het personeel van de ADIV en de militaire eenheden beschikken over beter uitgewerkte indicatoren om verdachte situaties tijdig te herkennen.

Naast 'interne' informatie, ontvangt de ADIV ook informatie en inlichtingen van andere openbare overheden, met name van de politie, de gerechtelijke overheden en de VSSE. Dit gebeurt echter niet systematisch.

Ten slotte kan de ADIV het initiatief nemen om een inlichtingenonderzoek te voeren wanneer het kennis krijgt van aanwijzingen van verdacht gedrag. Er dient op te worden gewezen dat het niet toegelaten is op een systematische en algemene

[51] De richtlijn 'Lidmaatschap bij organisaties met een slechte of bedenkelijke reputatie' van de Algemene Directie Human Resources vraagt alle korpschefs om de ADIV op de hoogte te brengen indien ze een personeelslid verdenken van activiteiten die de militaire veiligheid in gevaar kan brengen. In 2013-'14 heeft de ADIV een campagne gevoerd om korpschefs te informeren en bewust te maken over de problematiek van motorbendes met een bedenkelijke reputatie. Er werden briefings gegeven en er werd een informatienota verspreid.

wijze alle personeelsleden van Defensie te verifiëren, los van enige aanwijzing.[52] Het Comité wees er op dat dergelijke mogelijkheid op het ogenblik van het onderzoek ook niet gerechtvaardigd leek.

Hoewel het onderzoek van het Comité heeft aangetoond dat de ADIV zijn opdracht in deze met ernst vervult, moest het vaststellen dat de opvolging van het extremisme niet voldoende gedocumenteerd en becijferd werd. Dat was gedeeltelijk te verklaren door de tussenkomst van meerdere divisies en subdivisies. Om de problematiek optimaal te kunnen beheren, is vereist dat de ADIV beschikt over een algemeen en *up-to-date* beeld van de situatie.

II.3.5. WELKE MAATREGELEN KUNNEN WORDEN GENOMEN?

Op basis van een voorafgaande verificatie door de ADIV kan een kandidaat-militair, zoals gezegd, worden uitgesloten van de selectieprocedure. Hierbij moet worden opgemerkt dat het aantal kandidaat-militairen die worden uitgesloten wegens extremisme, zeer laag is. Bij de meeste negatieve adviezen ligt doorgaans 'gewone' criminaliteit aan de basis, zoals bijvoorbeeld het gebruik van verdovende middelen.

De personen die geen veiligheidsmachtiging bekomen of van wie de machtiging wordt ingetrokken omwille van extremistische activiteiten, verliezen hun statuut van militair of burgerpersoneel niet; zij zullen alleen kunnen geweerd worden uit functies waarvoor een dergelijke machtiging vereist is. Ook mogen de gegevens die werden verzameld in het kader van een veiligheidsonderzoek niet gebruikt worden voor andere doeleinden (bijvoorbeeld tuchtzaken).

Het spreekt voor zich dat medewerkers van Defensie die zich schuldig maken aan door extremisme ingegeven misdrijven of tuchtfeiten, kunnen worden geschorst, overgeplaatst, ontslagen…[53] De ADIV draagt geen verantwoordelijkheid voor deze administratieve en tuchtrechtelijke maatregelen; de dienst wordt er ook niet altijd op de hoogte van gebracht.[54]

II.3.6. ALGEMENE CONCLUSIE

Het Vast Comité I concludeerde dat de ADIV het extremisme binnen Landsverdediging correct en vrij doeltreffend opvolgde. Het onderzoek toonde aan dat

---

52 Dergelijke systematische algemene screening is alleen mogelijk in het kader van de aanwervingsprocedure.

53 Wanneer een persoon niet langer lid is van Defensie zal de ADIV de opvolging beëindigen, tenzij deze nog contacten onderhoudt met oud-collega's bij Defensie.

54 Zo bijvoorbeeld stelde de ADIV dat het geen *feedback* had gekregen over het feit dat Defensie in een bepaalde periode vier extremisten had ontslagen. Zie over deze ontslagen: *Hand*. Kamer 2012-13, 17 januari 2013, CRIV53PLEN125, 1442-1444.

gevaarlijke situaties op tijd werden opgespoord, maar dat er zich tot op heden weinig of zelfs geen gevallen voordeden van personen die zich tijdens hun dienst onopgemerkt hebben ontpopt tot gevaarlijke extremisten. De angst voor extremistische militairen of personen die vanuit een extremistische overtuiging een militaire training volgen, blijkt in de praktijk minder gegrond te zijn dan bepaalde media deden vermoeden.

II.4. DE OPVOLGING VAN SYRIËSTRIJDERS DOOR DE TWEE BELGISCHE INLICHTINGENDIENSTEN: EEN TUSSENTIJDS VERSLAG

Sinds 2013 oefent het Syrische strijdtoneel een grote aantrekkingskracht uit op de zogenaamde *foreign terrorist fighters* (FTF)[55] vanuit de hele wereld. Feit is dat daarbij – zeker verhoudingsgewijs – veel personen uit België afkomstig waren. Vandaar dat het Vast Comité I in oktober 2014 (en dus voor de aanslagen van 2015 in Frankrijk en België) besloot een toezichtonderzoek te openen naar '*de informatiepositie van de twee inlichtingendiensten (ADIV en VSSE) over de rekrutering, de zending, het verblijf en de terugkeer in België van jongeren (van Belgische en andere nationaliteiten die in België verblijven) die vertrekken of vertrokken zijn naar Syrië of Irak en aangaande de uitwisseling van inlichtingen met diverse overheden.*'[56] Het onderzoek moest een antwoord bieden op de volgende vragen: hoe volgen de inlichtingendiensten de problematiek op, hoe hebben zij zich georganiseerd en wat is hun informatiepositie? Het toezichtonderzoek omvatte de periode vanaf 2012 – op dat ogenblik doken immers de eerste berichten op over de zogenaamde '*returnees*' (naar hun land van oorsprong teruggekeerde strijders) – tot 2015.

Begin 2015 werd een eerste, tussentijds rapport opgesteld ten behoeve van de Begeleidingscommissie. Hierna worden de voorlopige conclusies van dat verslag weergegeven.[57]

Het Comité wil er op wijzen dat de uitdagingen waarvoor de (Belgische) inlichtingendiensten in deze materie zijn gesteld, zeer groot zijn. Vanzelfsprekend hebben deze diensten in het verleden ook op bepaalde 'crisissen' moeten reageren. Maar de reële impact op hun organisatie was in die gevallen hoe dan ook beperkt.

---

55 Aanvankelijk werd er niet gesproken over FTF. Er was eerder sprake van *Belgian freedom fighters* (die vertrokken naar Irak, Syrië… vanuit een humanitaire achtergrond) of – later – van *Belgian foreign fighters* (met militaire doelstellingen).

56 Het Vast Comité I voerde reeds eerder onderzoek naar gelijkaardige materies. In 1999 werd onderzocht hoe de inlichtingendiensten de dreiging die uitging van het GIA opvolgde (VAST COMITÉ I, *Activiteitenverslag 2001*, 89 e.v.). En in 2007 werd de opvolging van het radicaal-islamisme door de inlichtingendiensten belicht (VAST COMITÉ I, *Activiteitenverslag 2007*, 9 e.v.). Daarin werd onder meer aandacht besteed aan de opvolging door de VSSE en de ADIV van de *filières* die tot doel hadden jihad-strijders te rekruteren voor zogenaamde 'gevoelige zones' (Afghanistan, Pakistan, Irak…).

57 Het onderzoek werd afgesloten in februari 2016.

Het huidige fenomeen is van een andere orde: het is bijzonder complex, de dreiging heeft zich in een ongezien snel tempo ontwikkeld, er zijn een uitzonderlijk groot aantal personen bij betrokken én het is *quasi* wereldwijd vertakt.

II.4.1. DE GEOPOLITIEKE CONTEXT EN DE PRIORITEITEN VAN DE VSSE EN DE ADIV

Vanaf december 2010 ging er een golf van protesten, opstanden en revoluties doorheen de gehele Arabische wereld; de zogenaamde 'Arabische Lente' was aangebroken. Er waren revoluties in Tunesië, Egypte, Libië en Jemen, een burgeroorlog in Syrië, demonstraties en protesten in Bahrein, Jordanië, Marokko, Algerije, Irak, Oman en de Palestijnse gebieden en incidentele protesten in Mauritanië, Saoedi-Arabië, Soedan, Libanon en Koeweit. De oorzaken verschilden van land tot land: onderdrukking, oneerlijk verlopen verkiezingen, corruptie, prijsstijgingen, gebrek aan politieke vrijheid en werkloosheid. Telkenmale werden de zittende regeringen verantwoordelijk gesteld.

De regio was reeds langer het toneel van geweld, zeker in Irak waar sinds oktober 2006 de organisatie 'Islamitisch Staat in Irak' actief was. Deze mengde zich in de Syrische burgeroorlog. Later nam deze organisatie de naam 'Islamitische Staat in Irak en Syrië' (ISIS) of ook nog 'Islamitische Staat in Irak en de Levant' (ISIL) aan. In juni 2014 claimde Abu Bakr al-Baghdadi een nieuw wereldwijd kalifaat te hebben opgericht, waardoor hij zowel de religieuze als de burgerlijke macht tot zich trok. Sindsdien is de terreurbeweging gekend onder de naam Islamitische Staat (IS) of DAESH.

Veel van de jongeren die vanuit België en andere landen de weg naar Syrië en Irak vonden, sloten zich aan bij IS; anderen kozen voor andere gewapende groeperingen die tegen het regime van de Syrische president Assad vochten of die in onderlinge conflicten verwikkeld waren.

Het bestaan en de werking van zogenaamde '*filières*' vanuit België naar conflictgebieden in het buitenland was niet nieuw voor de VSSE. Reeds vanaf 2001 werd de aandacht van de dienst getrokken door het probleem van de Iraakse en Afghaanse *filières*.[58] De VSSE kreeg bijvoorbeeld te maken met de *moedjahedien* die naar Afghanistan vertrokken om er deel te nemen aan paramilitaire opleidingen of aan gevechten. Ook de problematiek van de terugkeer van deze personen en het gevaar dat ze hier netwerken zouden opstarten, was gekend ten tijde van de Irak-crisis. In 2005-'06 vormden deze *filières* een van de prioriteiten van de Veiligheid van de Staat. Ook in de jaren nadien werd de problematiek blijvend opgevolgd. De *filières* vanuit België naar buitenlandse strijdtonelen mochten dan al goed gekend zijn, toch belette dit niet dat de VSSE in 2011 niet kon voorspellen dat de *filière* naar Syrië zou uitgroeien tot een topprioriteit. In dat jaar had de

58 VAST COMITÉ I, *Activiteitenverslag 2007*, 21-22.

VSSE in zijn Activiteitenverslag wel aandacht voor de uitdijende volksopstand in Syrië, maar wat de *filières* betreft, noteerde de Veiligheid van de Staat *'dat de Europese kandidaat-strijders die op het punt staan te vertrekken, zich op […] conflictgebieden zullen richten, zoals meer bepaald Somalië en Jemen"*. En verder: *'zelfs al wordt België meestal niet rechtstreeks bedreigd, toch wordt het grondgebied beschouwd als een doorreisplaats […]. De geregelde passages van islamitische radicalen via België kunnen door verschillende factoren worden uitgelegd, waaronder de […] aanwezigheid van netwerken die documenten vervalsen, maar ook de geografisch centrale ligging van ons land in Europa en de aanwezigheid van de lagekost-luchtvaartmaatschappijen'*. Midden 2012 maakte de dienst melding van een eerste geval van een '*returnee'* en in het *Actieplan 2013* was de problematiek *as such* voor het eerst aan de orde. Sindsdien komt de Syriëproblematiek uiteraard veel explicieter aan bod in de Actieplannen van deze dienst.

Ook de ADIV was al langer vertrouwd met het fenomeen van *filières*. In 2007 verklaarde de dienst weliswaar nog dat hij, bij gebrek aan personeel én aan *input*, geen bijzondere aandacht besteedde aan de verplaatsingen van personen naar gevoelige zones (Pakistan en Afghanistan). De dienst oefende naar eigen zeggen geen stelselmatige controle uit op het fenomeen, maar ontving hierover van tijd tot tijd informatie uit het buitenland.

Er bestaan bij de ADIV twee stuurplannen waarin de jaarlijkse prioriteiten worden vastgelegd. Het stuurplan van de Divisie Veiligheidsinlichtingen is vooral op de binnenlandse (militaire) fenomenen[59] en bedreigingen gericht; dat van de Divisie Inlichtingen op de buitenlandse bedreigingen. De thematiek van het transnationaal jihadisme en de radicale islam is over de jaren heen weliswaar steeds opgenomen in de twee stuurplannen, maar de Syrië-problematiek kwam pas in 2013 uitdrukkelijk aan bod in het stuurplan van de Divisie Inlichtingen. Het is vooral deze afdeling die de problematiek van de '*foreign fighters*' en de '*returnees*' opvolgt. Ze speelt daarbij vooral een belangrijke rol in de contextualisering van het fenomeen in de betrokken regio's. Dit kwam overigens tegemoet aan de opdracht die de ADIV toebedeeld kreeg bij de Omzendbrief van 25 september 2014 betreffende het informatiebeheer en de maatregelen voor de opvolging van de '*foreign fighters*' die in België verblijven.[60] Om het fenomeen 'terrorisme' op een globale manier aan te pakken, bracht de ADIV personeelsleden van deze twee divisies samen in een *Joint Cell*. Zoals gezegd, bestudeerde de ADIV de Syrië-problematiek

[59] Binnen deze Divisie speelt ook de afdeling die zich bezig houdt met 'Veiligheid' (d.i. de vroegere Divisie S) een rol in het kader van het opvolgen van het fenomeen 'extremisme', maar dan specifiek binnen Defensie. Ze moet personeelsleden detecteren die door hun lidmaatschap van of hun toenadering tot extremistische (jihadistische) groeperingen of ideologieën een veiligheidsrisico kunnen vormen voor Defensie (Zie ook Hoofdstuk II.3 in verband met extremisme in het leger).

[60] Deze omzendbrief werd vervangen door de Omzendbrief van de ministers van Binnenlandse Zaken en Justitie van 21 augustus 2015 betreffende de informatie-uitwisseling rond en de opvolging van de foreign terrorist fighters afkomstig uit België. Daarin staat deze opdracht niet langer vermeld.

vooral vanuit een brede, geopolitieke context. Het oprichten van deze *Joint Cell* waar zowel de meer binnenlands gerichte aspecten als de buitenlandse ramificaties van het probleem aan bod komen, vormde daar een uiting van.

II.4.2. HET WERKVOLUME EN HET INGEZETTE PERSONEEL EN MIDDELEN: EEN EERSTE BEOORDELING

Het Comité stelde vast dat de Syriëcrisis een zeer grote impact heeft gehad op de werking van de VSSE. De kwantitatieve indicatoren inzake werkvolume (met name in- en uitgaande informatiestromen en het aantal ingezette bijzondere inlichtingenmethoden) lieten een zeer sterke stijging zien. Dit werkvolume werd echter niet opgevangen door een numerieke versterking van de diensten. Het werd opgevangen door interne verschuivingen, door een heroriëntering van medewerkers naar de Syriëproblematiek, of nog, door het opbouwen van overuren. Het stijgend werkvolume zorgde voor problemen. Het geheel van de materies die de VSSE moet opvolgen, kon immers in de verdrukking komen. De werkdruk was voor de rechtstreeks betrokken personeelsleden groot. Alhoewel het Vast Comité I kon vaststellen dat de betrokken afdelingen en personen hun taak met ijver en enthousiasme uitvoerden, beoordeelde het deze situatie als risicovol en niet stabiel. Ze vergde structurele oplossingen. Verder wees het Vast Comité I op een specifieke lacune: openstaande kaderfuncties werden niet systematisch ingevuld. Hieraan diende verholpen te worden.

Net zoals bij de VSSE, steeg het werkvolume bij de ADIV aanzienlijk.[61] Dit werd deels ondervangen door interne verschuivingen. Het Comité stelde ook vast dat de ADIV sinds 2010 heel wat projecten heeft opgestart (onder andere inzake CYBERHUMINT, HUMINT, OSINT en SOCMINT) om zijn informatiepositie inzake het internationale terrorisme te verbeteren. De problematiek van de Syriëcrisis en de *Belgian foreign fighters* maakte daar uiteraard deel van uit. Het Comité achtte het aangewezen om de voortgang van deze projecten te monitoren.

II.4.3. DE INVLOED OP DE ORGANISATIE EN DE STRATEGIE: EEN EERSTE BEOORDELING

Het Vast Comité I was van mening dat het Syriëdossier niet alleen voor de rechtstreeks betrokken diensten van de VSSE een belangrijk sleutelmoment vormde, maar ook voor de inlichtingendienst in zijn geheel. Er waren aanwijzingen dat het

[61] In dit eerste tussentijdse verslag beperkte het Comité zich voornamelijk tot de bespreking van de opvolging van de Syriëproblematiek vanuit 'binnenlands oogpunt'. Dit betekende dat wat betreft de ADIV nog geen rekening werd gehouden met de inspanningen van de Divisie Inlichtingen, die vooral in het buitenland actief is.

Syriëdossier als katalysator fungeerde voor veranderingen in de hele organisatie. Zo bijvoorbeeld werd er een aanvang genomen met het formuleren van een nieuwe strategie die tot structurele wijzigingen moest leiden. Daarbij ging het om de strategie op zich (bepalen welke materies meer of minder aandacht kunnen krijgen) maar ook om de transitie van de situatie op heden ('*as-is*') naar de gewenste toekomstige situatie ('*to-be*'). Dergelijke transitie is meer dan het 'eenvoudigweg' verschuiven van structuren en personeel; het raakt ook aan de kern van het inlichtingenwerk, met name het opbouwen van informatieposities in bepaalde materies. Dit vergt meestal vele jaren en vereist een hoge specialisatie. Dit betekent dat er op lange termijn moet worden gedacht aangezien een materie die vandaag minder belangrijk lijkt, morgen een prioriteit kan worden.

De ADIV van zijn kant poogde reeds een aantal jaren de problematiek van het (internationaal) terrorisme op thematische wijze te benaderen. Mede met het oog daarop, werd de analysecapaciteit inzake terrorisme van de Divisie Inlichtingen en van de toenmalige Divisie Counter-intelligence in 2010 samengevoegd tot één bureau. In 2013 bracht een doorlichting van de werking van dit bureau onvolkomenheden aan het licht. Daarom voerde de ADIV in 2014 een reorganisatie door en vormde het bureau om tot een *Joint Cell*. Het Vast Comité I besloot dat de ADIV daarmee over een structuur beschikt die het radicalisme, terrorisme en de *filières* bestudeert en opvolgt. Maar het Comité voegde daar aan toe dat deze gemeenschappelijke cel voor belangrijke uitdagingen stond: duidelijke aansturing, verschillende databases, personeel dat niet vervangen wordt …

II.5. DE PERSONEELSLEDEN VAN DE INLICHTINGENDIENSTEN EN DE SOCIALE MEDIA

De voorbije jaren hebben sociale netwerken zoals Facebook, LinkedIn en Netlog een enorme ontwikkeling doorgemaakt, met vandaag wereldwijd een gigantisch aantal gebruikers tot gevolg. Sindsdien maken sociale netwerkendiensten (SND) deel uit van het dagelijkse leven van zeer veel mensen.

In november 2012 verscheen er in de Belgische pers informatie volgens dewelke personeelsleden van de Belgische inlichtingendiensten hun beroepshoedanigheid zouden hebben meegedeeld op die sociale netwerken.[62] Dit zou niet zonder risico zijn: een medewerker van een inlichtingendienst die zijn of haar hoedanigheid kenbaar maakt, stelt zich immers bloot aan bedreigingen of aan

[62] N. VAN HECKE, *De Standaard,* 26 november 2012 ('*Belgische spionnen online te vinden*'); X., *7sur7.be*, 26 november 2012 ('*Des espions belges s'exposent sur le net*'); K. VAN EYKEN, *Het Laatste Nieuws*, 26 november 2012 ('Belgische spionnen online te vinden'). De informatie werd zelfs overgenomen door de internationale pers: C. DEWEY, *The Washington Post*, 26 november 2012 ('Belgian intelligence workers outed on Facebook, LinkedIn); X., *Voix de la Russie*, 27 november 2012 ('*Les espions belges se sont déclassifiés sur les réseaux sociaux*').

toenaderingspogingen vanwege buitenlandse diensten, aldus een anonieme bron uit de inlichtingenwereld.

Op vraag van de toenmalige Begeleidingscommissie in de Senaat, opende het Comité in december 2012 een onderzoek. De Senaat wenste immers nadere informatie over de omvang van het fenomeen, de risico's die er aan verbonden zijn en de maatregelen die kunnen worden getroffen.[63] Het onderzoek werd afgerond in april 2015. De resultaten werden in juli 2015 besproken binnen de nieuwe Begeleidingscommissie in de Kamer. Uit die bespreking bleek dat de Parlementsleden een aantal bijkomende gegevens wensten te bekomen. Het Comité voerde daarom een aanvullend onderzoek. Hierin ging het onder meer na of de twee inlichtingendiensten dwingende richtlijnen hadden uitgevaardigd over de problematiek en welke acties ze hadden ondernomen ten aanzien van personeelsleden die actief waren op SND en wat er met hun profielen was gebeurd. Tevens wenste de Begeleidingscommissie te weten of het wettelijk mogelijk was om personeelsleden van inlichtingendiensten – zelfs in de privésfeer – te verbieden om actief te zijn op SND. Wat dit laatste aspect betreft, won het Vast Comité I het advies in van de Privacycommissie.[64] Het aanvullend onderzoek werd afgesloten in december 2015.

De resultaten van het initiële en het aanvullende onderzoek worden hieronder samen weergegeven.

II.5.1. DE OMVANG VAN HET FENOMEEN

De VSSE verklaarde dat het kort na de persberichten uit 2012 gecontroleerd had of bepaalde medewerkers hun hoedanigheid kenbaar hadden gemaakt op LinkedIn. Dit zou volgens de VSSE niet het geval zijn geweest. De VSSE kon dezelfde *check* niet uitvoeren voor Facebook omdat ze toen nog niet over een profiel beschikte dat toegang gaf tot de profielen van de gebruikers.

Ook de ADIV verklaarde geen weet te hebben van gevallen waarbij leden van hun personeel zonder toelating[65] ruchtbaarheid zouden hebben gegeven aan hun hoedanigheid. Zij controleerden daarbij vier sociale netwerkdiensten.

In 2014 voerde het Comité zelf een beperkte controle uit op LinkedIn. Het identificeerde daarbij de namen van 17 personen die zich kenbaar maakten als

---

63 De Senaat wou de problematiek ook laten onderzoeken voor het personeel van het OCAD. Hiervoor werd een gemeenschappelijk toezichtonderzoek opgestart met het Vast Comité P (zie Hoofdstuk II.6).

64 Zie Advies nr. 45/2015 van 13 november 2015 met betrekking tot de adviesaanvraag van de Comités I en P met betrekking tot de mogelijkheid om de leden van de inlichtingendiensten en het OCAD te verbieden om, zelfs privé, actief te zijn op de sociale netwerken (www.privacycommission.be/nl/adviezen-cbpl?page=2).

65 Voor sommige functies is het uiteraard evident dat de hoedanigheid kenbaar wordt gemaakt (bijvoorbeeld het diensthoofd, de contactpersonen voor aanwervingen en de vakbondsvertegenwoordigers).

lid van een van beide diensten. Desgevraagd bevestigde de VSSE dat vijf actieve en twee gewezen leden van haar dienst actief waren op LinkedIn én er melding maakten van hun (voormalige) hoedanigheid.[66, 67] Vier personen deden zich voor als leden van de dienst, zonder dat ze dat ooit waren geweest. Wat betreft de ADIV, bleken zes actieve en twee gewezen leden van de dienst actief op deze SND. Niet al deze personen identificeerden zich echter expliciet als lid van ADIV; ze stelden zich veeleer voor als leden van Defensie. Niettemin kon hun functie worden opgemaakt uit gegevens die ze op het netwerk publiceerden. Deze twee gewezen medewerkers gingen daarbij zo ver dat ze ook gevoelige gegevens prijsgaven.[68]

Wat betreft 'de omvang van het fenomeen', besloot het Comité enerzijds dat het zeer beperkt is en anderzijds dat de diensten er mettertijd een beter zicht op hebben gekregen. Beide diensten gaven wel toe dat het moeilijk is om precies te weten hoeveel van hun agenten actief zijn op SND. Zoals vermeld, kon de VSSE het fenomeen oorspronkelijk zelfs niet controleren omdat ze geen profiel bleek te hebben op de betrokken netwerken.

II.5.2. RISICO'S VERBONDEN AAN HET GEBRUIK VAN SOCIALE NETWERKDIENSTEN

Uiteraard zijn er 'algemene' risico's verbonden aan het gebruik van SND, zoals een inbreuk op de privacy of een mogelijks misbruik van persoonlijke gegevens. De Senaat wenste echter geïnformeerd te worden over de risico's die specifiek gelden voor de betrokken agenten en de dienst waarvan ze deel uitmaken.

De VSSE noch de ADIV bleken een analyse te hebben gemaakt van de specifieke risico's die verbonden zijn aan het fenomeen.[69] Dat dergelijke risico's bestaan is nochtans evident: gevoelige of geclassificeerde informatie kan (ongewild) gecompromitteerd worden; vreemde diensten kunnen op basis van een analyse van persoonlijke gegevens trachten om Belgische agenten te rekruteren; de internet-identiteit kan overgenomen worden en leiden tot het publiceren van valse

66 Er werden nog andere leden van de VSSE aangetroffen op dit netwerk. Zij maakten echter geen gewag van hun hoedanigheid.

67 Wanneer het profiel van een VSSE-medewerker rechtstreeks of onrechtstreeks verwijst naar de dienst, wordt de betrokkene gevraagd (hij wordt hiertoe dus niet formeel verplicht) de bewuste verwijzing uit zijn profiel te verwijderen, aldus de VSSE. Het incident zou wel worden opgenomen in het veiligheidsdossier van de betrokken agent.

68 Desgevraagd liet de ADIV weten dat de *'profielen van personeelsleden die werden gevonden op sociale media werden opgeheven of aangepast zodat er geen enkele link meer was te leggen met de beroepshoedanigheid'*. De ADIV had hiertoe evenwel niet formeel de opdracht gegeven.

69 Binnen de ADIV is in 2009 wel een studie gemaakt over de bescherming van gevoelige gegevens bij operationele eenheden binnen het leger. Daaruit was onder meer gebleken dat militairen op zending soms (ongewild) gevoelige informatie in verband met de operaties, de militaire plannen, de infrastructuur, het materieel en het personeel uitwisselden op SND.

informatie; sommige informatie kan gebruikt worden als chantagemiddel; agenten en hun familie kunnen het doelwit worden van gewelddadige acties…[70]

Mede omdat beide diensten aanvankelijk geen zicht hadden op de problematiek (zie hierboven), hoefde het niet te verbazen dat zij zich ook niet echt bewust waren van de risico's. Volgens het Comité bleek uit sommige antwoorden van de VSSE zelfs dat deze dienst de risico's werkelijk onderschatte. De directie van dienst toonde zich nadien wel bereid om de risico's ernstig te nemen. Het Comité heeft dan ook vastgesteld dat er sinds 2014 een gunstige evolutie was op dit vlak.

II.5.3. MAATREGELEN DIE (KUNNEN) WORDEN GENOMEN

Er kunnen meerdere maatregelen worden genomen om de hierboven beschreven risico's te beperken of weg te nemen. Het Comité bestudeerde verschillende pistes en bevroeg hieromtrent de VSSE en de ADIV.

Vooreerst zou er kunnen gedacht worden aan de mogelijkheid om de aanwezigheid op SND eenvoudigweg te verbieden of dergelijk verbod te beperken tot ICT-netwerken van de dienst. De VSSE noch de ADIV hebben een dergelijk verbod uitgevaardigd. Wel is het gebruik van ICT-middelen van de dienst voor privédoeleinden gereglementeerd.

Volgens de Privacycommissie zou het verbieden van strikt persoonlijke activiteiten op sociale media en dit buiten de werkplek en de werkuren, overmatig zijn. Een dergelijk verbod mag dus wel worden opgelegd op de werkvloer en tijdens de werkuren. De werkgever heeft op dat ogenblik een (niet onbeperkt) controlerecht. De toepasselijke instructies dienen uiteraard vooraf ter kennis te worden gebracht van de betrokken ambtenaren.

Een andere mogelijkheid is het opstellen van regels (en dus niet het louter verbieden) met betrekking tot activiteiten op SND in de privésfeer. Omdat de vrijheid van meningsuiting geen absoluut recht is, is dit mogelijk om andere belangen (zoals de veiligheid van de Staat of de veiligheid van militairen) te beschermen. De VSSE had ten tijde van het onderzoek nog geen specifieke richtlijnen uitgevaardigd met betrekking tot het gebruik van SND door haar medewerkers. Wel werd het personeel voortdurend herinnerd aan de eisen van het beroepsgeheim en de discretie, ook in de persoonlijke levenssfeer. Dit betekent onder meer dat de personeelsleden er moeten op letten om via de sociale media rechtstreeks noch onrechtstreeks openbaarheid te verlenen aan hun hoedanigheid of die van een collega. De Privacycommissie was van mening dat een dergelijk verbod gerechtvaardigd is. De VSSE sensibiliseert zijn personeel ook in die zin tijdens briefings.

[70] Sommige van deze risico's werden omschreven in de kadernota van 13 mei 2013 betreffende het gebruik van sociale media door de leden en diensten van de Federale Politie. Het Vast Comité I vond dit een waardevol document voor de inlichtingendiensten.

In mei 2014 kondigde de VSSE aan dat het een specifieke richtlijn inzake SND-gebruik zou opstellen.

Ook bij de ADIV golden er geen specifieke instructies betreffende het privégebruik van SND. In het kader van het gebruik van SND voor beroepsactiviteiten waren er uiteraard wel relevante bepalingen. Bij het afsluiten van dit toezichtonderzoek stelde de ADIV in een intern document dat de discretie van het personeel onder alle omstandigheden vereist is, en verwees daarbij expliciet naar het gebruik van sociale media.

Een andere mogelijkheid (met name een algemeen verbod om zijn identiteit en beroepshoedanigheid mee te delen, ongeacht de omstandigheden) was in geen van de diensten van toepassing. Wel kent de VSSE de algemene verplichting tot discretie betreffende de identiteit en hoedanigheid als lid van de dienst, tenzij in de contacten met andere instanties. Hetzelfde geldt voor de ADIV: bij het gebruik van internet en van SND is het verboden informatie te publiceren of uit te wisselen die een rechtstreekse band zou kunnen aantonen tussen de gebruiker of een ander lid van de ADIV en zijn hoedanigheid van personeelslid, behalve wanneer hiervoor een uitdrukkelijke machtiging is verleend. Deze richtlijn wordt regelmatig toegelicht tijdens veiligheidsbriefings en opleidingen. De ADIV stelt daarenboven '*smartcards*' ter beschikking van personeelsleden van Defensie die actief zijn op sociale netwerken, met daarin een aantal *do's and don'ts*.

Nog een andere mogelijkheid bestaat er in om (*a priori* of *a posteriori*) toezicht uit te oefenen op het ITC-gebruik van personeelsleden en op de inhoud van hun berichten. Alhoewel dit vanuit privacy-oogpunt niet evident is, biedt de wet een aantal mogelijkheden. Zo kan naar aanleiding van een veiligheidsonderzoek het 'open profiel' van een agent gecontroleerd worden. Dit kan uiteraard ook in het kader van een inlichtingenonderzoek. Hierbij kunnen de inlichtingendiensten overigens ook inzage krijgen in de 'niet-publieke' delen van de berichten en dit door de inzet van bijzondere inlichtingenmethoden. Een algemene, preventieve opvolging van de inhoud van de berichten van hun personeelsleden in de privésfeer wezen de diensten af als disproportioneel en niet haalbaar.

Ten slotte onderzocht het Comité ook de tegenmaatregelen die kunnen genomen worden in geval van veiligheidsincidenten en besteedde het aandacht aan de reactiemogelijkheden van de diensten bij dergelijke incidenten (bijvoorbeeld intrekking van een veiligheidsmachtiging en een tuchtstraf).

II.5.4. ALGEMEEN BESLUIT

Bij wijze van algemeen besluit, stelde het Comité vast dat beide inlichtingendiensten in het kader van voorliggende problematiek voornamelijk een preventieve benadering volgden. Dit vooral vanuit de bezorgdheid om de vrijheid van meningsuiting van hun agenten niet aan banden te leggen. Deze preventieve benadering bestond erin het personeel bewust te maken van de risico's en hen

regelmatig te wijzen op hun plichten inzake geheimhouding en discretie. Het Comité was echter van oordeel dat het niet volstond om daarbij te verwijzen naar algemene veiligheidsvoorschriften. Een absoluut verbod op het gebruik van sociale netwerkdiensten is dan wel niet mogelijk (dit zou in strijd zijn met de rechten en vrijheden), toch moet er bij het nemen van specifieke maatregelen rekening worden gehouden met de bijzondere veiligheidsvoorwaarden voor inlichtingenagenten. Het Comité deed in dat kader diverse concrete aanbevelingen (zie IX.2.3).

II.6. DE PERSONEELSLEDEN VAN HET OCAD EN DE SOCIALE MEDIA

De Begeleidingscommissie van de Senaat vroeg in 2012 niet alleen een onderzoek te voeren naar de eventuele aanwezigheid van personeelsleden van de twee inlichtingendiensten op sociale netwerksites (SNS) (zie II.5). Het verzocht ook een onderzoek te doen naar dezelfde problematiek ten aanzien van de personeelsleden van het Coördinatieorgaan voor de dreigingsanalyse. Dit toezichtonderzoek diende gevoerd te worden samen met het Vast Comité P. Op 20 december 2015 beslisten beide Comités om een gemeenschappelijk onderzoek te openen naar '*de wijze waarop het OCAD omgaat met het bekendmaken van de identiteit en professionele hoedanigheid van zijn personeelsleden op sociale media op internet*'.[71]

Ook hier wensten de Parlementsleden van de Begeleidingscommissie een aantal bijkomende gegevens te bekomen. Het Comité voerde daarom een aanvullend onderzoek waarin het naging welke resultaten het pas opgerichte 'stuurcomité' van het OCAD reeds kon voorleggen en hoe de dienst had gereageerd op het feit dat vier van zijn personeelsleden actief bleken op de sociale media. Tevens wenste de Begeleidingscommissie te weten of het wettelijk mogelijk was om personeelsleden van het OCAD – zelfs in de privésfeer – te verbieden om actief te zijn op sociale netwerkdiensten. Wat dit laatste aspect betreft, wonnen de Vaste Comités I en P het advies in van de Privacycommissie.[72]

De resultaten van het initiële en het aanvullende onderzoek worden hieronder samen weergegeven.

---

71 Het onderzoek werd afgerond op 12 maart 2015.

72 Zie Advies nr. 45/2015 van 13 november 2015 met betrekking tot de adviesaanvraag van de Comités I en P met betrekking tot de mogelijkheid om de leden van de inlichtingendiensten en het OCAD te verbieden om, zelfs privé, actief te zijn op de sociale netwerken (www.privacycommission.be/nl/adviezen-cbpl?page=2).

II.6.1. DE OMVANG VAN HET FENOMEEN

Ook het OCAD vernam via de pers dat sommige van zijn personeelsleden hun naam en hoedanigheid bekend hadden gemaakt op sociale netwerken zoals LinkedIn en Facebook. Maar het OCAD had die informatie ook bekomen via zijn eigen ICT-dienst. Deze dienst nam geregeld steekproeven op het internet om na te gaan welke informatie er te vinden was over leden van het OCAD. Het OCAD beoordeelde de omvang van het fenomeen als 'gering'. Enerzijds betrof het slechts drie actieve en één gewezen lid van de dienst. Anderzijds werd geen gevoelige informatie onthuld. Bij een volgende bevraging in 2015 verklaarde de directie dat zij geen weet had van nieuwe gevallen.

II.6.2. RISICO'S VERBONDEN AAN HET GEBRUIK VAN SOCIALE NETWERKSITES

De Vaste Comités I en P stelden dat de leden van het OCAD zich uiterst bewust zouden moeten zijn van en aandacht hebben voor de mogelijkheden die sociale netwerksites bieden aan buitenlandse inlichtingendiensten: zij kunnen personen van nabij opvolgen met het oog op bijvoorbeeld spionage of informantenwerving.

Het OCAD ontkende het bestaan van de risico's niet, maar stelde dat het belang ervan moet gerelativeerd worden. Vooreerst is het zo dat de namen van alle analisten van het OCAD gekend kunnen zijn omdat ze bij hun benoeming in het Staatsblad gepubliceerd worden. Ten tweede stelde het OCAD dat het geen operationele taken heeft en geen activiteiten uitoefent die inherent zijn aan inlichtingendiensten.[73] Tot slot vertrouwde de leiding van het OCAD op het professionalisme van zijn personeelsleden en op de veiligheidsopleidingen die hen werden verstrekt.

II.6.3. MAATREGELEN DIE (KUNNEN) WORDEN GENOMEN

De meeste personeelsleden van het OCAD zijn gedetacheerd uit andere diensten (hoofdzakelijk politie- en inlichtingendiensten) en blijven onderworpen aan het statuut en de deontologie van hun dienst van oorsprong. Het koninklijk besluit van 23 januari 2007 betreffende het personeel van het OCAD bevat daarenboven een aantal bepalingen waarmee rekening moet worden gehouden bij de reglemen-

[73] De Comités waren het niet eens met deze stelling. Het evaluatiewerk van het OCAD berust in hoofdzaak op de verwerking en de analyse van (vaak geclassificeerde) informatie van inlichtingendiensten. Zelfs al is het OCAD niet bevoegd om zelf inlichtingen in te winnen, toch is ze belast met het verwerken en het analyseren van informatie. Deze draagt bij tot de inlichtingencyclus. Daardoor zijn de medewerkers van het OCAD gebonden aan dezelfde verplichtingen tot beroepsgeheim en discretieplicht en blootgesteld aan gelijkaardige veiligheidsrisico's als de personeelsleden van de inlichtingendiensten.

tering en de eventuele controle van hun handelwijze op SNS. Zo bijvoorbeeld stelt artikel 37 dat de analist, zelfs in zijn privéleven, de discretieplicht in acht dient te houden over alles wat betrekking heeft op zijn professionele activiteit.

Bovendien is elk lid van het OCAD houder van een veiligheidsmachtiging. Naar aanleiding van de toekenning of vernieuwing van dergelijke machtiging, kan ook een onderzoek gevoerd worden naar de 'open profielen' op netwerksites, dit wil zeggen naar informatie waarvan de toegang niet werd beperkt door de betrokkene.[74]

Wanneer een inlichtingendienst informatie ontvangt die erop wijst dat de handelwijze van een medewerker van het OCAD op SNS mogelijks een veiligheidsdreiging inhoudt, dan kan ook de informatie 'met beperkte toegang' bekomen worden en dit buiten medeweten van de betrokkene. Hiertoe dient evenwel een bijzondere inlichtingenmethode te worden aangewend.

In de meest recente versie van de 'veiligheidsinstructies' bestemd voor het personeel, werd specifiek aandacht besteed aan de discretieplicht bij het gebruik van sociale media. Ook kregen de personeelsleden in 2014 en 2015 een aantal veiligheidsbriefings.

Ten slotte werd er binnen het OCAD een zogenaamd 'stuurcomité' in het leven geroepen dat vier opdrachten meekreeg: (a) een lijst opmaken van de mogelijke veiligheidsproblemen; (b) voor elk van deze problemen een risicoanalyse maken; (c) vervolgens actieprioriteiten te bepalen; en ten slotte (d) te nemen maatregelen voorstellen op het vlak van investeringen, instructies en bewustmaking. In 2015 was dit stuurcomité klaar met het oplijsten van de problemen en waren de actieprioriteiten vastgelegd. De veiligheid gelinkt aan het gebruik van *ICT-tools* in ruime zin was daarvan een essentieel onderdeel. Tevens werd een werkgroep opgericht die de interne regels voor het goed gebruik van sociale media moest voorbereiden. De initiatieven werden echter opgeschort omdat prioriteit diende te worden gegeven aan de problematiek van de *foreign terrorist fighters* en aan de gebeurtenissen die zich voordeden in Parijs en in Brussel.

Net zoals voor de leden van de inlichtingendiensten, stelde zich voor de OCAD-medewerkers de vraag in welke mate preventieve controles op het privaat of professioneel gebruik van SNS mogelijk zijn. Aangezien alle medewerkers houder moeten zijn van een veiligheidsmachtiging, moet hun hiërarchie zich ervan kunnen vergewissen dat ze in alle omstandigheden blijven voldoen aan de veiligheidsvoorwaarden, meer in het bijzonder wanneer ze ICT-tools gebruiken in het kader van hun functie. Voor een dergelijke controle is de voorafgaande instemming van de betrokken medewerker niet vereist. In dat verband waren de Comités ook van mening dat de hiërarchie van het OCAD in staat moet zijn om de handelwijze van zijn medewerkers op de sociale media in het algemeen na te gaan.

---

74 Het raadplegen van sociale media is in de reglementering niet uitdrukkelijk voorzien als middel om informatie in te winnen tijdens een veiligheidsonderzoek. Naar oordeel van de Comités kan het gelijkgesteld worden met het consulteren van open bronnen.

In zijn advies stelde de Privacycommissie dat het verbieden van strikt persoonlijke activiteiten op de sociale media en dit buiten de werkplek en de werkuren, overmatig zou zijn. Een dergelijk verbod mag dus wel worden opgelegd op de werkvloer en tijdens de werkuren. De werkgever heeft op dat ogenblik een (niet onbeperkt) controlerecht. De toepasselijke instructies dienen uiteraard vooraf ter kennis te worden gebracht van de betrokkenen.

II.6.4. ALGEMEEN BESLUIT

Aangezien er slechts vier personeelsleden van het OCAD als dusdanig actief waren op sociale media, minimaliseerde het OCAD aanvankelijk de omvang van het probleem en wees er – terecht – op dat de namen van alle analisten van het OCAD gemakkelijk kunnen teruggevonden worden op het internet. Volgens de Vaste Comités I en P leek het OCAD zich in de loop van 2014 meer bewust te zijn geworden van het probleem en van de risico's.

De Comités waren van mening dat met de oprichting van een stuurcomité dat zich bezighoudt met veiligheidsproblemen, een belangrijke stap werd gezet voor een grondige aanpak van de problematiek. Evenwel moeten de rol van dat comité ter zake, de passende opsporingsmethoden en hun grenzen zorgvuldig gedefinieerd worden.

Vanuit zijn bekommernis om de vrijheid van meningsuiting van zijn medewerkers niet in te perken, heeft de leiding van het OCAD het gebruik van SNS voornamelijk preventief benaderd, meer bepaald door zijn personeelsleden te sensibiliseren. Hun aandacht wordt geregeld gevestigd op hun discretieplicht.

De Comités waren echter van oordeel dat het inroepen van algemene veiligheidsinstructies niet voldoende is. Een absoluut verbod op het gebruik van SND is dan wel niet mogelijk (dit zou in strijd zijn met de rechten en vrijheden), toch moet er bij het nemen van maatregelen rekening mee worden gehouden met de bijzondere veiligheidsvoorwaarden voor de betrokken medewerkers. Preventie door het opstellen van regels van goed gedrag en controle *a posteriori* (*social media policy*) blijken de ordewoorden te zijn. De Comités formuleerden in dit verband talrijke concrete aanbevelingen (zie IX.2.4).

II.7. DE INTERNATIONALE CONTACTEN VAN HET OCAD

Een van de opdrachten van het Coördinatieorgaan voor de dreigingsanalyse bestaat er in contacten te onderhouden met 'gelijkaardige buitenlandse of internationale diensten'. Begin mei 2013 besloten de Vaste Comités I en P een onder-

zoek te voeren naar de wijze waarop het OCAD deze opdracht invult.[75] In de periode voordien ontvingen de Comités immers verschillende anonieme brieven waarin werd aangeklaagd dat de toenmalige directeur vele dienstreizen zou maken én dubieuze contacten zou onderhouden met bepaalde buitenlandse inlichtingendiensten en -overheden.[76] Hij zou ook proberen om bepaalde dossiers te beïnvloeden ten gunste van bepaalde landen. Ten slotte zou hij zonder enig mandaat besprekingen hebben gevoerd over de informatie-uitwisseling met een buitenlandse dienst en over de wederzijdse toegang tot databanken.

Het eindverslag werd goedgekeurd op 22 juni 2005 en kort daarop besproken in de Begeleidingscommissie van de Kamer. Deze commissie vroeg de Comités een aanvullend onderzoek uit te voeren aangaande de aanwezigheid van twee communicatiesystemen bij het OCAD. Deze systemen waren aangeleverd door twee buitenlandse diensten. De Comités onderzochten de informaticaveiligheid van het OCAD en de wettelijkheid van beide systemen.[77]

II.7.1. DRIE EERDERE ONDERZOEKEN IN VERGELIJKBARE MATERIES

Het was niet de eerste maal dat de Comités de internationale contacten van het OCAD onderzochten.

Het eerste onderzoek dateerde uit 2009.[78] Het was onder meer gericht op de dienstreizen van de directeur. De Comités stelden hierover echter geen grote disfuncties vast.

In de loop van 2011 werd een onderzoek gevoerd naar een missie die het OCAD plande naar de Democratische Republiek Congo.[79] Met die missie wilde het OCAD een beter zicht krijgen op de veiligheidssituatie ter plaatse en op de eventuele aanwezigheid van radicale, extremistische of terroristische groeperingen in dat land. De Comités wezen onder meer op het feit dat de wetgever niet gewild heeft dat het OCAD zelf informatie inwint op het terrein, in de plaats van de ondersteunende diensten.

Het derde onderzoek – eveneens uit 2011 – handelde over de Belgische vertegenwoordiging bij internationale vergaderingen inzake terrorisme.[80] De Comités stelden vast dat de Belgische politie- en inlichtingendiensten en het OCAD

---

75 'Gemeenschappelijk toezichtonderzoek over de wijze waarop het OCAD internationale relaties onderhoudt met gelijkaardige buitenlandse of internationale diensten in toepassing van artikel 8, 3° van de W.OCAD van 10 juli 2006'.

76 Om dit aspect van het onderzoek na te gaan, werd ook onderzocht wat de inlichtingendiensten en de Federale Politie wisten over de contacten die het OCAD had aangeknoopt met bepaalde buitenlandse diensten, hoe die diensten die contacten ervoeren en hoe ze erop reageerden.

77 Het aanvullend verslag werd op 11 augustus 2015 afgerond.

78 VAST COMITÉ I, *Activiteitenverslag 2009*, 49.

79 VAST COMITÉ I, *Activiteitenverslag 2011*, 33.

80 VAST COMITÉ I, *Activiteitenverslag 2011*, 43.

geregeld samen deelnamen aan internationale vergaderingen inzake de strijd tegen het terrorisme en/of het extremisme. Dit gebeurde echter zonder veel overleg of coördinatie. Het onderzoek bracht diverse punctuele problemen aan het licht.

In de drie onderzoeken hebben de Vaste Comités I en P aanbevolen dat het OCAD er altijd op zou toezien dat zijn specifieke identiteit niet tot verwarring leidt bij de buitenlandse diensten en instellingen waarmee het contact heeft. Aangezien het coördinatieorgaan geen inlichtingendienst is, vonden de Comités het essentieel dat het daaraan actief en systematisch aandacht besteedt in zijn communicatie en in zijn werking, en dit zowel in België als in het buitenland. Er werd dus aanbevolen dat het OCAD uiterst voorzichtig te werk zou gaan bij de voorbereiding en de uitvoering van zijn opdrachten in het buitenland en dat het zijn studiereizen strikt zou beperken. Tot slot hebben de Vaste Comités I en P er ook voor gepleit dat het toenmalige Ministerieel Comité voor inlichting en veiligheid zo snel mogelijk een richtlijn zou opstellen om het begrip 'gelijkaardige diensten' waarmee het OCAD 'specifieke contacten' mag onderhouden nauwkeurig te bepalen.[81]

II.7.2. HET WETTELIJK KADER

In dit onderzoek waren vooral de artikelen 8, 9 en 10 W.OCAD van belang.

Zoals vermeld, heeft het OCAD de opdracht om met gelijkaardige buitenlandse of internationale diensten specifieke contacten te onderhouden (art. 8, 3° W.OCAD). Het is de taak van de Nationale Veiligheidsraad om te verduidelijken wat dit betekent. Bij het afsluiten van het onderzoek was dit nog niet gebeurd. De Comités wezen er op dat dergelijke oefening niet evident zou zijn, gelet op de diversiteit van de structuren die landen in plaats hebben gesteld om de analyse van de terroristische en/of extremistische dreiging te coördineren.[82]

Artikel 9 W.OCAD vormt de wettelijke basis voor de gegevensbank en de werkbestanden van het OCAD. De bepaling verplicht de directeur om passende technische en organisatorische maatregelen te treffen om te verhinderen dat onbevoegden er toegang tot zouden krijgen. Elke koppeling tussen de databank van het OCAD en andere, nationale of buitenlandse informatiesystemen is streng verboden.

Tot slot is er artikel 10 W.OCAD. Deze bepaling beperkt de mededeling van OCAD-evaluaties tot welbepaalde Belgische diensten en overheden; buitenlandse of internationale overheden of instellingen worden daarin niet vernoemd. Daarenboven bepaalt artikel 8 W.OCAD dat de gegevens die het coördinatieorgaan

81 Aan de door de Comités geformuleerde aanbevelingen werd pas onlangs gevolg gegeven. De Nationale Veiligheidsraad heeft begin 2016 een richtlijn in die zin uitgevaardigd. Deze richtlijn maakte evident niet het voorwerp uit van dit toezichtonderzoek.

82 Zie hierover VAST COMITÉ I (ed.), *Fusion Centres Throughout Europe, All-Source Threat Assessments in the Fight Against Terrorism*, Antwerpen, Intersentia, 2010, 220 p.

verkrijgt vanuit het buitenland moeten worden doorgegeven aan de bevoegde Belgische diensten.

II.7.3. DE CONCLUSIES VAN DE VASTE COMITÉS I EN P

Een eerste luik van het onderzoek was toegespitst op de buitenlandse dienstreizen van leden van het OCAD. Uit de meegedeelde cijfers bleek dat het aantal in het buitenland verrichte opdrachten niet overdreven was.

De frequentie van de contacten in België met bepaalde buitenlandse overheden en diensten was evenmin problematisch. Ze bewees dat het OCAD toegankelijk is, wat vermeldenswaardig is.

De Comités waren echter van mening dat de organisatie van de contacten met het buitenland niet het gevolg was van een duidelijke en weldoordachte strategie. Er kwam evenmin tot uitdrukking dat over die contacten overlegd werd met andere diensten; ze leken eerder het resultaat van persoonlijke initiatieven die werden genomen afhankelijk van externe verzoeken en aangediende kansen.

De Comités stelden ook een gebrek vast aan rapportering over de contacten, zowel intern als extern de organisatie. Zelden was er duidelijk een toegevoegde waarde, tenzij een eventuele kennisverwerving bij het personeelslid dat op missie werd gestuurd.

De contacten van het OCAD met buitenlandse en internationale diensten die geen 'gelijkaardige' diensten zijn, waren problematisch omdat ze voor verwarring konden zorgen over de verantwoordelijkheid van de verschillende Belgische diensten.

Uit het onderzoek was ook gebleken dat het OCAD soms informatie kreeg van buitenlandse diensten, zonder dat die informatie systematisch werd doorgezonden aan de bevoegde Belgische overheden. Bovendien gaf het OCAD toe dat het zelf ook informatie verstrekte aan die buitenlandse diensten. Die werkwijze was in strijd met artikel 8, 3°, tweede lid en artikel 10 W.OCAD.

Zonder de voorgaande conclusies te minimaliseren, onderstreepten de Comités dat het Ministerieel Comité voor inlichting en veiligheid (nu de Nationale Veiligheidsraad) ten tijde van het onderzoek nog geen richtlijn had uitgevaardigd die deze internationale contacten reglementeerden (zoals vereist door de W.OCAD). Dergelijke richtlijn moest verduidelijken wat het OCAD ter zake mag en niet mag doen.[83]

De Vaste Comités I en P deelden de bezorgdheden geuit door de leidinggevenden van de inlichtingendiensten over de wijze waarop de toenmalige directeur van het OCAD zijn internationale contacten beheerde. De Comités meenden dat de directeur, gelet op de contacten die hij aanknoopte met verscheidene buitenlandse partners soms sinds lang voor zijn benoeming in die functie, op zijn minst de indruk

[83] De Comités voegden er evenwel aan toe dat het OCAD nooit enig initiatief had genomen ten aanzien van zijn bevoegde ministers om deze kwestie op te helderen.

wekte dat hij onvoldoende omzichtig te werk ging. Hij hield verder onvoldoende afstand ten overstaan van bepaalde diensten van wie de activiteiten in België bijzonder aandachtig worden gevolgd door de VSSE en de ADIV, ook al hadden zijn voogdijministers hun goedkeuring gegeven om die officiële contacten te leggen.

Het gebrek aan transparantie, traceerbaarheid en rapportering in verband met deze contacten had bovendien voor gevolg dat de objectiviteit zelf van bepaalde evaluaties in twijfel werd getrokken door de Belgische inlichtingendiensten. Die vaststelling was bijzonder verontrustend.

De Vaste Comités I en P waren ook uiterst bezorgd over de wijze waarop de toenmalige directeur van het OCAD bepaalde contacten met het buitenland onderhield; die contacten werden gepercipieerd als het betreden van het bevoegdheidsdomein van de VSSE en van de ADIV en waren dus problematisch voor de samenwerking met die diensten. Die situatie moest grondig herdacht worden.

De Comités stelden opnieuw vast dat het OCAD in gebreke bleef om zijn wettelijke plicht na te komen om tweemaal per jaar een activiteitenverslag over zijn strategische doelstellingen, zijn activiteiten en zijn organisatie voor te leggen aan de Nationale Veiligheidsraad, die dat verslag moet overzenden aan de toezichtsorganen.

Wat betreft de twee communicatiesystemen die het OCAD deelde[84] met twee buitenlandse diensten, deden de Comités, zoals vermeld, bijkomend onderzoek. Dit onderzoek bevestigde en illustreerde de eerdere conclusies, en dit vooral op het vlak van de contacten met niet-homologe diensten en de uitwisseling van operationele informatie en persoonsgegevens. Los van de evidente noodzaak van internationale informatie-uitwisseling inzake extremisme en terrorisme, moesten beide Comités opmerken dat de vastgestelde handelwijzen strijdig waren met de letter en de geest van de W.OCAD. Bovendien hielden zij geen rekening met de bevoegdheden en verplichtingen van andere federale diensten en overheden wat een verstoring van de internationale samenwerking en de onderlinge relaties kon teweegbrengen.

II.8. ONTERECHT OPGEVOLGD DOOR DE INLICHTINGENDIENSTEN?

In februari 2014 beklaagt een persoon van Noord-Afrikaanse afkomst die in België verblijft zich over het feit dat hij op 'beklemmende wijze' in het oog wordt gehouden door de inlichtingendiensten. Hij beweert geen enkel idee te hebben waarom hij de aandacht zou trekken: hij heeft nooit problemen gehad in zijn land van herkomst noch in het Aziatisch land waar hij meerdere jaren heeft gewerkt; hij zegt geen gerechtelijke antecedenten te hebben noch banden met terroristische of radicale milieus.[85]

84 De systemen zijn niet langer operationeel.

85 Het onderzoek werd op 3 juli 2014 geopend. In februari 2015 werd het eindrapport verzonden naar de voorzitter van de Begeleidingscommissie, alsook naar de ministers van Justitie en Defensie.

Zijn problemen begonnen naar eigen zeggen in 2011. Toen werd hij zes uur vastgehouden op een buitenlandse luchthaven die hij aandeed in het kader van zijn werk. Een veiligheidsverantwoordelijke zou hem later hebben gezegd dat zijn naam op een lijst van het Amerikaanse *Transportation Security Agency* (TSA) zou voorkomen. Hij verklaarde dat hij sindsdien onder toezicht stond bij elke reis naar dit land. Ook werd ooit een visumaanvraag naar een derde land geweigerd. Dienvolgens werd hij overgeplaatst naar de Belgische zetel van het bedrijf.

De betrokkene verklaarde dat hij vanaf zijn aankomst in België, in mei 2012, het voorwerp was geweest van toezichtoperaties en zei te vrezen dat verschillende inlichtingendiensten hem onterecht opvolgden. Dit gevoel werd nog versterkt door de bijzondere behandeling die hem tweemaal te beurt viel op de luchthaven van Zaventem. Zo werd hij ooit gecontroleerd door de luchthavenpolitie én werd hij zelf kort vastgehouden toen hij een vliegtuig wilde nemen.

Het Vast Comité I ging na of de klager effectief onder de aandacht was gekomen van de Veiligheid van de Staat of de ADIV en zo ja, wat de informatiepositie en de acties van de inlichtingendiensten waren.

II.8.1. DE FEITEN

In november 2011 – de klager is op dat ogenblik nog niet in België – ontvingen het OCAD, de ADIV en de VSSE van een buitenlandse inlichtingendienst een verzoek om informatie in verband met de betrokkene. Hij zou sympathiseren met een radicale moslimpreker.

Volgend op de vraag van de buitenlandse dienst en bij gebrek aan enige informatie over de betrokkene, vraagt het OCAD aan de Federale Politie om hem in de algemene politiedatabank te seinen in de 'context Terroristische Informatie', en dit voor een periode van zes maanden.

De VSSE van haar kant voert een administratief onderzoek.[86] Daaruit blijkt niet dat de betrokkene deel zou uitmaken van islamistische milieus. De buitenlandse partnerdienst wordt hiervan in kennis gesteld.

Omdat de klager niet in zijn database voorkomt en omdat er geen rechtstreeks verband is met zijn wettelijke opdrachten, onderneemt de ADIV in deze geen actie.

Op 28 mei 2012 landt de betrokkene op de luchthaven van Zaventem.[87] Een dag later bezorgt de buitenlandse inlichtingendienst opnieuw inlichtingen, ditmaal aan de VSSE, het OCAD en de Federale Politie. Zo deelt de dienst mee dat de betrokkene het Aziatisch land waarin hij werkte, heeft verlaten. Omdat dit

[86] In dit kader heeft de VSSE haar eigen database en de bestaande databases (de politiedatabank, het Rijksregister, de Dienst Vreemdelingenzaken…) geraadpleegd. De dienst verklaarde ook opzoekingen te hebben verricht op sociale netwerken (Facebook…).

[87] Ondanks het feit dat hij geseind staat, wordt hij niet gecontroleerd wanneer hij voor het eerst in België aankomt.

document geen nieuwe informatie bevat, beslist de VSSE om geen bijkomend onderzoek te voeren. Wel vraagt de VSSE de partnerdienst naar een risicoanalyse en een evaluatie van de bedreiging. Ze krijgt als antwoord dat een analyse van het e-mailverkeer van de betrokkene geen doorslaggevende elementen aan het licht heeft gebracht.

In augustus 2012 – na een kort verblijf in het buitenland – wordt de betrokkene door de luchthavenpolitie gecontroleerd bij zijn aankomst in Zaventem.[88] Ditmaal wordt hij effectief ondervraagd. Een kopie van het rapport wordt bezorgd aan het OCAD, de ADIV en de VSSE. De verbalisanten stellen evenwel geen enkel betekenisvol element vast.

Diezelfde maand bevraagt het OCAD toch nog de drie betrokken ondersteunende diensten naar de eventuele banden van de klager met radicale, islamistische milieus. De VSSE antwoordt dat het niet over bijkomende elementen beschikt.

Begin 2013 ontvangt de VSSE een nieuw verzoek om informatie, ditmaal van de inlichtingendiensten van het Aziatische land waar de betrokkene heeft gewoond. Het verzoek bevat gedetailleerde informatie over zijn vermeend lidmaatschap van een radicale, islamistische stroming. De VSSE opent nu wel een nieuw onderzoek en doet daarbij onder meer een beroep op haar informatiekanalen. Er werd dus een grondiger onderzoek gevoerd, waarbij de dienst proportioneel te werk ging: zo werd bijvoorbeeld geen gebruik gemaakt van BIM-methoden. Alle ondernomen acties waren wettelijk.

In maart 2013 bezorgt de VSSE het resultaat van haar onderzoek aan de betrokken buitenlandse dienst. Opnieuw blijkt geen band met welke radicale islamistische milieus ook. Het resultaat van dit bijkomend onderzoek, ook al was het negatief, werd echter niet ter kennis gebracht van het OCAD. Ook de informatie van het Aziatische land werd niet verspreid buiten de VSSE.

Sinds maart 2013 ontving de VSSE geen nieuwe informatie of vragen meer over de betrokkene.

II.8.2. DE PROBLEMATIEK VAN TERRORISMELIJSTEN

Er bestaan sterke aanwijzingen dat de problemen die de klager in het buitenland ondervonden heeft, gerelateerd zijn met de problematiek van de terrorismelijsten.[89] Betrokkene zou bijvoorbeeld voorgekomen zijn op een lijst van de Amerikaanse *Transportation Security Administration* (TSA). Ook bleek de klager tijdelijk op een Belgische 'lijst' te zijn geplaatst, te weten de algemene politiedatabank.

---

88 Deze controle vond dus plaats toen de betrokkene voor de tweede keer naar België kwam.

89 Zie hierover P. DE HERT en K. WEIS, 'Europese terrorismelijsten. Beperkte rechtsbescherming', *Nieuw Juridisch Weekblad*, 2009, 199.

Het Comité wijst er op dat Staten en multilaterale instellingen diverse lijsten hanteren in de strijd tegen het terrorisme en ter beveiliging van de burgerluchtvaart. Doel daarbij is bijvoorbeeld de personen die er op vermeld worden te onderwerpen aan grondige controles, hen verbieden te vliegen of meldingen toe te laten aan de signalerende overheden. Dergelijke lijsten zijn gebaseerd op nationale en/of internationale wetgeving (bijv. de resoluties van de Verenigde Naties of richtlijnen van de Europese Unie).

Het Vast Comité I trekt het nut of de noodzaak van dergelijke lijsten niet in twijfel, integendeel. Recente terroristische acties tonen aan dat inlichtingen soms nog onvoldoende gedeeld worden met andere landen. Het Comité wil evenmin uitsluiten dat er in de concrete situatie van de klager gegronde redenen of vermoedens konden of hebben bestaan om hem op een dergelijke lijst te plaatsen.

In het voorliggend geval heeft het Vast Comité I, binnen het kader van zijn bevoegdheidsdomein, kunnen vaststellen dat de Belgische diensten op een professionele en correcte wijze gehandeld hebben ten opzichte van de klager en ten opzichte van de buitenlandse diensten.

Vanuit het perspectief van de burger, blijft een plaatsing op een lijst evenwel problematisch. Het is immers niet evident om zijn rechten te laten gelden ten opzichte van veiligheidsmaatregelen die vaak op basis van procedures zijn genomen die verlopen buiten medeweten van de betrokkene (geen kennisgeving, geen tegenspraak). Deze procedures, inclusief hun geheim karakter, kunnen legitiem zijn, voor zover de redenen en de doelstellingen ervan dat ook zijn en voor zover de uitvoering van de maatregelen niet buitensporig is.[90] Er bestaan inderdaad voorbeelden die aantonen dat het plaatsen van personen op terrorismelijsten tot disproportionele gevolgen kan leiden.[91] De praktijk leert ook dat het niet evident is om personen van dergelijke lijsten geschrapt te worden.

II.8.3. CONCLUSIES VAN HET ONDERZOEK

Het Comité benadrukte dat de klager niet het voorwerp is geweest van toezichtoperaties door de Belgische inlichtingendiensten. Zij zijn evenmin verantwoordelijk voor de seining in de 'context Terroristische Informatie'. Het lijkt echter zeer waarschijnlijk dat de klager werd gevolgd door de inlichtingendiensten van het Aziatische land waar hij een tijd heeft gewoond.

Verder vond het Comité geen enkele aanwijzing dat de VSSE door een partnerdienst zou zijn 'aangestuurd'. Er zijn daarenboven geen aanwijzingen dat bui-

---

90 Zie over dergelijke lijsten ook VAST COMITÉ I, *Activiteitenverslag 2005*, 158-168.

91 Maher ARAR is een Canadees-Syrisch burger die op basis van Canadese meldingen tijdens een tussenstop in de Verenigde Staten als terrorismeverdachte werd aanzien, werd overgeleverd aan Syrië en daar werd gefolterd. Later werd hij van alle verdenkingen vrijgesproken en ontving hij een schadevergoeding.
Zie http.//ccrjustice.org/ourcases/current-cases/arrar-v.ashcroft.

tenlandse diensten acties tegen de betrokkene zouden hebben ondernomen op Belgisch grondgebied.

De Belgische inlichtingendiensten hebben in dit dossier op legale en proportionele wijze gehandeld en zijn hun bevoegdheden niet te buiten gegaan. Ze hebben nooit deelgenomen aan toezichtactiviteiten zoals de klager die had beschreven. Het Comité stelde vast dat de VSSE dit geval efficiënt heeft beheerd.

Tot slot stelde het Comité zich de vraag of en in welke mate de Belgische inlichtingendiensten, krachtens de Grondwet[92] of het EVRM, een 'positieve verplichting' hebben ten aanzien van een ingezetene om hem te beschermen tegen eventueel ongegronde beschuldigingen vanwege buitenlandse inlichtingendiensten of overheden en, desgevallend, een inbreuk op zijn privacy te doen ophouden.

II.9. KLACHT OVER HET VERSTREKKEN VAN PERSOONLIJKE INFORMATIE DOOR EEN INLICHTINGENAGENT AAN EEN DERDE

Begin oktober 2014 wordt er bij het Vast Comité I een klacht neergelegd door een particulier. Volgens de klager zou de inhoud van persoonlijke e-mails die hij had verzonden naar een lid van het ministerie van Defensie, via de militaire inlichtingendienst bij zijn werkgever zijn beland. Kort daarop wordt hij ontslagen. Daarbij verwijst de werkgever expliciet naar het feit dat hij in het bezit was gesteld van een kopie van de bewuste e-mails door een personeelslid van de ADIV. Het onderzoek moest duidelijk maken op welke wijze het dossier werd behandeld door de ADIV, of de dienst zich daarbij hield aan de vigerende regelgeving en of er inderdaad informatie was doorgegeven aan een derde.[93]

De e-mails in kwestie waren bij de ADIV terecht gekomen via het lid van het ministerie van Defensie. De klager had in zijn berichten immers – bij wijze van grap, zo bleek achteraf – gemeld dat hij een computervirus had doorgezonden. De ADIV is de aangewezen dienst om dergelijke potentiële dreiging te onderzoeken; dit behoort tot zijn wettelijke opdrachten.

Naast het informaticaonderzoek, won de ADIV ook inlichtingen in over de klager zelf om zo de eventuele bedreiging te kunnen beoordelen. Ook dit behoort tot zijn bevoegdheden.

Het resultaat van dit technisch onderzoek (waaruit bleek dat er geen bedreiging was) werd in algemene bewoordingen ter kennis gebracht van de veiligheids-

92 Zie bijvoorbeeld art. 191 Grondwet: *'Iedere vreemdeling die zich op het grondgebied van België bevindt, geniet de bescherming verleend aan personen en aan goederen, behoudens de bij de wet gestelde uitzonderingen'.*

93 Het onderzoek werd afgerond in juni 2015. Het Vast Comité I was uiteraard niet bevoegd om zich uit te spreken over de reden en de wettelijkheid van het ontslag van de betrokkene.

officier van de onderneming waar de klager werkte. Deze mededeling vindt haar wettelijke grondslag in artikel 19 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst.[94] Wel stelde het Comité dat de verzending van alle e-mails naar de veiligheidsofficier en dit zonder de toelating van de betrokkenen, niet in overeenstemming leek met de Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

De ADIV had de mailberichten ook doorgezonden naar de Nationale Veiligheidsoverheid (NVO) die bevoegd is voor de eventuele intrekking van de veiligheidsmachtiging van de betrokkene en van de onderneming. Hoewel de bedreiging in dit geval niet ernstig was, kon het gedrag van de klager wel een mogelijk veiligheidsprobleem vormen. In dit opzicht leek de mededeling ervan aan de NVO legitiem.

Ten slotte stelde het Comité vast dat de ADIV de verschillende aspecten van het probleem onvoldoende had gecoördineerd en niet volledig handelde volgens de wettelijke of reglementaire procedures die gelden in geval van veiligheidsincidenten.

II.10. DE VSSE EN DE TOEPASSING VAN DE REGLEMENTERING MET BETREKKING TOT ZIEKTEVERLOVEN

Midden 2014 diende een beschermingsassistent van de VSSE een klacht in. Na een periode van ziekteverlof werd hij op non-activiteit[95] geplaatst voor de volledige periode van medische vrijstelling en kreeg hij het bevel een niet onaanzienlijk bedrag terug te betalen. Deze beslissing werd genomen omdat er zich tijdens zijn ziekteverlof problemen hadden voorgedaan op het vlak van de verplichte geneeskundige controle. Daarnaast beklaagde hij zich over het feit dat hij verplicht werd zijn overuren aan te zuiveren alvorens zijn werk te hervatten.

Het Comité besliste daarop een toezichtonderzoek te openen '*naar de wijze waarop de VSSE het arbeidsreglement en meer in het bijzonder de regels inzake ziekteverlof interpreteert en er uitvoering aan geeft*'.[96]

Uit het onderzoek bleek dat de VSSE goed op de hoogte is van de geldende arbeidsreglementering en de dienst ten aanzien van het personeel interne richtlij-

---

94 *"De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen die het voorwerp zijn van een bedreiging bedoeld in de artikelen 7 en 11 […]"* (art. 19 W.I&V).

95 Art. 62 van het KB van 19 november 1998 betreffende de verloven en afwezigheden toegestaan aan de personeelsleden van de rijksbesturen.

96 In februari 2015 werd het eindrapport verzonden naar de minister van Justitie en naar de voorzitter van de Begeleidingscommissie.

nen heeft uitgevaardigd. De regelgeving en de interne richtlijnen werden echter – in voorliggend geval – niet in acht genomen.

Wat betreft de problematiek van de overuren, verwees het Vast Comité I ook naar zijn toezichtonderzoek naar de uitvoering door de VSSE van haar wettelijke opdracht van persoonsbescherming.[97] De daarin vastgestelde problemen, golden nog steeds ten tijde van het onderzoek naar de klacht.

Ten slotte wees het Comité op een gebrek aan communicatie vanwege de administratieve diensten van de VSSE, zowel met interne personeelsleden als met de personeelsleden van de buitendiensten.

II.11. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2015 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2015 WERDEN OPGESTART

Dit onderdeel bevat een opsomming en een korte situering van alle in 2015 opgestarte toezichtonderzoeken alsook van die onderzoeken waaraan tijdens het werkingsjaar 2015 werd verder gewerkt maar die nog niet konden worden afgerond.

II.11.1. DE BESCHERMING VAN HET WETENSCHAPPELIJK EN ECONOMISCH POTENTIEEL EN DE SNOWDEN-ONTHULLINGEN

De onthullingen van Edward Snowden gaven een inkijk in uitermate geheime programma's van voornamelijk de Amerikaanse *National Security Agency* (NSA). Ze waren het startschot voor vele (parlementaire, gerechtelijke en inlichtingen-) onderzoeken over heel de wereld. Zo ook in België. Het Vast Comité I opende vier toezichtonderzoeken die uiteraard nauw met elkaar verweven waren.

Drie van de vier onderzoeken werden in 2014 afgerond.[98] Een laatste toezichtonderzoek[99] behandelt de mogelijke implicaties van deze buitenlandse program-

97 Hierover: VAST COMITÉ I, *Activiteitenverslag 2014* ('II.4. De VSSE en haar wettelijke opdracht van persoonsbescherming'), 44-51, in het bijzonder 49.

98 Zie VAST COMITÉ I, *Activiteitenverslag 2014*, 7-43 (het betreft respectievelijk 'II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten', 'II.2. Privacybescherming en massale datacaptatie' en 'II.3. Het gebruik in strafzaken van informatie afkomstig van massale data-captatie door buitenlandse diensten').

99 Toezichtonderzoek 'over de aandacht die de Belgische inlichtingendiensten (al dan niet) besteden aan de mogelijke dreigingen voor het Belgisch wetenschappelijk en economisch potentieel uitgaande van op grote schaal door buitenlandse grootmachten en/of inlichtingendiensten gehanteerde elektronische bewakingsprogramma's op communicatie- en informatiesystemen'.

ma's op de bescherming van het wetenschappelijk en economisch potentieel van het land. Het wil nagaan of de Belgische inlichtingendiensten:
– aandacht hebben besteed aan dit fenomeen;
– een reële of mogelijke bedreiging hebben gedetecteerd voor het Belgische wetenschappelijk en economisch potentieel;
– er de bevoegde overheden van in kennis hebben gesteld en beschermingsmaatregelen hebben voorgesteld; en
– over voldoende en adequate middelen beschikken om deze problematiek op te volgen.

Ook werd, op verzoek van de toenmalige Begeleidingscommissie van de Senaat, bestudeerd welke de gevolgen waren van het PRISM-programma en/of andere analoge systemen voor het wetenschappelijk en economisch potentieel van het land. Het rapport werd begin 2016 afgerond.

II.11.2. DE PROBLEMATIEK VAN DE '*FOREIGN FIGHTERS*' EN DE SYRIËGANGERS

Sinds 2013 oefent het Syrische strijdtoneel een grote aantrekkingskracht uit op de zogenaamde '*foreign (terrorist) fighters*' vanuit de hele wereld. Feit is dat daarbij – verhoudingsgewijs – veel strijders uit België komen.

Vandaar dat het Vast Comité I in oktober 2014 besloot een toezichtonderzoek te openen naar '*de informatiepositie van de twee inlichtingendiensten (ADIV en VSSE) over de rekrutering, de zending, het verblijf en de terugkeer in België van jongeren (van Belgische en andere nationaliteiten die in België verblijven) die vertrekken of vertrokken zijn naar Syrië of Irak en aangaande de uitwisseling van inlichtingen met diverse overheden.*' Daarbij zijn verschillende thema's aan de orde: welke opdracht hebben de Belgische inlichtingendiensten in dit kader en op welke wijze werden/worden zij aangestuurd? Hebben de inlichtingendiensten een kijk op de rekruterings- en vertrekfase? Kunnen zij zich een beeld vormen van de samenstelling van deze Syriëstrijders? Zijn ze op de hoogte van de activiteiten die deze strijders ter plaatste ontwikkelen? Wordt de evolutie in het buitenland vertaald naar mogelijke binnenlandse dreigingen, en zoja, welke? En wat met de opvolging en aanpak bij hun terugkeer naar België? Op welke wijze wordt samengewerkt (ADIV, VSSE, OCAD maar ook politie) in deze? Op welke wijze en aan wie wordt gerapporteerd?…

Begin 2015 werd een eerste, tussentijds rapport opgesteld ten behoeve van de Begeleidingscommissie (hierover Hoofdstuk II.4). Het eindverslag werd afgrond in 2016.

II.11.3. DE VSSE EN HET SAMENWERKINGSPROTOCOL MET DE STRAFINRICHTINGEN

Op 1 oktober 2014 werd een toezichtonderzoek opgestart naar de wijze waarop de VSSE het '*protocolakkoord tot regeling van de samenwerking tussen de Veiligheid van de Staat en het Directoraat-generaal Uitvoerig van Straffen en Maatregelen*' uitvoert. Rechtstreekse aanleiding van het onderzoek vormden twee eerder afgesloten toezichtonderzoeken.[100] Het doel lag er in te bestuderen of het akkoord efficiënt wordt toegepast, of de VSSE er voor de uitvoering van zijn opdrachten nuttige informatie uit kan putten en, zij het in de marge, na te kijken of de uitwisseling van gegevens van gedetineerden conform de bescherming van de rechten die de Grondwet en de wet aan de personen waarborgen verloopt.

Het onderzoek werd afgerond in 2016.

II.11.4. DE OPVOLGING VAN EEN POTENTIËLE DREIGING TEGEN EEN BUITENLANDSE BEZOEKER

In maart 2015 richt een agent van de Buitendiensten van de VSSE zich tot de Dienst Enquêtes van het Vast Comité I. Hij beklaagde zich over de wijze waarop de Analysediensten zouden gewerkt hebben in een bepaald dossier. Het betrof meer bepaald de wijze waarop informatie werd verzameld en geanalyseerd over het nakende bezoek van de Congolese dr. Mukwege aan België. Betrokkene voert sinds lang oppositie tegen het actuele bewind in Congo. Volgens de klager werd ook het OCAD niet correct op de hoogte gebracht van alle relevante informatie om een correcte evaluatie op te stellen over de potentiële dreiging die op de betrokkene rustte.

Het toezichtonderzoek werd in 2016 afgerond. De resultaten werden besproken binnen de Begeleidingscommissie van het Parlement.

II.11.5. EEN KLACHT TEGEN EEN INDISCRETE COLLEGA

In juli 2015 dient een hoofdofficier van ADIV een klacht in bij het Vast Comité I. Een medewerker van de ADIV zou immers in een publieke ruimte in de gemeente waar zowel hij als de medewerker wonen, gegevens over diens persoonlijke en professionele leven verspreid hebben. Hij vreesde zelfs dat dit gevolgen zou kunnen hebben voor zijn veiligheid en die van zijn gezin.

De klager richtte zich tweemaal tot de directie van de ADIV, maar vond dat er niet kordaat gereageerd werd. Uiteindelijk diende hij klacht in bij het Vast

[100] VAST COMITÉ I, *Activiteitenverslag 2011*, 22-25 ('II.3. De informatiepositie en acties van de inlichtingendiensten met betrekking tot Lors Doukaev') en *Activiteitenverslag 2012*, 28-33 ('II.3. De eventuele opvolging van een particulier tijdens en na zijn opsluiting in België').

Comité I. De klacht had zowel betrekking op het beweerde indiscreties als op de wijze waarop de ADIV hierop reageerde.

Het eindrapport werd in 2016 goedgekeurd.

II.11.6. EEN KLACHT OVER EEN (ON)VERSCHULDIGDE BETALING

Een gewezen inspecteur van de VSSE richtte in april 2015 een klacht aan het Vast Comité I. Hij werd namelijk verplicht een (klein) bedrag terug te betalen dat hij ten onrechte zou ontvangen hebben uit de kas van de speciale fondsen. Nadat hij zijn standpunt tevergeefs had trachten te verdedigen bij de VSSE, richtte hij zich tot het Vast Comité I. Bovendien meldde hij dat de problemen die hij had ondervonden met zijn directe hiërarchie, hem er mee toe hadden gebracht om de VSSE te verlaten.

Het Comité opende hierop een '*toezichtonderzoek naar aanleiding van de klacht van een gewezen agent van de VSSE betreffende het beheer van de afdelingskas van een provinciepost*'. Ook dit onderzoek werd afgerond in 2016.

II.11.7. EEN OMSTREDEN INTERVENTIE VAN TWEE PROTECTIEASSISTENTEN?

Tijdens een opdracht op de openbare weg in juni 2015 doet zich een incident voor met twee leden van de (toenmalige) Dienst Persoonsbescherming van de VSSE. De protectieassistenten staan in voor de veiligheid van een hoogwaardigheidsbekleder, wanneer de wagen van een particulier hen kort blijft volgen en hun bevelen om afstand te houden negeert. Wanneer het voertuig van de betrokkene stilstaat, gaan de protectieassistenten over tot een interventie. Zij zouden daarbij brutaal tewerk zijn gegaan. Een van hen trok zelfs zijn wapen. De bestuurster van de wagen heeft deze feiten aangegeven bij het Comité.

Het onderzoek naar het verloop van de interventie werd afgerond in 2016.

II.11.8. EEN KLACHT OVER EEN TUSSENKOMST VAN HET OCAD

In 2015 opende het Vast Comité I, samen met het Vast Comité P, een onderzoek naar de wijze waarop het OCAD een rol had gespeeld bij de intrekking van de licentie van een lijnpiloot. Betrokkene had namelijk klacht ingediend omdat het OCAD ten onrechte een dreigingsevaluatie zou hebben opgemaakt die vervolgens kon gebruikt worden om zijn licentie als piloot in te trekken.

In 2015 werd de meeste onderzoekverrichtingen afgerond. Het onderzoek zal in de tweede helft van 2016 worden gefinaliseerd.

II.11.9. INDIVIDUELE DREIGINGSEVALUATIES DOOR HET OCAD

In maart 2015 openden de Vaste Comités I en P een gemeenschappelijk onderzoek naar '*de wijze waarop het OCAD het dreigingsniveau bepaalt dat uitgaat van een individu of waaraan een individu blootstaat, naar de gevolgen die de bepaling van dat dreigingsniveau heeft voor de taakverdeling, de te nemen maatregelen en de informatieuitwisseling tussen de betrokken diensten, alsook naar de praktische gevolgen voor de betrokken persoon en diens opvolging*'. Dit gebeurde op verzoek van de Begeleidingscommissie van de Kamer. Deze wenste geïnformeerd te worden over volgende vragen:

- Welke criteria hanteert het OCAD om het dreigingsniveau te bepalen ten aanzien van een individu?
- Welke instantie legt de taken vast van de betrokken diensten eens het dreigingsniveau is bepaald?
- Welke operationele maatregelen resulteren uit een bepaald dreigingsniveau en welke dienst is belast met de coördinatie?
- Hoe zijn de informatiestromen tussen de diverse diensten geregeld?
- Wat zijn de concrete gevolgen voor een individu die het voorwerp is van een bepaald dreigingsniveau?
- Hoe wordt de 'classificatie' van dit individu opgevolgd door de lokale politionele en administratieve overheden?

In februari 2016 werd een tussentijds rapport verzonden aan de Begeleidingscommissie. Het eindrapport is voorzien voor de tweede helft van 2016.

II.11.10. SPECIFIEKE DISFUNCTIES BINNEN HET OCAD

In de tweede helft van 2015 ontvingen de Vaste Comités I en P twee anonieme brieven. Ze maken melding van 'onregelmatigheden' en 'ernstige structurele problemen' binnen het OCAD. Zo bijvoorbeeld zouden de experten taken moeten uitvoeren die statutair tot de opdrachten van de analisten behoren. Ook zouden bepaalde personen naar het OCAD gedetacheerd zijn met miskenning van de geldende regels.

Wat later ontvangen de Comités nog een klacht over de interne werking van het OACD. De klager verwijst onder meer naar de wijze waarop er een einde werd gesteld aan zijn detachering.

De Comités bundelden alle kwesties in een gemeenschappelijk onderzoek. Het eindrapport is voorzien voor de tweede helft van 2016.

II.11.11. TOEZICHTONDERZOEK OVER DE INFORMATIEPOSITIE VAN DE TWEE INLICHTINGENDIENSTEN VOOR DE AANSLAGEN IN PARIJS

Op 13 november 2015 gebeuren in Parijs meerdere aanslagen. In de buurt van het *Stade de France* laten zelfmoordterroristen zich ontploffen en nabij terrassen van cafés en restaurants van de Franse hoofdstad volgen raids. Op datzelfde moment worden in de concertzaal Bataclan de bezoekers gegijzeld waarop vervolgens het vuur wordt geopend. Het aantal dodelijke slachtoffers loopt op tot 130. Een vierde aanslag was gepland nabij de zakenwijk *La Défense*. De aanslagen zijn het werk van teruggekeerde *foreign terrorist fighters* en aangestuurd door de terreurgroep IS.

Vrij vlug duikt er informatie op die wijst op het bestaan van een nauwe band met België: zo waren meerdere terroristen afkomstig van of woonachtig in België, waren de voertuigen die gebruikt werden bij de aanslagen in België gehuurd, waren er Belgische onderduikadressen, werden de bommengordels waarschijnlijk in een appartement in Schaarbeek geassembleerd…

Het Vast Comité I opende vrijwel onmiddellijk een toezichtonderzoek.[101] Wel wachtte het met de eerste onderzoekverrichtingen. In de turbulente weken en maanden na de aanslagen kon van de VSSE en de ADIV immers niet verwacht worden dat ze veel tijd zouden vrijmaken voor het Comité en zijn enquêtedienst.

Het onderzoek werd afgerond in 2016.

[101] '*Toezichtonderzoek over de informatiepositie van de twee inlichtingendiensten, voorafgaand aan 13 november 2015 's avonds, over de individuen of groepen die de aanslagen te Parijs hebben uitgevoerd of hierbij betrokken waren*'. Begin 2016 werd samen met het Vast Comité P eenzelfde onderzoek geopend maar dan met betrekking tot de informatiepositie van het OCAD.

HOOFDSTUK III
CONTROLE OP DE BIJZONDERE INLICHTINGENMETHODEN

Dit hoofdstuk bevat nadere cijfers over de inzet door de VSSE en de ADIV van de bijzondere inlichtingenmethoden en over de wijze waarop het Vast Comité I zijn jurisdictionele taak waarneemt. Het is gebaseerd op het verslag over de inzet van bijzondere methoden door de inlichtingendiensten dat jaarlijks ten behoeve van het Parlement wordt opgesteld in uitvoering van artikel 35 § 2 W.Toezicht.

Voorafgaand wil het Comité melding maken van de overeenkomst van 16 november 2015 tussen de Nationale Bank van België (NBB) en de VSSE waarbij deze laatste op eenvoudig verzoek toegang zou worden verleend tot de gegevens opgenomen in het Centraal Aanspreekpunt (CAP). Dit is een databank waaraan alle bank-, wissel-, krediet- en spaarinstellingen de identiteit van hun cliënten en hun rekeningnummers kenbaar moeten maken. De VSSE was van oordeel dat dergelijke raadpleging een gewone methode vormde (met name deze voorzien in artikel 14 W.I&V). Het Comité was het daar echter niet mee eens. Alhoewel het Comité van oordeel was dat het initiatief van de VSSE aantoonde dat de dienst op actieve wijze nuttige informatiekanalen aanboorde, wees het op artikel 18/15 § 1, 1° W.I&V. Dit artikel beschouwt het opvragen van lijsten van bankrekeningen als een uitzonderlijke methode. Daarbij wordt geen voorbehoud gemaakt bij welke instantie die informatie wordt bekomen. Dus ook indien de NBB niet als een 'bank' of een 'financiële instelling' zou mogen gezien worden in de zin van artikel 18/5 § 2 W.I&V, dan nog blijven de lijsten 'beschermd' door het mechanisme van de uitzonderlijke methode. Indien de VSSE dus lijsten van bankrekeningen wenst te bekomen via het CAP, dient eerst een uitzonderlijke methode te worden aangevraagd. De minister van Justitie stelde dat de VSSE, in afwachting van bijkomend overleg, de BIM-procedure moet toepassen bij de bevraging van het CAP.[102]

[102] *Hand.* Kamer 2015-16, 6 januari 2016, CRIV54COM301, 3, Vr. nr. 8170.

III.1. CIJFERS MET BETREKKING TOT SPECIFIEKE EN UITZONDERLIJKE METHODEN

Tussen 1 januari en 31 december 2015 werden door de twee inlichtingendiensten samen 1392 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 1271 door de VSSE (waarvan 1143 specifieke en 128 uitzonderlijke) en 121 door de ADIV (waarvan 87 specifieke en 34 uitzonderlijke).

Onderstaande tabel maakt een vergelijking met de cijfers van de afgelopen jaren.

	ADIV		VSSE		TOTAAL
	Specifieke methode	**Uitzonderlijke methode**	**Specifieke methode**	**Uitzonderlijke methode**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392

Daar waar er in 2014 een daling met 7% werd geregistreerd, kende het aantal bijzondere inlichtingenmethoden in 2015 een iets grotere stijging. De groei situeerde zich volledig op het niveau van de door de VSSE ingezette specifieke methoden (van 976 in 2014 naar 1143 in 2015). Zowel alle bijzondere methoden ingezet door de ADIV, als de uitzonderlijke methoden ingezet door de VSSE, kenden een significante daling.

In wat volgt worden, per dienst, drie rubrieken onderscheiden: cijfers over de specifieke methoden, cijfers over de uitzonderlijke methoden en cijfers inzake de dreigingen en de te verdedigen belangen die door de methoden geviseerd worden.

III.1.1. METHODEN MET BETREKKING TOT DE ADIV

III.1.1.1. De specifieke methoden

AARD SPECIFIEKE METHODE	**AANTAL 2013**	**AANTAL 2014**	**AANTAL 2015**
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	14	7	4
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0	0	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	0	0	0

AARD SPECIFIEKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015
Kennisnemen van identificatiegegevens van elektronisch communicatieverkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	66 methoden	67 methoden	55 methoden
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	15	12	12
Kennisnemen van lokalisatiegegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	36	28	16
TOTAAL	**131**[103]	**114**	**87**

De in 2014 geobserveerde tendens waarbij minder gebruik werd gemaakt van observaties en lokalisaties, zette zich door in 2015. Er viel ook een vermindering van het aantal identificaties te noteren, terwijl de kennisname van oproepgegevens stabiel bleef.

III.1.1.2. Uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	1	1	3
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	0	1	0
Oprichten en gebruiken van een fictieve rechtspersoon	0	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	0	0	0
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	5	5	3
Binnendringen in een informaticasysteem	0	03	3
Afluisteren, kennisnemen en opnemen van communicaties	17	26	25
TOTAAL	**23**[104]	**36**	**34**

103 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

104 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

Wat betreft de uitzonderlijke methoden moet vastgesteld worden dat het aantal tapmaatregelen stabiel bleef (25 in 2015 tegenover 26 in 2014), en dit in tegenstelling tot 2013 waar er een gevoelige stijging te noteren viel.

III.1.1.3. De belangen en dreigingen die de inzet van de bijzondere methoden rechtvaardigen[105]

De ADIV mag specifieke en 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 VAN DE OPDRACHT	AANTAL 2013	AANTAL 2014	AANTAL 2015
Inlichtingenopdracht	111	109	112
Militaire veiligheid	15	5	6
Bescherming geheimen	28	36	4

Wat betreft de aard van de opdracht valt een *status quo* te noteren voor de 'inlichtingenopdracht' en de 'militaire veiligheid'. De 'bescherming van geheimen' kent evenwel een sterke daling (van 36 in 2014 naar amper 4 in 2015).

AARD DREIGING	AANTAL 2013	AANTAL 2014	AANTAL 2015
Spionage	94	123	101
Terrorisme (en radicaliseringsproces)	6	7	4
Extremisme	24	15	13
Inmenging	1	0	4
Criminele organisatie	16	2	0
Andere	13	0	0

[105] Per toelating kunnen meerdere belangen en dreigingen aan de orde zijn.

Wat betreft de aard van de dreiging, blijkt de tendens om minder BIM-methoden in te zetten in de strijd tegen terrorisme en extremisme zich in 2015 door te zetten (30 in 2013, 22 in 2014 en slechts 17 in 2005). Dat mag verbazen gezien de relatieve toename van deze dreigingen in 2015. Ook inzet van BIM-methoden tegen de dreiging 'spionage' kent in 2015 een neerwaartse trend (101 tegen 123 in 2014).

III.1.2. METHODEN MET BETREKKING TOT DE VSSE

III.1.2.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	109	86	86
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0	0	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	0	0	0
Kennisnemen van identificatiegegevens van elektronisch communicatie-verkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	613 methoden	554 methoden	663 methoden
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	136	88	33
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator	244	248	361
TOTAAL	**1102**	**976**	**1143**

Eerder werd reeds aangegeven dat het globale aantal toelatingen met betrekking tot de inzet van specifieke methoden door de VSSE was toegenomen. Zo kon in 2015 een significante stijging worden opgetekend van de kennisname van de identificatiegegevens (554 in 2014 tegen 663 in 2015) alsook van de kennisname van lokalisatiegegevens (248 in 2014 naar 361 in 2015). De kennisname van oproepgegevens daalde dan weer (van 88 naar 33 in 2015). Wat betreft de observaties werd een *quasi* verdubbeling vastgesteld inzake het aantal gevolgde personen (71 in 2014 tegen 141 in 2015).

III.1.2.2. De uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	6	9	6
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	6	21	8
Oprichten en gebruiken van een fictieve rechtspersoon	0	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	6	18	5
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	11	8	6
Binnendringen in een informaticasysteem	12	18	16
Afluisteren, kennisnemen en opnemen van communicaties	81	86	87
TOTAAL	**122**	**156**[106]	**128**

De daling van het aantal toegepaste uitzonderlijke methoden is in hoofdzaak het gevolg van de gevoelige daling van het aantal 'doorzoekingen' (9 in 2015 tegenover nog 21 in 2014) en het aantal 'openen van post' (18 in 2014 tegenover nog maar 5 in 2015). Dit in tegenstelling tot het aantal 'afluisteren van communicaties' dat licht blijft stijgen (81 in 2013, 86 in 2014 tot 91 voor 2015).

III.1.2.3. De dreigingen en belangen die de inzet van de bijzondere methoden rechtvaardigen

De volgende tabel toont in het kader van welke (potentiële) dreigingen de VSSE specifieke en uitzonderlijke toelatingen verleende. 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). De wet hanteert volgende definities:

106 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

1. spionage: het opzoeken of het verstrekken van inlichtingen die voor het publiek niet toegankelijk zijn en het onderhouden van geheime verstandhoudingen die deze handelingen kunnen voorbereiden of vergemakkelijken;
2. terrorisme: het gebruik van geweld tegen personen of materiële belangen om ideologische of politieke redenen met het doel zijn doelstellingen door middel van terreur, intimidatie of bedreigingen te bereiken;
   Radicaliseringproces: een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen
3. extremisme: racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat;
4. proliferatie: de handel of de transacties betreffende materialen, producten, goederen of knowhow die kunnen bijdragen tot de productie of de ontwikkeling van non-conventionele of zeer geavanceerde wapensystemen. In dit verband worden onder meer bedoeld de ontwikkeling van nucleaire, chemische en biologische wapenprogramma's, de daaraan verbonden transmissiesystemen, alsook de personen, structuren of landen die daarbij betrokken zijn;
5. schadelijke sektarische organisaties: elke groep met filosofische of religieuze inslag of die voorwendt dat te zijn en die qua organisatie of in haar praktijk schadelijke onwettige activiteiten uitoefent, individuen of de maatschappij nadeel berokkent of de menselijke waardigheid schendt;
6. inmenging: de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden;
7. criminele organisaties: iedere gestructureerde vereniging van meer dan twee personen die duurt in de tijd, met als oogmerk het in onderling overleg plegen van misdaden en wanbedrijven, om direct of indirect vermogensvoordelen te verkrijgen, waarbij gebruik gemaakt wordt van intimidatie, bedreiging, geweld, listige kunstgrepen of corruptie, of waarbij commerciële of andere structuren worden aangewend om het plegen van misdrijven te verbergen of te vergemakkelijken. In dit kader worden bedoeld de vormen en structuren van de criminele organisaties die wezenlijk betrekking hebben op de activiteiten bedoeld in voorgaande dreigingen of die destabiliserende gevolgen kunnen hebben op het politieke of sociaaleconomische vlak.

In acht genomen dat per toelating verschillende dreigingen aan de orde kunnen zijn, komen we tot volgende cijfers:

AARD DREIGING	AANTAL 2013	AANTAL 2014	AANTAL 2015
Spionage	359	319	253
Terrorisme (en radicaliseringsproces)	580	499	812
Extremisme	246	267	171
Proliferatie	15	33	30
Schadelijke sektarische organisaties	9	0	0
Inmenging	8	10	10
Criminele organisaties	9	8	0

Bovenstaande cijfers tonen aan dat wat betreft de inzet van BIM-methoden, 'terrorisme' de absolute prioriteit blijft bij de VSSE (van 499 in 2014 naar 812 in 2015). Dat maakt evenwel dat minder toelatingen worden genoteerd inzake dreigingen gelieerd aan 'extremisme' (171 tegenover 207 in 2014) en 'spionage' (van 319 in 2014 naar 253 in 2015). De inzet van de beschikbare BIM-middelen is dus gedeeltelijk verschoven naar de strijd tegen het terrorisme.

De bevoegdheid van de VSSE wordt niet alleen bepaald door de aard van de dreiging. De dienst mag slechts optreden ter vrijwaring van welbepaalde belangen:

- de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde zijnde,
  a) de veiligheid van de instellingen van de Staat en het vrijwaren van de continuïteit van de regelmatige werking van de rechtsstaat, de democratische instellingen, de elementaire beginselen die eigen zijn aan iedere rechtsstaat, alsook de mensenrechten en de fundamentele vrijheden;
  b) de veiligheid en de fysieke en morele vrijwaring van personen en de veiligheid en de vrijwaring van goederen
- de uitwendige veiligheid van de Staat en de internationale betrekkingen: het vrijwaren van de onschendbaarheid van het nationaal grondgebied, van de soevereiniteit en de onafhankelijkheid van de Staat, van de belangen van de landen waarmee België gemeenschappelijke doeleinden nastreeft, alsook van de internationale en andere betrekkingen die België met vreemde Staten en internationale of supranationale instellingen onderhoudt;
- de vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

In acht genomen dat per toelating verschillende belangen aan de orde kunnen zijn, komen we tot volgende cijfers voor 2015:

AARD BELANG	AANTAL 2013	AANTAL 2014	AANTAL 2015
De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde	1177	1100	1258
De uitwendige veiligheid van de Staat en de internationale betrekkingen	1160	1075	1150
De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel	11	10	4

III.2. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS JURISDICTIONEEL ORGAAN EN ALS PREJUDICIEEL ADVIESVERLENER

III.2.1. DE CIJFERS

In dit onderdeel wordt ingegaan op de activiteiten van het Vast Comité I met betrekking tot de specifieke en uitzonderlijke inlichtingenmethoden. Daarbij zal uitsluitend aandacht besteed worden aan de ter zake genomen jurisdictionele beslissingen. Vooraf dient evenwel te worden onderlijnd dat het Comité *alle* toelatingen tot de inzet van bijzondere methoden aan een *prima facie*-onderzoek onderwerpt, en dit met het oog op de al dan niet vatting.

Artikel 43/4 W.I&V stelt dat het Vast Comité I op vijf manieren kan worden gevat:

- 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.

Daarnaast kan het Comité ook gevat worden in zijn hoedanigheid van 'prejudicieel adviesverlener' (art. 131*bis*, 189*quater* en 279*bis* Sv.). In dat geval 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 onderzoeks-

gerechten of de strafrechters. Strikt genomen treedt het Comité alsdan niet op als jurisdictioneel orgaan.

WIJZE VAN VATTING	AANTAL 2013	AANTAL 2014	AANTAL 2015
1. Op eigen initiatief	16	13[107]	16
2. Privacycommissie	0	0	0
3. Klacht	0	0	0
4. Schorsing door BIM-Commissie	5	5	11[108]
5. Toelating minister	2	1	0
6. Prejudicieel adviesverlener	0	0	0
TOTAAL	**23**	**19**	**27**

Eens gevat, kan het Comité verschillende soorten (tussen)beslissingen nemen. In twee gevallen (1. en 2. hieronder) wordt evenwel een beslissing genomen vóór de eigenlijke vatting.

1. nietigheid van de klacht wegens vormgebrek of afwezigheid van een persoonlijk en rechtmatig belang (art. 43/4, eerste lid, W.I&V);
2. beslissing om geen gevolg te geven aan een klacht die kennelijk niet gegrond is (art. 43/4, eerste lid, W.I&V);
3. schorsing van de betwiste methode in afwachting van een definitieve beslissing (art. 43/4, laatste lid, W.I&V);
4. vordering tot bijkomende informatie ten aanzien van de BIM-Commissie (43/5 § 1, eerste tot derde lid, W.I&V);
5. vordering tot bijkomende informatie ten aanzien van de betrokken inlichtingendienst (43/5 § 1, derde lid, W.I&V);
6. onderzoeksopdracht voor de Dienst Enquêtes I (art. 43/5 § 2 W.I&V). In deze rubriek wordt zowel verwezen naar de veelvuldige bijkomende informatie die door de Dienst Enquêtes I op eerder informele wijze wordt ingewonnen vóór de eigenlijke vatting als naar informatie die op verzoek van het Comité wordt ingewonnen na de vatting;
7. horen van de BIM-Commissieleden (art. 43/5 § 4, eerste lid, W.I&V);
8. horen van het diensthoofd of de leden van de betrokken inlichtingendienst (art. 43/5 § 4, eerste lid, W.I&V);
9. 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);

107 In twee gevallen viel de beslissing van het Comité pas in januari 2015.

108 In één dossier vond de vatting plaats in 2015 maar viel de beslissing van het Comité in 2016.

10. 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);
11. 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);
12. gedeeltelijke stopzetting van een toegelaten methode. 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.
13. 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;
14. onbevoegdheid van het Vast Comité I;
15. ongegrondheid van de aanhangige zaak en geen stopzetting van de methode;
16. advies als prejudicieel adviesverlener (artt. 131*bis*, 189*quater* en 279*bis* Sv.).

Het Vast Comité I moet binnen een termijn van een maand volgend op de dag waarop het werd gevat een definitieve uitspraak doen (art. 43/4 W.I&V). In alle dossiers werd die termijn gerespecteerd.

AARD VAN DE BESLISSING	2013	EIND-BESLISSING 2013	2014	EIND-BESLISSING 2014	2015	EIND-BESLISSING 2015
1. Nietige klacht	0		0		0	
2. Kennelijk ongegronde klacht	0		0		0	
3. Schorsing methode	0		3		2	
4. Bijkomende informatie van BIM-Commissie	0		0		0	
5. Bijkomende informatie van inlichtingendienst	0		1		1	
6. Onderzoeksopdracht Dienst Enquêtes	50		54		48	
7. Horen BIM-Commissieleden	0		0		2	

AARD VAN DE BESLISSING	2013	EIND-BESLISSING 2013	2014	EIND-BESLISSING 2014	2015	EIND-BESLISSING 2015
8. Horen leden inlichtingendiensten	0		0		2	
9. Beslissing mbt geheim van onderzoek	0		0		0	
10. Gevoelige informatie tijdens verhoor	0		0		0	
11. Stopzetting methode	9		3		3	
12. Gedeeltelijke stopzetting methode	5		10		13	
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	2	**23**	0	**17**	4	**26**
14. Onbevoegd	0		0		0	
15. Wettige toelating / Geen stopzetting methode / Ongegrond	7		4		6	
16. Prejudicieel advies	0		0		0	

Het Vast Comité I heeft in 2015 26 beslissingen genomen tegenover 17 in 2014. Deze stijging vindt zijn oorsprong in het feit dat het Comité zichzelf in 2015 meer vatte (van 13 naar 16 keer) maar vooral omdat de BIM-Commissie vaker toelatingen schorste (van 5 keer in 2014 naar 11 keer in 2015).

Vermeldenswaard is ook dat het Vast Comité I voor het eerst leden van de BIM-Commissie hoorde en dit in twee dossiers.

III.2.2. DE RECHTSPRAAK

Hieronder wordt de essentie weergegeven van de eindbeslissingen die het Vast Comité I in 2015 nam. De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk worden opgenomen. Het Comité diende hierbij de nodige omzichtigheid aan de dag te leggen omdat vele beslissingen dienden geclassificeerd te worden (zeven als VERTROUWELIJK; vijf als GEHEIM; twee als ZEER GEHEIM). Daardoor zag het Comité zich genoodzaakt om bepaalde elementen van het juridische vraagstuk soms niet expliciet op te nemen.

De beslissingen werden gegroepeerd onder vijf rubrieken:
- wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode;
- motivering van de toelating;
- de proportionaliteits- en de subsidiariteitseis;
- wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging;
- de gevolgen van een onwettig(e) (uitgevoerde) methode.

Indien relevant werden sommige beslissingen onder meerdere rubrieken opgenomen.

III.2.2.1. Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode

III.2.2.1.1. Voorafgaande kennisgeving BIM-Commissie

Een specifieke methode kan pas effectief worden aangewend na kennisgeving van de toelating aan de BIM-Commissie (art. 18/3 § 1, tweede lid, W.I&V). In dossiers 2015/4355, 2015/4356 en 2015/4199 was de Commissie in kennis gesteld van een toelating, terwijl de methode reeds eerder was opgestart of was de verlenging van de methode laattijdig aan de Commissie ter kennis gebracht. De Commissie schorste dan ook de methoden voor het gedeelte vóór de kennisgeving. Het Comité bevestigde telkenmale die beslissingen.

III.2.2.1.2. Voorstel tot machtiging, eensluidend advies en machtiging van een uitzonderlijke methode

Een inlichtingendienst formuleerde een voorstel van machtiging om gedurende één maand tot een tapmaatregel over te gaan (dossier 2015/4170). De BIM-Commissie verleende hiervoor een eensluidend advies. De uiteindelijke machtiging van het diensthoofd stelde echter dat de tapmatregel toegelaten was voor 48 uur (en dus niet meer voor een maand). Alhoewel dit niet conform het eensluidend advies was, stelde het Comité '*dat deze vermindering van de duur geen probleem stelt*' (vertaling).

In dossier 2015/3713 was een andere problematiek aan de orde. De inlichtingendienst had de toelating om een target gedurende twee maanden af te luisteren. Wanneer die termijn verloopt stopt de methode niet, maar vergeet hij echter een verlenging aan te vragen. De dienst merkt dit na een aantal dagen zelf op en verwittigt de BIM-Commissie. Deze schorst de methode vanaf het einde van het eerste (en wettige) mandaat. Het Comité besliste daarop dat het '*moet vaststellen dat de methode van [xxx] 2015 om 00 uur onwettig is gelet op de afwezigheid van een beslissing tot verlenging van de methode*' (vertaling).

In een derde dossier (2015/3718) was een machtiging verleend om een welbepaalde gsm van een target af te luisteren. Maar de dienst ging ook over tot het afluisteren van een tweede toestel dat gebruikt werd door de betrokkene. Toen zij dit vaststelde, ging de BIM-Commissie over tot de gedeeltelijke schorsing van de methode aangezien hiervoor geen ontwerp van machtiging voorlag en geen eensluidend advies was bekomen. '*Overwegende dat de BIM-commissie in haar beslissing tot gedeeltelijke schorsing terecht stelde dat er, wat dat onderdeel van de methode betreft, geen eensluidend advies was verstrekt door de BIM-Commissie. Dat zij daarop terecht een gedeeltelijke schorsing uitsprak, voor wat betreft de tweede gsm*', aldus het Comité.

In dossier 2015/3545 ten slotte had de BIM-Commissie een negatief advies verleend bij een ontwerp van machtiging. Bij vergissing werd de uitzonderlijke methode toch gemachtigd door het diensthoofd. Toen de vergissing aan het licht kwam, werd de methode onmiddellijk stopgezet. Ze werd nadien ook onwettig verklaard door het Comité. '*Overwegende dat in afwezigheid van een eensluidend advies van de BIM-Commissie, de uitzonderlijke methode niet in uitvoering kan gebracht worden gelet op artikel 18/10 § 3 tweede lid en dat tegen die beslissing van de van de BIM-Commissie geen beroep mogelijk is*' (vertaling).

III.2.2.1.3. Verplichte vermeldingen in de toelating

In vier dossiers moest het Vast Comité I zich buigen over de vraag of in een toelating van het diensthoofd bepaalde gegevens verplicht dienen te worden opgenomen. Het betrof de datum van de beslissing, de naam van de target en het correcte wetsartikel inzake de bevoegdheid van de dienst.

Zo was de toelating tot een specifieke methode niet gedagtekend (dossier 2015/4065). Het Comité oordeelde dat de beslissing hierdoor niet nietig was, in tegenstelling met wat bepaald is in artikel 18/10 § 2, eerste lid, W.I&V voor uitzonderlijke methoden.

Ook de naam van de target moet niet per definitie in de beslissing vermeld staan (dossiers 2015/4064 en 2015/4065). Het Comité stelde vast dat de vermelding van de identiteit van een target niet vereist wordt door de wet en dat hij op een andere wijze identificeerbaar was, zodat er zich *in casu* geen probleem stelde om de wettigheid, proportionaliteit en subsidiariteit te beoordelen. Het Comité benadrukte tevens dat de geheimhoudingsverplichtingen die rusten op de leden van een inlichtingendienst de wettelijke controleopdracht zoals omschreven in artikel 43/5 §§ 1 en 4 W.I&V niet in de weg kan staan.

In het laatste dossier (2015/3687) had de betrokken inlichtingendienst een foutief wetsartikel vermeld. De dienst wenste via een technisch middel te achterhalen waar en wanneer een target zijn gsm gebruikte. Vervolgens zouden de door hem gecontacteerde nummers geïdentificeerd worden. Het Comité merkte op dat de dienst '*ten onrechte, bij de juridische kwalificatie van de methode, beroep doet*

op art. 18/4 W.I&V in combinatie met art. 18/7, § 1, 1° W.I&V'. Artikel 18/4 W.I&V viseert enkel de observatie van personen, zaken, plaatsen of gebeurtenissen. Het gebruikte technische middel werd slechts aangewend om een identificatie van telefoonnummers te bekomen. Het Comité oordeelde dat de '*operatie in zijn geheel moet worden bekeken bij het kwalificeren van de methode*' zodat de dienst zich enkel had moeten beroepen op artikel 18/7 § 1, 1° W.I&V voor beide onderdelen van de methode. Maar dit maakte de methode niet onwettig.

III.2.2.1.4. Hoogdringendheidsprocedure bij de vordering van een operator

Een inlichtingendienst was bij hoogdringendheid overgegaan tot de kennisname, identificatie en lokalisatie van oproepgegevens van een bepaald toestel (art. 18/7 § 2 en art. 18/8 § 2 W.I&V) (dossier 2015/4171). De vereiste mondelinge beslissing van het diensthoofd was bevestigd door een met reden omklede schriftelijke beslissing. Deze beslissing was ter kennis gebracht van de BIM-Commissie die bijkomende inlichtingen wenste over de duur van de methode. Maar, onder verwijzing van een eerdere uitspraak (dossier 2011/227), merkte het Comité op dat in de beslissing nog een aantal andere elementen ontbraken: de naam van de vorderende inlichtingenofficier, datum en uur van de vordering en datum en uur van de schriftelijke bevestiging. *'Overwegende dat de afwezigheid van informatie over voorgaande elementen het Vast Comité I niet toelaat om te beoordelen of de voorwaarden gesteld in art. 18/7 § 2 en 18/8 § 2 van de W.I&V om beroep te doen op de procedure voor een vordering bij hoogdringendheid, werden nageleefd'* (vertaling). Op verzoek van het Comité kon de betrokken dienst deze gegevens alsnog verschaffen. De methode werd dan ook wettelijk bevonden.

III.2.2.1.5. Rechtmatigheid van de hoogdringendheidsprocedure

Omdat de inzet van een uitzonderlijke methode zeer dringend moest kunnen plaatsgrijpen, vroeg de inlichtingendienst aan de voorzitter van de BIM-Commissie of het *in casu* mogelijk was zeer snel een beslissing te bekomen van de voltallige Commissie (dossier 2015/3530). Zo niet zou hij een beroep doen op de hoogdringendheidsprocedure *ex* artikel 18/10 § 4 W.I&V. De voorzitter raadde aan om deze uitzonderingsprocedure te hanteren omdat het volgens hem onmogelijk was de Commissie die dag nog bijeen te roepen. Er werd dan ook samen afgesproken alleen het mondelinge advies van de voorzitter in te winnen. Enkele dagen later bevestigde de voorzitter zijn mondelinge advies en, in uitvoering van artikel 10 van het KB van 12 oktober 2010, deelde hij zijn beslissing mee aan de andere leden van de Commissie. Het Comité stelde vast dat '*de voorzitter van de BIM-Commissie geoordeeld heeft dat het niet mogelijk was om de Commissie vrijdagnamiddag bijeen te roepen, dit om redenen die hem toebehoren en waarover het Vast Comité I zich niet heeft uit te spreken; Overwegende echter dat het Vast Comité I doet opmerken dat deze beslissing op een vrijdagnamiddag werd genomen tijdens*

de normale kantooruren en dat, in geval van verhindering van een of meer leden van de BIM-Commissie, plaatsvervangende leden zijn benoemd die kunnen gecontacteerd worden om het verhinderde lid of leden te vervangen; Overwegende dat het Vast Comité I in casu moet beoordelen of de beslissing van de inlichtingendienst om een beroep te doen op de hoogdringendheidsprocedure al dan niet wettig is; Overwegende dat in dit geval de urgentie van de situatie en de ernst van de dreiging maakten dat men zonder uitstel moest gebruik maken van de procedure bepaald bij art. 18/10 § 4' (vertaling).

De methode was dan ook voor 48 uren gemachtigd. Maar aangezien deze termijn afliep tijdens het weekend en de noodzaak van verdere uitvoering zich aandiende, moest worden uitgemaakt of de verlenging via de gewone of via de uitzonderingsprocedure zou gebeuren (dossier 2015/3531). Daartoe nam de betrokken dienst opnieuw contact op met de voorzitter van de BIM-Commissie. Zowel de dienst als de voorzitter waren er van op de hoogte dat er zich een verlenging van de methode zou opdringen en dat dit in het weekend zou moeten gebeuren. Toch opteerde de voorzitter er voor om zijn Commissie niet onmiddellijk of tijdens het weekend bijeen te roepen. Het Comité merkte op dat '*een vergadering van de BIM-Commissie vóór het verstrijken van de 48 uren, mogelijk was door de andere leden en/of hun plaatsvervangers bijeen te roepen; Overwegende dat het Vast Comité I in casu moet beoordelen of de beslissing van de inlichtingendienst om een beroep te doen op de hoogdringendheidsprocedure al dan niet wettig is; Overwegende dat in gelijkaardige omstandigheden het Vast Comité I reeds heeft beslist dat in geval van onmogelijkheid om, om welke reden ook, de BIM-Commissie bijeen te roepen met het oog op een beslissing over een uitzonderlijke methode, de inlichtingendienst een andere in de wet voorziene procedure mag hanteren zoals een beroep doen op de bevoegde minister zonder het aflopen van de termijn van vier dagen ex art. 18/10 § 3 van de wet, af te wachten (BIM dossier 2012/1308 – 2012/1309 – 2013/2327 et 2013/2328)*' (vertaling).

III.2.2.2. Motivering van de toelating

Beslissingen tot het hanteren van bijzondere methoden moeten voldoende accuraat gemotiveerd worden. Zoals ieder jaar diende het Vast Comité I een aantal malen te wijzen op deze verplichting.

Een inlichtingendienst wenste zoveel als mogelijk aan de weet te komen over de Belgische contacten van een aantal buitenlandse gsm-nummers (dossier 2015/4101). Daarbij wou hij ook bepaalde lokalisatie- en identificatiegegevens inwinnen. Maar deze aspecten van de methode werden niet gemotiveerd zodat '*bij afwezigheid van een motivering de twee methoden onwettig zijn*' (vertaling) (dossier 2015/4101).

Ook in dossiers 2015/4150 en 2015/4170 stelde het Comité vast dat de methoden in de toelating niet gemotiveerd waren. Het besloot dan ook tot de onwettigheid.

In zijn beslissing om een observatie te verrichten had het diensthoofd in de ene paragraaf gesteld dat de methode een termijn van twee maanden zou bestrijken, terwijl verder in de tekst sprake was van een termijn van één maand (dossier 2015/4163). Het Comité stelde bovendien vast dat voor hetzelfde target voorheen telkens een methode werd voorgesteld die slechts één maand bestreek. '*Overwegende dat, derhalve, mede gelet op de tegenstrijdigheid qua termijnen vermeld in de BIM-beslissing, het Vast Comité I van oordeel is dat de methode slechts gedurende 1 maand kan worden toegepast*'. Het Comité besliste dan ook dat de methode gedeeltelijk onwettig was.

III.2.2.3. De proportionaliteits- en de subsidiariteitseis

Een methode dient niet alleen te voldoen aan een aantal wettelijke vereisten, ze moet ook in verhouding staan tot de onderliggende dreiging en ze mag niet intrusiever zijn dan noodzakelijk.

Een inlichtingendienst wil overgaan tot de identificatie van de communicatiemiddelen van een persoon, de kennisname van zijn communicatiegegevens en lokalisatie van de oorsprong en de bestemming van de communicaties en dit gedurende een lange periode (15 maanden) (dossier 2015/3818). De dienst wenste onder meer na te gaan of die persoon '*al dan niet betrokken zou kunnen zijn in een processus van rekrutering door een vreemd land*' (vertaling). Het Comité oordeelde weliswaar dat '*de potentiële dreiging reëel is, gelet op de afkomst van de target en de praktijken van het betrokken land en dat de gewone methoden niet toelaten de gezochte informatie te verkrijgen*' (vertaling), maar het stelde zich vragen bij de proportionaliteit: '*de methode tot identificatie (artikel 18/7§ 1-1°) en tot kennisname (artikel 18/8§ 1-1°) laat toe om nuttige informatie te bekomen maar de lokalisatie (artikel 18/8§ 1-2°) lijkt op dit ogenblik disproportioneel in verhouding met de reële ernst van de beschreven dreiging, gezien het meer intrusieve karakter van deze methode*' (vertaling).

In twee dossiers (2015/3999 en 2015/4000) wenste de dienst gedurende zes maanden een aantal specifieke methoden toe te passen op een target waarvan geweten was dat hij zich in die periode een paar dagen op het Belgisch grondgebied zou bevinden. De dienst specifieerde dat de methode alleen op dat moment zou worden toegepast. Het Comité vond, gegeven de concrete elementen van het dossier, de termijn van zes maanden niet proportioneel en oordeelde dat '*de methode, in de huidige stand van zaken, slechts gedurende 1 maand kan worden toegepast*.'

In dossier 2015/4154 wou de betrokken dienst drie specifieke methoden inzetten: de opsporing van oproepgegevens, de identificatie en de lokalisatie van elk Belgisch nummer dat in contact stond met een buitenlands nummer. Het Comité oordeelde dat '*de beginselen van proportionaliteit en subsidiariteit slechts worden nageleefd voor zover de methode van lokalisatie enkel en alleen beperkt*

wordt tot de lokalisatie van de opgespoorde telefoonnummers op het moment van de communicatie met het buitenlandse target. Dat inderdaad de geïdentificeerde nummers nooit het voorwerp kunnen uitmaken van een algemene lokalisatie, dus ook buiten de contacten die zij hebben met het buitenlandse target. Het Comité stelde daarom vast dat '*de specifieke methode […] onder de hoger vermelde precisering wettig is*'.

Wanneer een inlichtingendienst de observatie van een bepaalde locatie met een vaste camera met een jaar wil verlengen (de methode liep toen reeds meerdere jaren), stelt zich de vraag naar de proportionaliteit (dossier 20156/4199). Het Comité wees er op dat '*de W.I&V geen bijzondere procedures bepaalt voor de verlenging of de vernieuwing van een specifieke methode, met uitzondering van het feit dat de nieuwe beslissing van het diensthoofd moet beantwoorden aan de voorwaarden bepaald in artikel 18 § 3 van de wet; dat de wet geen striktere voorwaarden oplegt om de proportionaliteit en de subsidiariteit te beoordelen*' (vertaling). Aangezien de te maken beelden inlichtingen konden opleveren over een organisatie die als terroristisch wordt beschouwd en omdat inlichtingenwerk zich noodzakelijk over een lange periode afspeelt, had het Comité geen bezwaar tegen deze verlenging. Het Comité wees er overigens op dat het eerdere werk reeds vruchten had afgeleverd. *'Dat het Comité reeds meerdere malen heeft beslist dat de duur van één jaar redelijk was gelet op de opdrachten van de inlichtingendiensten die er onder meer in bestaan om te werken op middellange of lange termijn; dat deze bijzonderheid in de aard van het inlichtingenwerk essentieel verschilt van het politiewerk dat specifiek gelieerd is met het opsporen van de daders van een misdrijf*' (vertaling).

In de drie laatste dossiers ten slotte greep het Comité terug naar zijn vaste rechtspraak die stelt dat in bepaalde gevallen eerst de resultaten van eerdere methoden gekend moeten zijn, vooraleer kan uitgemaakt worden of de daaropvolgende methoden proportioneel en subsidiair zijn.

Zo wenste een inlichtingendienst tal van specifieke methoden in te zetten om een maximum aan gegevens te bekomen over een bepaald gsm-nummer: de kennisname van in- en uitgaande oproepen; de lokalisatie ervan, waarbij de dienst ook één jaar terug wou gaan in de tijd; de identificatie van de bekomen nummers indien ze niet via een gewone methode konden worden bekomen; de historiek van de gebruikers van het gsm-nummers sinds zijn eerste activatie; nagaan in welke gsm-toestellen dit nummer is gebruikt en – ten slotte – de identiteit van de gebruikers van deze toestellen nagaan. Het Comité oordeelde dat deze laatste methode onwettig was. Vooreerst dienden de resultaten van de andere methoden te worden afgewacht (dossier 2015/3842).

In dossier 2015/4101 was dezelfde problematiek aan de orde. Een inlichtingendienst wou tal van gegevens bekomen over de Belgische contacten van een aantal buitenlandse gsm-nummers. Daartoe zou de dienst vooreerst kennis nemen van de oproepgegevens van die buitenlandse nummers om op basis daar-

van de Belgische nummers te filteren. Maar in dezelfde beslissing wenste men meteen een hele reeks verdere methoden uit te voeren op de verkregen nummers. De BIM-Commissie ging over tot een gedeeltelijke schorsing: '*gelet op het feit dat op het ogenblik van de notificatie het niet mogelijk is om de resultaten van nog uit te voeren methoden te onderwerpen aan het legaliteits-, subsidiariteit- en proportionaliteitsonderzoek alvorens wordt overgegaan tot een bijzondere inlichtingenmethode*'. Het Comité oordeelde ook dat de dienst in eerste instantie diende na te gaan of en welke Belgische nummers in contact stonden met de buitenlandse nummers en wie de gebruiker er van was. '*Overwegende dat het op dit ogenblik niet mogelijk is om te oordelen over de wettelijkheid, de proportionaliteit en de subsidiariteit van elke andere methode die betrekking heeft op deze Belgische nummers, die eventueel zouden geïdentificeerd worden via de wettige methoden*' (vertaling).

In een laatste dossier (2015/4322) wou de dienst in eerste instantie kennis nemen van de oproepgegevens vanuit een bepaald gsm-toestel en overgaan tot de identificatie van de personen waarmee de target het afgelopen jaar in contact was gekomen. Maar vervolgens was het ook de bedoeling om over te gaan tot de kennisname van de oproepgegevens van andere telefoonnummers van dezelfde target. Het Comité oordeelde dat dit laatste niet toegelaten was. '*Overwegende dat de derde gevraagde methode betrekking heeft op een aantal nummers die tot op heden onbekend zijn en waarvoor de dienst de kennisname van in- en uitgaande oproepen vraagt en hun lokalisatie; dat zelfs indien de titularis van de gsm die het voorwerp uitmaakt van de methode gekend is, het mogelijk is dat hij anonieme prepaid kaarten heeft gebruikt, die het voorwerp zouden moeten uitmaken van bijzondere opsporingen of dat hij kaarten heeft gebruikt die hem geleend werden door andere personen die al dan niet een band hebben met de geviseerde persoon; dat het, gelet op het gebrek aan een meer precieze identificatie, op dit ogenblik niet mogelijk is het respect voor de principes van proportionaliteit en subsidiariteit te beoordelen voor deze verkregen nummers*' (vertaling).

III.2.2.4. Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging

De inlichtingendiensten kunnen uiteraard niet zomaar elke techniek aanwenden om bij wie dan ook informatie in te winnen. De wet stelt duidelijke grenzen en dit op diverse niveaus: Voor welke dreiging en ter verdediging van welk belang mag een methode worden aangewend? Welke handelingen mogen daarbij gesteld worden en welke niet? Door wie, ten aanzien van wie én ten aanzien van welke gegevens? Hoelang mag een techniek worden aangewend? Mogen de maatregelen buiten België worden toegepast?… In enkele beslissingen verduidelijkte het Vast Comité I bepaalde van deze grenzen.

III.2.2.4.1. Welbepaalde (ernstige) dreiging tegen welbepaald te verdedigen belang

Een inlichtingendienst wenste een bijzondere methode toe te passen op een persoon die mogelijk nuttige informatie kon aanleveren maar die zelf geen bedreiging op zich vormde (dossier 2015/4064). Het Comité benadrukte dat de wet het gebruik van BIM-methoden niet voorziet in dergelijke gevallen. Maar uit de beslissing bleek duidelijk dat de betrokkene activiteiten ontwikkelde die onder de bevoegdheid van de dienst vielen. Het Comité oordeelde dan ook dat die activiteiten de methode rechtvaardigden.

In dossier 2015/4320 stelde het Comité vast dat de bijzondere methoden ten dele ingezet werden op een problematiek die niet tot de bevoegdheid van de betrokken inlichtingendienst behoorde. De dienst wenste observaties uit te voeren op een welbepaald persoon die op dat ogenblik op de vlucht was en op een aantal andere personen van wie vermoed werd dat ze de voortvluchtige verborgen hielden. Het Comité oordeelde dat '*de persoon die in eerste instantie geviseerd werd door de methode niet gelokaliseerd is en dat deze persoon daarenboven actief opgespoord wordt door de gerechtelijke autoriteiten voor zijn deelname aan extreem zware delictuele handelingen; dat het bijgevolg momenteel niet mogelijk is de betrokkene te observeren en dat, indien hij ontdekt wordt, de diensten hierover de gerechtelijke autoriteiten moeten informeren met het oog op zijn arrestatie; overwegende dat er in de huidige stand van zaken geen inlichtingenfinaliteit bestaat voor deze persoon, maar een gerechtelijke finaliteit die overigens moet primeren*' (vertaling). Wat betreft de andere personen speelde deze redenering niet: '*de inlichtingenfinaliteit is wel aanwezig onafhankelijk van het bestaan of niet van gerechtelijke vervolgingen tegenover hen; dat het inderdaad noodzakelijk is voor de inlichtingendienst om de personen die aan de gezochte persoon welke logistieke steun dan ook verlenen, beter te kennen en op te volgen*' (vertaling).

III.2.2.4.2. Medewerking van buitenlandse diensten

Het Comité oordeelde reeds eerder dat de Belgische inlichtingendiensten ook in het kader van de bijzondere methoden mogen samenwerken met buitenlandse partnerdiensten, weze het onder de voorwaarde dat de Belgische dienst de daadwerkelijke controle behoudt over de ingezette methode.[109]

In dossier 2015/3823 herhaalde het Comité die rechtspraak. Een Belgische inlichtingendienst verleende de machtiging om gesprekken af te luisteren en te registreren. Het bijzondere aan de zaak was dat het afluisterapparaat zou geplaatst worden door een buitenlandse inlichtingendienst. De buitenlandse dienst zou pas kennis nemen van eventueel gevoerde gesprekken op het moment dat de target

[109] Zie bijvoorbeeld VAST COMITÉ I, *Activiteitenverslag 2013*, 83 en *Activiteitenverslag 2014*, 85-86.

zich in het buitenland bevindt. De bekomen informatie zou naderhand wel worden gedeeld met de Belgische dienst. Conform artikel 13/1 § 2, vijfde lid W.I&V had de BIM-Commissie haar akkoord verleend met het feit dat de buitenlandse agenten het technisch middel zouden plaatsen. Het Comité preciseerde dat '*de interventie van de [buitenlandse] collega's enkel beperkt kan blijven tot noodzakelijke en rechtstreekse hulp of bijstand, voor zover dit essentieel is voor het welslagen van de methode. Dat de [Belgische dienst] bij deze methode er dan ook moet over waken om zelf op een zeer strikte manier meester te zijn en blijven van de operatie op Belgisch grondgebied. Overwegende dat het Vast Comité I daarnaast aan de [Belgische dienst] oplegt om ook strikt toe te zien op de verdere afwikkeling van de methode, en meer in het bijzonder toe te zien op wat er gebeurt met de geregistreerde communicatie. Dat immers blijkt dat de gevoerde gesprekken in eerste instantie zullen verwerkt worden door de [buitenlandse] dienst op [zijn] grondgebied, en pas nadien met de [Belgische dienst] zal worden gedeeld. Dat ook hier de [Belgische dienst] meester moet zijn en blijven van de operatie en de nodige verplichtingen moeten naleven inzake de overschrijving van relevante passages en latere vernietiging van de opname.*' Aangezien uit bijkomende informatie bleek dat de Belgische dienst aan deze eisen kon voldoen, stelde het Comité de wettigheid van de machtiging vast.

III.2.2.4.3. De BIM-Wet en het Verdrag van Wenen inzake diplomatiek verkeer van 18 april 1961

Het Comité nam opnieuw een beslissing (dossier 2015/3805) waarin het Verdrag van Wenen van 1961 aan de orde was.[110] Een inlichtingendienst wenste over te gaan tot een specifieke methode. Omdat de BIM-Commissie wou nagaan of die methode in overeenstemming was met de eisen van dit Verdrag, vroeg het de dienst tot tweemaal toe nadere gegevens. Desondanks kreeg de Commissie onvoldoende zicht op de precieze aard van de methode en ging daarom over tot de schorsing. Het Vast Comité I oordeelde dat deze schorsing terecht was nu er *in casu* een mogelijkheid bestond dat de methode een schending inhield van het Verdrag.

III.2.2.5. De gevolgen van een onwettig(e) (uitgevoerde) methode

Een inlichtingendienst wenste een uitzonderlijke methode toe te passen in combinatie met enkele specifieke methoden. Aangezien de uitzonderlijke methode niet wettig bleek aangevraagd (zie hoger III.2.2.1.2. – dossier 2015/3545), schorste de BIM-Commissie ook de specifieke methoden '*ingevolge het rechtstreekse verband met de betrokken uitzonderlijke methode*' (vertaling). Het Vast Comité I was echter een ander oordeel toegedaan. '*Overwegende dat het Vast Comité I vaststelt dat de specifieke methoden niet in die mate verbonden zijn met de uitzonderlijke*

110 Zie ook VAST COMITÉ I, *Activiteitenverslag 2014*, 86.

methoden dat het lot van deze laatste automatisch het lot bepaalt van de andere methoden en dat het diensthoofd in zijn voorstel van beslissing en in zijn beslissing voldoende de inwerkingstelling van deze specifieke methoden heeft gerechtvaardigd, methoden die nog steeds een belang vertonen voor de dienst' (vertaling).

III.3. CONCLUSIES

Op basis van de cijfers uit het werkingsjaar 2015 trok het Vast Comité I volgende algemene conclusies:

- Daar waar er in 2014 een daling werd geregistreerd, kwam het aantal bijzondere methoden in 2015 terug op het niveau van 2013. De groei ten opzichte van 2014 situeerde zich volledig bij de door de VSSE ingezette specifieke methoden (van 976 in 2014 naar 1143 in 2015). Zowel de bijzondere methoden ingezet door de ADIV, als de uitzonderlijke methoden ingezet door de VSSE, kenden een significante daling.
- De toename van de specifieke methoden bij de VSSE situeerde zich voornamelijk in het aantal 'kennisnames van identificatiegegevens' (van 554 naar 663) en van 'kennisnames van lokalisatiegegevens' (van 248 naar 361). De 'kennisname van oproepgegevens' kende een daling (van 88 naar 33).
- Ondanks de lichte daling van het aantal uitzonderlijke methoden bij de VSSE viel er opnieuw een lichte stijging te noteren van het aantal tapmaatregelen: 81 in 2013, 86 in 2014 tot 91 voor 2015.
- Wat betreft de ADIV blijkt de tendens om minder BIM-methoden in te zetten in de strijd tegen terrorisme en extremisme zich in 2015 door te zetten (30 in 2013, 22 in 2014 en slechts 17 in 2015). Dat mag verbazen gezien de relatieve toename van deze dreigingen in 2015. Ook inzet van BIM-methoden tegen de dreiging 'spionage' kende in 2015 een neerwaartse trend (101 tegen 123 in 2014).
- Wat betreft de VSSE is het aantal BIM-methoden inzake 'terrorisme' niet alleen in absolute cijfers maar ook in verhouding tot de andere dreigingen zoals 'extremisme' en 'spionage', enorm toegenomen. De inzet van de beschikbare BIM-middelen is dus gedeeltelijk verschoven naar de strijd tegen het terrorisme.
- Tevens valt er te noteren dat er in het kader van de uitzonderlijke methoden steeds meer gebruik wordt gemaakt van de hoogdringendheidsprocedure waarbij alleen de voorzitter van de BIM-Commissie om advies wordt gevraagd: 11 maal in 2013; 19 maal in 2014 en 25 maal in 2015.
- Het Vast Comité I heeft in 2015 26 beslissingen genomen tegenover 17 in 2014. Deze stijging vindt zijn oorsprong in het feit dat het Comité zich in 2015 meer vatte (van 13 naar 16 keer) maar vooral omdat de BIM-Commissie vaker schorste (van 5 keer in 2014 naar 11 keer in 2015).

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).

Deze zogenaamde 'BIM-intercepties' moeten evenwel duidelijk worden onderscheiden van '*het zoeken, 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 tweede vorm van afluisteren was al langer mogelijk en kan worden ingezet 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 externe 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 Defensie 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 Comité I. Het Vast Comité I heeft in 2015 opnieuw[111] moeten aandringen op de overzending van de lijst. Hij werd pas midden april 2015 bezorgd.

---

111 VAST COMITÉ I, *Activiteitenverslag 2010*, 105 ('IX3.2. Tijdig overzenden van geviseerde veiligheidsintercepties').

Mede op basis van zijn bevindingen naar aanleiding van de Snowden-onthullingen[112] en gelet op de verklaringen van de ADIV dat het in de toekomst de mogelijkheid wil benutten om telecommunicatiekabels af te tappen, nam het Comité zich voor om zijn kennis over de SIGINT-activiteiten van de ADIV te verdiepen en te actualiseren onder de vorm van een studie. Het Comité startte in de tweede helft van 2015 met diverse concrete inspecties en bezoeken en liet zich voorlichten tijdens meerdere briefings.[113] De studie werd in 2016 gefinaliseerd en in juli overgelegd aan de minister van Defensie en de ADIV.

112 VAST COMITÉ I, *Activiteitenverslag 2014*, 8-35 ('II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten').

113 In 2015 werd ook een advies gegevens over een nieuw internationaal samenwerkingsverband met betrekking tot SIGINT-informatie (zie Hoofdstuk V.1.).

HOOFDSTUK V
ADVIEZEN, STUDIES EN ANDERE ACTIVITEITEN

Het takenpakket van het Vast Comité I is zeer verscheiden: het uitvoeren van toezichtonderzoeken; rechtscollege inzake bijzondere inlichtingenmethoden, opdrachten in het kader van de interceptiebevoegdheid van de ADIV, de invulling van gerechtelijke taken door zijn Dienst Enquêtes, zijn rol in het Beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen… Daarnaast levert het Comité ook studies af en wordt het geconsulteerd omwille van zijn expertise. Daarbij valt te noteren dat het Comité in 2015 driemaal werd verzocht een officieel advies te verlenen bij diverse kwesties.

V.1. ADVIES INZAKE INTERNATIONALE SAMENWERKING MET BETREKKING TOT SIGINT

Begin november 2015 verzocht de minister van Defensie het Comité om zijn advies in verband met een multilaterale samenwerking inzake *foreign terrorist fighters* (FTF) waarbij persoonsgegevens en meta-data worden uitgewisseld en gemeenschappelijke analyses worden opgesteld.

Gelet op het actuele belang en de noodzaak van een zo ruim mogelijke internationale samenwerking en informatie-uitwisseling én mede omwille van de beperkte eigen collectemiddelen van de Belgische inlichtingendiensten in het buitenland, verleende het Comité hiervoor een positief advies. Het herinnerde daarbij evenwel aan volgende beginselen:

– de medewerking moet zich beperken tot de problematiek van de FTF en de *returnees*. Indien de ADIV rond andere materies wil samenwerken, dienen die uiteraard binnen zijn bevoegdheid te vallen. Het Comité stelde wel dat het hiervan in kennis moet gesteld worden en dit in uitvoering van artikel 33, tweede lid, W.Toezicht;
– het Vast Comité I was van oordeel dat de ADIV in de huidige situatie bevoegd was voor de opvolging van de betrokken problematiek, vermits er een ernstig en reële militaire bedreiging uitgaat van FTF en *returnees* tegenover '*de bescherming of het voortbestaan van de bevolking*' (artikel 11 § 2, 1°, W.I&V).

Het Comité achtte het evenwel aangewezen de bevoegdheid van de ADIV inzake jihadistisch terrorisme duidelijker en ruimer vast te stellen op basis van een besluit dat kan genomen worden in uitvoering van artikel 11 § 1, 1° W.I&V[114];

- verder herinnerde het Comité met aandrang aan de verplichting opgenomen in artikel 20, § 3, W.I&V waarbij de Nationale Veiligheidsraad moet voorzien in de nodige richtlijnen inzake informatie-uitwisseling en samenwerking. Meer *in concreto*:
  - dient nader omschreven te worden welke criteria de ADIV moet hanteren bij zijn besluit om al dan niet (beperkt) samen te werken met bepaalde landen en hun respectieve inlichtingendiensten;
  - dienen nadere criteria te worden opgesteld voor het overzenden van (persoons)gegevens aan die derde landen waarmee (beperkt) wordt samengewerkt. Hierbij dient men alleszins oog te hebben voor het gebruik dat die derde landen kunnen maken van die informatie, bijvoorbeeld bij het opnemen ervan in 'zwarte lijsten'. Daarom dient onder meer voor elke meegedeelde informatie duidelijk te worden aangegeven welk gebruik er mag van worden gemaakt door die derde landen;
  - dienen de eisen van de Privacywet te worden gerespecteerd. Het Comité verwees onder meer naar de kwaliteit en de pertinentie van overgezonden gegevens. Met het oog hierop is een indicatie van de waarde van de meegedeelde informatie een nuttig instrument;
  - dienen versterkte garanties te worden voorzien voor de overzending van gegevens naar landen binnen het netwerk die niet dezelfde garanties zouden bieden op het vlak van dataprotectie (artt. 21 en 22 Privacywet);
- wanneer andere Belgische diensten (politie, gerechtelijke autoriteiten, VSSE …) door tussenkomst van de ADIV informatie willen delen via het samenwerkingsverband, dienen ze er zelf over te waken dat dit gebeurt binnen het kader van hun respectieve bevoegdheden. Tevens dienen de bevoegde administratieve of gerechtelijke overheden duidelijk aan te geven welke informatie kan meegedeeld worden, zeker indien het om persoonsgegevens gaat;
- wanneer de ADIV een *Request for Information* afkomstig van een andere Belgische dienst doorzendt naar het samenwerkingsverband, dient de ADIV er steeds over te waken dat deze vraag ook kadert binnen zijn eigen bevoegdheid. Zo dient de ADIV bijvoorbeeld de limieten van de mogelijkheden om '*medewerking en in het bijzonder […] technische bijstand te verlenen*' (artikel 20 W.I&V) in acht te nemen;
- het Vast Comité I oefent conform zijn wettelijke opdrachten een daadwerkelijk toezicht uit op alle aspecten van deze samenwerking.

---

114 De ADIV is bevoegd voor '*elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van het Ministerieel Comité*' (art. 11, § 1, eerste lid, W.I&V).

Tot slot stelde het Comité dat het aanbevolen is een algemene, politieke reflectie te houden over de werking van de ADIV wat betreft zijn bevoegdheden, SIGINT-mogelijkheden, bijstand aan gerechtelijke overheden en samenwerking met buitenlandse partners.

V.2. ADVIES OVER DE TOEKENNING VAN EEN VEILIGHEIDSMACHTIGING VOOR DE LEDEN VAN DE NIEUWE BEGELEIDINGSCOMMISSIE

Al in 2014 werd, ingevolge de zesde Staatshervorming, het Kamerreglement in die zin aangepast dat de begeleiding van het Vast Comité I en de parlementaire opvolging van de politie- en inlichtingendiensten moest gebeuren door een Begeleidingscommissie in de Kamer van Volksvertegenwoordigers. De mogelijkheid tot inzage in geclassificeerde informatie gekoppeld aan het bezit van een veiligheidsmachtiging voorafgegaan door een veiligheidsonderzoek, vormde daarbij opnieuw[115] onderwerp van debat.

Op verzoek van de voorzitter van de Begeleidingscommissie gaf het Vast Comité I hierover een advies op basis van de geldende wetgeving. Daarin werden een aantal voor- en nadelen weergegeven van deze of gene keuze en werden een aantal buitenlandse voorbeelden aangehaald.[116]

Finaal besliste de Commissie om niets te veranderen: de commissieleden wensten géén veiligheidsmachtiging en géén toegang tot geclassificeerde informatie.

Het feit dat geen geheime informatie mag meegedeeld worden aan de betrokken parlementsleden is niet noodzakelijk problematisch voor de kwaliteit van de democratische controle.[117] De praktijk heeft uitgewezen dat het Vast Comité I doorgaans op een betekenisvolle wijze kan rapporteren aan de Begeleidingscommissie, zonder daarbij geheimen prijs te geven.

---

115 Hierover werd reeds eerder gediscuteerd: Zie onder meer T. VAN PARYS, 'Van parlementaire onderzoekscommissie over Pinksterplan tot Toezichtwet' en H. VAN HEVELE, 'Parlementair toezicht na de Toezichtwet' in W. VAN LAETHEM en J. VANDERBORGHT, *Inzicht in toezicht, Twintig jaar democratische controle op de inlichtingendiensten*, Antwerpen, Intersentia, 2013.

116 Waar illustratief, werd een vergelijking gemaakt met naburige landen (hierover uitvoerig '4.5. Access to classified information by parliaments and specialised oversight bodies' in EUROPEAN PARLIAMENT, Directorate-General for Internal Policies, Policy Department Citizens' Rights and Constitutional Affairs, Justice, Freedom and Security, *Parliamentary oversight of security and intelligence agencies in the European Union*, 2011, 117-131).

117 Hierover: W. VAN LAETHEM, 'Alles onder controle! Een (ver)nieuw(d)e Kamercommissie die toeziet op de politie- en de inlichtingendiensten', *Vigiles*, 2015/1, 9-16., i.h.b. 14 e.v.

V.3. ADVIES BIJ EEN WETSVOORSTEL INZAKE HET TOEZICHT OP DE ACTIVITEITEN VAN BUITENLANDSE INLICHTINGENDIENSTEN IN BELGIË

In juli 2015 vroeg de Begeleidingscommissie op basis van artikel 33, zevende lid, W.Toezicht het advies van het Vast Comité I bij het wetsvoorstel tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten aangaande het toezicht op de activiteiten van de buitenlandse inlichtingendiensten in België.[118]

Het Comité benadrukte in zijn advies[119] dat het zich volledig akkoord verklaarde met de geest van het voorstel. Immers, het Comité had reeds diverse malen[120] aanbevolen om werk te maken van een wetswijziging waarbij de Belgische veiligheids- en inlichtingendiensten expliciet bevoegd zouden worden gemaakt voor de opvolging van de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied, los van een eventuele dreiging van spionage, inmenging, extremisme… De achterliggende idee is daarbij dat de activiteiten van buitenlandse inlichtingenagenten op het grondgebied potentieel problematisch zijn.

V.4. ACADEMISCHE ZITTING

In 2015 knoopte het Comité opnieuw aan met de traditie om een academische zitting te organiseren. Deze had als thema 'Het belang van opleiding in de inlichtingenwereld' en vond plaats in de Senaat. Het onderwerp werd toegelicht door professor Philip H.J. Davies, directeur van het *Brunel Centre for Intelligence and Security Studies* (Londen), Lucile Dromer-North, directrice van de Franse *Académie du renseignement* en luitenant-generaal Eddy Testelmans, chef ADIV.

In het kader van deze zitting werd door de ministers van Justitie en Defensie de officiële oprichtingsakte ondertekend van de *Belgian Intelligence Academy* (BIA). Deze academie organiseert opleidingen[121] voor analisten uit zowel de burgerlijke als de militaire inlichtingendienst en heeft als missie '*de motor en de referentie [te] vormen op vlak van de professionele opleiding inzake burgerlijke en militaire inlichtingen, en in deze te worden erkend voor zijn expertise en zijn competenties. Hij heeft als opdracht te voorzien in kwaliteitsvolle, gemeenschappelijk en gestructureerde opleidingen voor het personeel van de inlichtingendiensten*' (vrije vertaling).

---

118 *Parl. St.* Kamer, 2014-15, 54K0553/001.

119 *Parl. St.* Kamer, 2014-15, 54K0553/002.

120 Zie VAST COMITÉ I, *Activiteitenverslag 2006*, 132; *Activiteitenverslag 2008*, 2; *Activiteitenverslag 2012*, 91; *Activiteitenverslag 2014*, 3.

121 In 2015 vonden twee opleidingsmomenten ('Basisopleiding Analyse') plaats.

V.5. CONFERENTIE IN HET EUROPEES PARLEMENT OVER HET DEMOCRATISCH TOEZICHT OP DE INLICHTINGENDIENSTEN

Hoewel de werkzaamheden van de inlichtingendiensten binnen de bevoegdheid van de EU-Lidstaten vallen en artikel 4, lid 2, van het Verdrag betreffende de werking van de Europese Unie (VWEU) duidelijk bepaalt dat de nationale veiligheid de uitsluitende verantwoordelijkheid van elke lidstaat blijft, tonen recente gebeurtenissen aan dat het meer dan ooit nodig is samen te werken tussen de nationale inlichtingendiensten en in het verlengde hiervan, hun toezichthoudende organen in de hele Unie. De ontwikkeling van een EU-strategie voor interne veiligheid toont eveneens aan dat het nodig is de samenwerking en de uitwisseling van nationale informatie te verbeteren. Bovendien is het zo dat, hoewel de preventie van veiligheidsbedreigingen, zoals terreuraanvallen, een strikt nationale bevoegdheid blijft, de vervolging ervan juridische en justitiële samenwerking vereist, zoals expliciet wordt erkend in artikel 83 VWEU.

Binnen bovenstaande context organiseerde de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement, samen met de Belgische Kamer van Volksvertegenwoordigers, de Duitse *Bundestag* en het Italiaanse Parlement op 28 en 29 mei 2015 een conferentie over het democratisch toezicht op inlichtingendiensten in de Europese Unie.[122] De conferentie stelde zich tot doel relevante nationale en Europese spelers op het vlak van inlichtingendiensten en het toezicht hierop samen te brengen om recente ontwikkelingen en de gevolgen hiervan voor hun respectieve bevoegdheidsterreinen, te bespreken. Zowel de voorzitter van de Begeleidingscommissie, Siegfried Bracke, als de voorzitter van het Vast Comité I, Guy Rapaille, namen tijdens deze conferentie het woord.

V.6. EXPERT OP DIVERSE FORA

Leden van het Vast Comité I en van zijn personeel werden in 2015 diverse malen als expert geconsulteerd door binnen- en buitenlandse publieke en private instellingen:

– de voorzitter van het Vast Comité I oefent sinds 2011 het voorzitterschap uit van het *Belgian Intelligence Studies Centre (BISC)*. Het centrum stelt zich tot doel de inlichtingen- en veiligheidsdiensten en de wetenschappelijke wereld dichter bij elkaar brengen en een bijdrage te leveren aan de reflectie over inlichtingenvraagstukken.[123] In 2015 organiseerde het BISC twee studieda-

[122] www.europarl.europa.eu/activities/committees/nl/LIBE/home.html.
[123] www.intelligencestudies.be.

gen: een eerste over 'Politie en inlichtingenactiviteiten tijdens de Groote Oorlog: parallellen naar vandaag' (juni 2015) en een tweede ter gelegenheid van een aantal 'verjaardagen': 185 jaar Veiligheid van de Staat, 100 jaar militaire veiligheid, 70 jaar Koninklijke Unie der Inlichtings- en Actiediensten (KUIAD) en vijf jaar BISC[124];
- een vertegenwoordiger van het Vast Comité I nam deel aan een panelgesprek 'Hoe kostbaar is onze online privacy' georganiseerd naar aanleiding van de vertoning van de documentaire 'Citizenfour' van Laura Poitras over de Snowden-onthullingen;
- er werd eveneens een beroep gedaan op de expertise van het Comité in een praktijkseminarie bestemd voor politie, magistratuur en advocatuur inzake de 'screening van personen' en dit in de context van de Wet betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;
- in november 2015 nam een delegatie van het Vast Comité I deel aan de tweede expertenmeeting '*National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies*', georganiseerd op initiatief van het hoofd van de *Sector of Information Society, Privacy and Data Protection Freedoms and Justice Department* van het *European Union Agency for Fundamental Rights* (FRA). Deze is, in opdracht van het Europees Parlement en naar aanleiding van de Resolutie van 12 maart 2014, belast met een vergelijkende studie over democratisch toezicht op de inlichtingendiensten in de Europese lidstaten[125];
- de voorzitter van het Vast Comité I en de griffier begeleidden eind april 2015 een delegatie van de Commissie voor Landsverdediging bij hun bezoek aan de inlichtingendiensten. In het Kwartier Koningin Elisabeth werd de delegatie ontvangen door luitenant-generaal Eddy Testelmans, ACOS IS, chef ADIV om vervolgens te worden verwelkomd in de lokalen van de VSSE door administrateur-generaal Jaak Raes;
- het Comité blijft tevens deelnemen aan de vergaderingen van de *Groupe européen de recherche sur l'éthique du renseignement* (GERER). Hierin reflecteert een werkgroep, samengesteld uit vertegenwoordigers vanuit het academische wereld en practici (vertegenwoordigers vanuit de (militaire) Franse, Belgische

---

124 Dit ging gepaard met de publicatie van twee omstandige uitgaven (M. COOLS et al. (eds.), *1915-2015. Het verhaal van de Belgische militaire inlichtingen- en veiligheidsdienst*, Antwerpen, Maklu, 2015, 672 (met onder meer een bijdrage van de voorzitter van het Vast Comité I: 'Le SGRS et le Comité permanent R: "une aventure en terre inconnue"', 577-586) en Baron R. COEKELBERGS et al. (eds.), *Gedenkboek Inlichtings- en Actie Agenten*, Antwerpen, Maklu, 2015, 860) alsook met de tentoonstelling 'Classified' in Brussel (7 november tot 5 december 2015).

125 European Union Agency for Fundamental Rights, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks* (http://fra.europa.eu).

en Luxemburgse inlichtingendiensten, het Vast Comité I…) over de relatie 'ethiek – inlichtingendiensten';
- in 2015 was een vertegenwoordiger van het Vast Comité I aanwezig op een aantal vergaderingen van de zogenaamde 'Werkgroep Analyse'[126];
- in maart 2015 gaf de voorzitter op vraag van het Departement de Sciences Politiques van de Rechtsfaculteit van de Universiteit van Luik een uiteenzetting over '*Le renseignement, ses défis et son contrôle*';
- in april 2015 nam de voorzitter van het Comité, op uitnodiging van de Franse *Ecole nationale de la Magistrature* deel aan een rondetafelgesprek over *'Justice et renseignement: quelle coopération?*' in het kader van de opleiding '*La réponse judiciaire au terrorisme en Europe*';
- op uitnodiging van het *Geneva Centre for the Democratic Control of Armed Forces* (DCAF) nam de griffier van het Comité in het Tunesische 'Institut de Défense Nationale' deel aan een conferentie over parlementaire controle op de inlichtingendiensten. Deze conferentie vond plaats in het kader van een jaarlijkse cyclus onder de noemer '*L'établissement d'un nouveau service de renseignement pour la Tunisie*', gefinancierd door het *Fonds d'affectation pour l'Afrique du Nord* (TFNA) van het DCAF;
- verder nam de directeur van de Dienst Enquêtes I het woord op het 4Instance ICT-security colloquium (september 2015) waarbij de cyberbevoegdheden van de militaire inlichtingendienst werden toegelicht ('(Counter) Attack is the best Defence');
- ten slotte werd de griffier van het Vast Comité I in maart 2015 uitgenodigd in het kader van het opleidingsonderdeel 'Intelligence' van Master in de internationale betrekkingen en diplomatie (Universiteit Antwerpen) om er de werking van het Comité toe te lichten.

V.7. SAMENWERKINGSPROTOCOL MENSENRECHTEN

In België bestond geen publieke instantie die nagaat of de huidige en toekomstige wetgeving conform is met de arresten van het Europees Hof voor de Rechten van de Mens en met internationale mensenrechtenverdragen. Het ontbreken van een 'publieke mensenrechteninstantie' werd beschouwd als een aanzienlijke leemte.[127]

---

126 VAST COMITÉ I, *Activiteitenverslag 2014*, 93 en *Activiteitenverslag 2013*, 94.

127 De Mensenrechtenraad van de Verenigde Naties stelde dit vast in 2011 tijdens zijn zogenaamd 'Universeel Periodiek Onderzoek (UPO)'. In 2016 wordt België opnieuw aan dit onderzoek onderworpen. Eerder werd vanuit diverse hoeken aangedrongen om, net als in de buurlanden, ook in ons land een onafhankelijk, nationaal mensenrechteninstituut op te richten (zie bijvoorbeeld *Parl. St.* Kamer 2012-13, 53K2946/001).

Diverse voorbereidende vergaderingen met andere instellingen met een mandaat op gebied van mensenrechten[128], resulteerde halfweg januari 2015 in een samenwerkingsprotocol[129] waarin alle deelnemende instanties overeen kwamen om hun praktijken en methoden uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen. In afwachting van een formeel federaal mensenrechteninstituut zouden ze tevens fungeren als een gemeenschappelijk overlegplatform van instellingen die door een volledig of gedeeltelijk mandaat gelast zijn met het toezicht op de eerbiediging van de fundamentele rechten en vrijheden. De activiteiten van dit platform namen in 2015 de vorm aan van maandelijkse overlegvergaderingen waarin zowel algemene problematieken (bijvoorbeeld het verloop van het Universeel Periodiek Onderzoek van de VN-Mensenrechtenraad, maar ook de werking van het Beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen), als zeer concrete casussen worden besproken.

V.8. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

In het verlengde van een werkbezoek georganiseerd in Brussel (mei 2014) tussen een vertegenwoordiging van het Vast Comité I en de Nederlandse Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD), organiseerde het Nederlandse toezichtsorgaan halverwege november 2014 een tweede overlegmoment. De vergadering werd uitgebreid met vertegenwoordigers van de Zwitserse *Strategic Intelligence Service Supervision*. In oktober 2015 vond in datzelfde kader in Bern opnieuw een vergadering onder toezichthouders plaats. Ditmaal waren er ook delegaties vanuit Zweden (*Commission on Security and Integrity Protection*), Noorwegen (*Parliamentary Oversight Committee*) en Denemarken (*Intelligence Oversight Board*). Er werden vijf topics geagendeerd: (het meten van) efficiëntie, de toegang voor de toezichthouders tot informatie van de betrokken inlichtingendiensten, het inzicht in lopende operaties en de internationale uitwisseling van gegevens tussen inlichtingendiensten en tussen toezichthouders en het toezicht op het gebruik van persoonsgegevens door inlichtingendiensten.

De vergadering besliste een gelijkaardig toezichtonderzoek op te starten in alle deelnemende landen over de internationale samenwerking tussen de diverse inlichtingendiensten met betrekking tot de strijd tegen de *foreign terrorist fighters*. Dit initiatief kreeg nadien de uitdrukkelijke steun van de voorzitter van de Begeleidingscommissie. Het ligt daarbij in de bedoeling dat elke toezichthouder,

[128] Zoals het Unia (het voormalige Interfederaal Gelijkekansencentrum), het Federaal Migratiecentrum, het Instituut voor de gelijkheid van vrouwen en mannen, de Privacycommissie, de federale Ombudsman, de Hoge Raad voor Justitie, de Vaste Comités I en P.

[129] Samenwerkingsprotocol van 13 januari 2015 tussen de instellingen met een volledig of gedeeltelijk mandaat belast met de eerbiediging van de rechten van de mens.

vanuit zijn eigen perspectief en bevoegdheid maar vanuit eenzelfde filosofie en met een zekere gemeenschappelijke aanpak, dit thema bestudeert.

Verder onderhield het Vast Comité I in 2015 ook nauwe contacten met de Franse *Commission nationale de contrôle des interceptions de sécurité* (CNCIS) en de nieuwe *Commission nationale de contrôle des techniques de renseignement* (CNCTR). De voorzitter van het Comité stond eveneens een delegatie te woord van de Japanse *Survey Delegation of the House of Councillors*, tijdens hun '*fact-finding mission to learn about the protection of secrets and parliamentary involvement in these activities*'.

V.9. CONTROLE OP DE SPECIALE FONDSEN

Het Rekenhof houdt namens de Kamer van Volksvertegenwoordigers toezicht op het gebruik van de financiële middelen door overheidsdiensten. Het Rekenhof controleert de wettigheid en de rechtmatigheid van alle uitgaven. Dat geldt in principe ook voor alle uitgaven van de inlichtingendiensten. Echter, omwille van de gevoeligheid van de materie wordt een deel van het budget van de VSSE en de ADIV (met name de 'speciale fondsen' met uitgaven voor bijvoorbeeld operaties en informanten) niet onderzocht door het Rekenhof. Voor de VSSE wordt de controle van deze uitgaven verricht door de directeur algemeen beleid van de minister van Justitie. Sinds 2006 wordt de controle van de speciale fondsen van de ADIV alleen uitgevoerd door het hoofd van de Krijgsmacht en dit vier maal per jaar. Op suggestie van het Rekenhof gebeurt dit sinds 2010 in aanwezigheid van de voorzitter van het Vast Comité I.

V.10. AANWEZIGHEID IN DE MEDIA

Het Vast Comité I wordt regelmatig gesolliciteerd door de geschreven en gesproken media om toelichting te geven over zijn werkzaamheden dan wel deze van de inlichtingendiensten. Het Vast Comité I ging een aantal maal op deze verzoeken in.

Datum	Onderwerp/titel	Forum
13 januari 2015	'Nos services de renseignement et de sécurité sont-ils à la hauteur?'	RTBF
18 januari 2015	'Belgique: en guerre contre les terroristes?'	RTBF (Mise au point)
18 januari 2015	'Terreurdreiging: Comité I evalueert Belgisch veiligheidsapparaat'	MO*
18 januari 2015	'Services de sécurité: un débat sur les mesures prioritaires au Parlement?'	RTBF

Datum	Onderwerp/titel	Forum
25 januari 2015	'Le mystère de la toute nouvelle académie pour les espions belges pour lutter contre les terroristes'	RTL
11 maart 2015	'Staatsveiligheid heeft alleen nog tijd voor Syriëstrijders'	De Standaard
11 maart 2015	'Opvolging Syriëstrijders loopt gevaarlijk mank'	De Tijd
11maart 2015	'Syriëcrisis verstikt Staatsveiligheid'	De Tijd
11 maart 2015	'La crise syrienne étouffe la Sûreté de l'État'	L'Echo
22 april 2015	'Bescherming staatshoofden en vips in België is een knoeiboel'	Nieuwsblad
25 april 2015	'Screenings voor kerncentrales en andere hotspots falen'	De Tijd
25 april 2015	'La surveillance des centrales nucléaires présente des failles'	L'Écho
28 april 2015	'Proximus vraagt uitleg over 'mollen''	De Tijd
6 mei 2015	'Baas geheime dienst geeft foute info over drie aanslagen'	De Tijd
6 mei 2016	'De waarheid komt uiteindelijk toch bovendrijven'	MO*
8 mei 2015	'Quand la France prend exemple sur la Belgique du renseignement'	L'Écho
28 mei 2015	'Les services secrets allemands auraient piraté des câbles de communication de Belgacom'	La Libre Belgique
2 juni 2015	'Comité I vraagt controle op lijsten met terrorismeverdachten'	De Tijd
2 juni 2015	'Staatsveiligheid richt blik op gevangenissen'	De Tijd
3 juli 2015	'Militaire inlichtingendienst gaat datakabels bespioneren'	De Standaard
14 juli 2015	'Antiterreurorgaan komt in vaarwater van andere inlichtingendiensten'	De Standaard
15 juli 2015	'Activités de renseignements: l'OCAM sortirait de son rôle'	RTBF
15 juli 2015	'Antiterreurorgaan OCAD Iigt onder vuur wegens overschrijden bevoegdheid'	Knack
31 juli 2015	'Staatsveiligheid past meer drastische middelen toe'	Het Laatste Nieuws

Datum	Onderwerp/titel	Forum
16 september 2015	'Besluit Comité I: 'België heeft niet voor NSA gespioneerd''	Het Laatste Nieuws
16 september 2015	'Nos agents n'ont pas épié pour la NSA'	Le Soir
30 september 2015	'André Vandoren stopt dit jaar als topman antiterreurdienst OCAD'	De Tijd
30 september 2015	'André Vandoren quitte l'OCAM'	Le Soir
23 oktober 2015	'Guy Rapaille: 'Les services sont près d'un point de rupture''	Le Vif
26 oktober 2015	'Sûreté de l'État et Service Général de Renseignement et de Sécurité'	RTBF (Le Forum)
16 november 2015	'Drie personen gelinkt aan Parijse aanslagen stonden op lijst van Belgisch antiterreuror-gaan'	MO*
17 november 2015	'Comité I start onderzoek inlichtingendien-sten'	Het Laatste Nieuws
17 november 2015	'Nos services de renseignements pas la hauteur?'	RTBF
17 november 2015	'Drie daders stonden op terreurlijst'	De Morgen
17 november 2015	'Ging Staatsveiligheid de mist in?'	De Morgen
17 november 2015	'Voorzitter Guy Rapaille – TV journaal in verband met onderzoek Syrië'	RTBF
26 november 2015	'Tijdelijke commissie monopoliseert in Kamer volledig antiterreurbeleid'	De Standaard
26 november 2015	'Zo delen geheime diensten binnen de EU informatie met elkaar'	MO*
26 november 2015	'Militaire inlichtingendienst moet alerter zijn voor extremisme in leger'	De Standaard
27 november 2015	'La Belgique, miroir de l'Europe'	Le Vif
16 december 2015	'Staatsveiligheid en Nationale Bank onder vuur'	De Tijd
16 december 2015	'La Sûreté de l'État a désormais accès à nos comptes bancaires'	L'Écho

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.[130] 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) en 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).

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*

130 Hierover uitvoerig: P. NIVELLE, 'Een parlementair controleorgaan met een gerechtelijke opdracht … Over de tweede pet van de Dienst Enquêtes I', in W. VAN LAETHEM en J. VANDERBORGHT, *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, Intersentia, Antwerpen, 2013, 295-305.

is voor de uitoefening door het Vast Comité I van zijn opdrachten' (art. 43, derde lid, W.Toezicht).

Ook in 2015 voerde de Dienst Enquêtes I onderzoeksdaden uit in het kader van gerechtelijke onderzoeken.

Een eerste dossier betrof een onderzoek in opdracht van de gerechtelijke overheden te Luik. Samen met de Federale gerechtelijke Politie onderzocht de Dienst Enquêtes I de mogelijke betrokkenheid van een lid van een inlichtingendienst in sociale en fiscale fraude.[131] In 2015 nam de enquêtedienst deel aan een reeks huiszoekingen uitgevoerd in het kader van dit onderzoek. Het dossier is nog steeds lopende.

Een tweede gerechtelijk onderzoek betrof de mogelijke betrokkenheid van een lid van een inlichtingendienst aan misdaden en wanbedrijven tegen de uitwendige veiligheid van de Staat.[132] Het dossier werd opgestart in 2014, kreeg uitvoering in 2015 en werd eind 2015 zonder gevolg geklasseerd.

In het kader van andere in 2014 opgestarte dossiers[133] werden door de Dienst Enquêtes I geen gerechtelijke opdrachten uitgevoerd.

131 Over datzelfde gerechtelijk onderzoek, zie VAST COMITÉ I, *Activiteitenverslag 2012*, 78.

132 Het betrof een dossier aangaande oneigenlijk gebruik van geclassificeerde gegevens en gegevens afkomstig van een derde dienst.

133 VAST COMITÉ I, *Activiteitenverslag 2014*, 100.

HOOFDSTUK VII

DE GRIFFIE VAN HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN

De voorzitter van het Vast Comité I neemt ook het voorzitterschap van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen waar. De griffiefunctie wordt uitgeoefend door de griffier 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 kan het Beroepsorgaan ook optreden 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.[134]

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 de 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.

In 2015 daalde het aantal beroepen en beslissingen significant tegenover het jaar voordien, te weten van respectievelijk 171 naar 130 en van 163 naar 137. Deze dalende tendens is zichtbaar in het aantal beroepen tegen negatieve veiligheidsadviezen en, zij het in mindere mate, tegen het aantal geweigerde veiligheidsattesten

134 Zie hierover uitgebreid het *Activiteitenverslag 2006* van het Vast Comité I (91-119).

voor het betreden van plaatsen of gebeurtenissen. Daartegenover moet worden vastgesteld dat het aantal geweigerde veiligheidsmachtigingen waartegen beroep werd ingesteld, is gestegen terwijl dit aantal in 2014 nog gedaald was tegenover 2013. Ten slotte moet opgemerkt worden dat het aantal beroepen tegen beslissingen in het kader van veiligheidsmachtigingen die buiten de wettelijke termijn werden genomen, zeer sterk gedaald is van 15 in 2013 en 2014 naar 2 in 2015.

Achter deze dalende cijfers gaat echter een toegenomen werklast schuil voor zowel de griffie als voor het Beroepsorgaan zelf. De te behandelen dossiers worden immers steeds complexer op het vlak van administratief beheer, de terechtzittingen en de beslissingen.

Zo bijvoorbeeld blijken de administratieve dossiers die door de veiligheidsoverheden worden overgemaakt, niet steeds compleet zodat de griffie bijkomende handelingen moet stellen om ze te vervolledigen. Hetzelfde geldt voor de toepassing van artikel 5 § 3 W.Beroepsorgaan: het verzoek om bepaalde stukken niet ter inzage te verlenen van de verzoeker is zelden gemotiveerd of gaat uit van de verkeerde instantie, zodat de griffie ook hier bijkomende informatie moet inwinnen.

Verder dient te worden vastgesteld dat de zittingen veel meer tijd in beslag nemen dan een aantal jaren geleden. Dit heeft verschillende oorzaken. Steeds meer verzoekers laten zich bijstaan door een advocaat die ter zitting het standpunt van zijn cliënt toelicht. Ook vragen de betrokken politie- of inlichtingendiensten steeds vaker om te worden gehoord. Gelet op de complexiteit van sommige zaken, wordt hier veel tijd aan besteed. Ten slotte moeten – anders dan vroeger – veel zaken op een tweede of derde zitting worden hernomen, ofwel omdat een verzoeker uitstel vraagt ofwel omdat in het dossier gewacht wordt op bijkomende informatie.

Ook het beslissingsproces zelf vergt meer tijd dan een aantal jaren geleden. Hiervoor zijn twee belangrijke redenen aan te halen. Enerzijds worden er meer procedurele kwesties opgeworpen (bijv. debat over ontvankelijkheid, taalproblematiek, rechten van verdediging, motiveringsplicht…). Anderzijds wordt het Beroepsorgaan vaker geconfronteerd met extreem gevoelige dossiers die verband houden met de problematiek van de radicalisering en met de actuele terreurdreiging. Dergelijke dossiers vereisen uiteraard een uiterst zorgvuldige behandeling en een aangepaste motivering. Daarenboven nopen ze soms tot specifieke veiligheidsmaatregelen.

Tabel 1. Betrokken veiligheidsoverheid

	2013	2014	2015
Nationale Veiligheidsoverheid	98	99	68
Veiligheid van de Staat	1	0	1
Algemene Dienst inlichting en veiligheid	78	60	47

Federaal Agentschap voor Nucleaire Controle	9	8	10
Federale politie	1	3	3
Lokale politie	2	1	1
TOTAAL	**189**	**171**	**130**

Tabel 2. Aard van de bestreden beslissing

	2013	2014	2015
Veiligheidsmachtigingen			
Vertrouwelijk	5	5	9
Geheim	56	43	35
Zeer geheim	5	4	4
Totaal veiligheidsmachtigingen	66	52	48
Weigering	41	25	36
Intrekking	5	9	7
Weigering en intrekking	4	-	-
Machtiging voor beperkte duur	1	2	3
Machtiging voor lager niveau	0	1	0
Geen beslissing binnen termijn	15	15	2
Geen beslissing binnen verlengde termijn	0	0	0
Totaal veiligheidsmachtigingen	66	52	48
SUBTOTAAL VEILIGHEIDSMACHTIGINGEN	**66**	**52**	**48**
Veiligheidsattesten geclassificeerde documenten			
Weigering	0	4	6
Intrekking	0	0	0
Geen beslissing binnen termijn	0	0	0
Veiligheidsattesten plaats of gebeurtenis			
Weigering	15	16	12
Intrekking	0	0	1
Geen beslissing binnen termijn	0	0	0
Veiligheidsadviezen			
Negatief advies	106	99	63
Geen advies	2	0	0
'Herroeping' van een positief advies	0	0	0
Normatieve rechtshandelingen	0	0	0
Beslissing van publieke overheid om attesten te eisen	0	0	0

	2013	2014	2015
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	**123**	**119**	**82**
TOTAAL BESTREDEN BESLISSINGEN	**189**	**171**	**130**

Tabel 3. Hoedanigheid van de verzoeker

	2013	2014	2015
Ambtenaar	4	0	4
Militair	26	17	29
Particulier	159	145	93
Rechtspersoon	0	6	4

Tabel 4. Taal van de verzoeker

	2013	2014	2015
Franstalig	92	92	75
Nederlandstalig	97	76	54
Duitstalig	0	0	0
Anderstalig	0	0	1

Tabel 5. Aard van de door het Beroepsorgaan genomen voorbereidende beslissingen[135]

	2013	2014	2015
Volledig dossier opvragen (1)	187	168	130
Aanvullende informatie opvragen (2)	12	16	7
Horen lid overheid (3)	3	11	7
Beslissing voorzitter (4)	0	0	0

135 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 2015, terwijl de beslissing pas viel in 2016.

	2013	2014	2015
Informatie uit dossier halen door Beroepsorgaan (5)	68	78	50
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.
(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

	2013	2014	2015
Dossierinzage door klager / advocaat	103	84	84
Horen van de klager / advocaat[136]	138	115	107

Tabel 7. Aard van de beslissingen van het beroepsorgaan

	2013	2014	2015
Veiligheidsmachtigingen			
Beroep onontvankelijk	2	0	4
Beroep zonder voorwerp	3	3	3
Beroep ongegrond	20	12	19
Beroep gegrond (volledige of gedeeltelijke toekenning)	35	14	24
Bijkomende onderzoeksdaden door overheid	0	0	0
Bijkomende termijn voor overheid	14	12	1

136 In bepaalde dossiers wordt de klager/advocaat meermaals gehoord.

	2013	2014	2015
Zonder gevolg	–	–	1
Veiligheidsattesten geclassificeerde documenten			
Beroep onontvankelijk	0	0	0
Beroep zonder voorwerp	0	0	0
Beroep ongegrond	0	2	4
Beroep gegrond (toekenning)	0	0	2
Veiligheidsattesten plaats of gebeurtenis			
Beroep onontvankelijk	1	0	0
Beroep zonder voorwerp	0	0	0
Beroep ongegrond	6	6	8
Beroep gegrond (toekenning)	11	8	10
Verleent akte van afstand van beroep	–	–	2
Veiligheidsadviezen			
Beroep onbevoegd	0	4	0
Beroep onontvankelijk	4	4	6
Beroep zonder voorwerp	1	4	0
Bevestiging negatief advies	25	53	28
Omvorming in positief advies	65	41	23
Beroep tegen normatieve rechtshandelingen	0	0	0
Verleent akte van afstand van beroep	–	–	2
TOTAAL	**187**	**163**	**137**

HOOFDSTUK VIII
DE INTERNE WERKING VAN HET VAST COMITÉ I

VIII.1. SAMENSTELLING VAN HET VAST COMITÉ I

De samenstelling van het Comité bleef in 2015 ongewijzigd: voorzitter Guy Rapaille (F), advocaat-generaal bij het hof van beroep te Luik en raadsheren Gérald Vande Walle (F) en Pieter-Alexander De Brock (N).

Ook bij de Dienst Enquêtes I vielen er geen wijzigingen te noteren. De dienst bestaat uit vijf commissaris-auditoren, waaronder de directeur Frank Franceus (N).

De administratieve staf van het Vast Comité I, onder leiding van griffier Wouter De Ridder (N), kende evenmin verschuivingen en bleef op een totaal van 16 personeelsleden.

VIII.2. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE

In de loop van 2015 vonden zes vergaderingen plaats met de Bijzondere Commissie belast met de parlementaire begeleiding van het Vast Comité van toezicht op de politiediensten en het Vast Comité van toezicht op de veiligheids- en inlichtingendiensten. Deze telde in 2015 nog steeds dertien stemgerechtigde leden[137], die als volgt werden aangewezen[138]: Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Hendrik Vuye (N-VA), Laurette Onkelinx (PS), André Frédéric (PS), Denis

[137] Hierover Art. 149, nr. 1 van het Reglement van de Kamer van Volksvertegenwoordigers (*'De Kamer wijst bij het begin van iedere zittingsperiode, overeenkomstig de artikelen 157 en 158, uit haar midden de vaste leden aan van de commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I, bedoeld in artikel 66bis van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, waarbij zoveel leden worden benoemd als nodig is opdat elke politieke fractie ten minste een commissielid telt. Artikel 22 is niet van toepassing'*).

[138] De samenstelling van de Commissie werd ondertussen in 2016 op vier plaatsen gewijzigd: Peter De Roover (N-VA), Hans Bonte (sp.a), Gilles Vanden Burre (Ecolo-Groen) en Vanessa Matz (cdH) namen de plaats in van Kamerleden Hendrik Vuye, Karin Temmerman, Stefaan Van Hecke en Christian Brotcorne.

Ducarme (MR), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld), Karin Temmerman (sp.a), Stefaan Van Hecke (Ecolo-Groen) en Christian Brotcorne (cdH). De Commissie vergadert onder het voorzitterschap van Kamervoorzitter Siegfried Bracke (N-VA).

In zijn plenaire vergadering van 26 maart 2015 werd door de Kamer het 'Huishoudelijk reglement van de Commissie bedoeld in artikel 66*bis*, § 1, eerste lid, van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse'[139] goedgekeurd. Daarin werd onder meer opgenomen dat de leden van de commissie '*de nodige maatregelen nemen om de vertrouwelijke aard te waarborgen van de feiten, handelingen of inlichtingen waarvan zij wegens hun functie kennis krijgen*' en ze verplicht zijn het vertrouwelijke karakter ervan te bewaren (art. 7).

Tijdens de commissievergaderingen werden – achter gesloten deuren – diverse toezichtonderzoeken alsook het Activiteitenverslag 2014 van het Vast Comité I besproken. De Commissie nam '*akte van het activiteitenverslag 2014 van het Comité I en verleent haar goedkeuring aan de aanbevelingen van het Comité*'.[140] Ook werd een wetsvoorstel tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten aangaande het toezicht op de activiteiten van buitenlandse inlichtingendiensten geagendeerd en vond een gedachtewisseling plaats inzake de opstart van de toezichtonderzoeken naar aanleiding van de aanslagen in Parijs van november 2015.

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 voorzitterschap van deze gezamenlijke vergaderingen wordt afwisselend waargenomen door de voorzitters van beide Vaste Comités (art. 54 W.Toezicht). Het doel van de vergaderingen is tweeërlei: enerzijds het uitwisselen van informatie en anderzijds het bespreken van lopende gemeenschappelijke toezichtonderzoeken, zoals *in casu* de onderzoeken naar de *Joint Information Box* (II.1), naar de personeelsleden van het OCAD en sociale media (II.6), naar de internationale contacten van het OCAD (II.7) of nog, naar het bepalen – door het OCAD – van het niveau van de dreiging (II.11.9) en naar de informatiepositie van het OCAD, voorafgaand aan de aanslagen te Parijs in november 2015.[141]

In 2015 vonden zeven gemeenschappelijke vergaderingen plaats.

---

139 www.dekamer.be/kvvcr/pdf.sections/publications/reglement/controle.

140 *Parl. St.* Kamer 2014-15, nr. 54K1340/001 (Activiteitenverslag 2014 van het Vast Comité I, Verslag namens de bijzonder commissie).

141 Dit gemeenschappelijk toezichtonderzoek werd opgestart in 2016.

VIII.4. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Het budget 2015 van het Vast Comité I werd vastgelegd op 3,865 miljoen euro.[142] Dit houdt een vermeerdering in van 3% ten aanzien van het budget 2014, en was daarmee identiek aan de dotatie van 2013. Behalve de gewone verhoging van de werkingskosten, was dit budget eveneens voorzien om de eerder vastgestelde toegenomen werklast, op te vangen. Rationeel beheer van de ter beschikking gestelde fondsen en het uitstel van de aanwerving van twee bijkomende personeelsleden[143], leverden een budgettaire bonus op van 1,082 miljoen euro.

Deze positieve bilan verheelt evenwel een geheel andere financiële realiteit. De Commissie Comptabiliteit van de Kamer herbevestigde het eerder aangenomen principe waarbij *zoveel als mogelijk* de boni van het boekjaar worden toegekend aan de financiering van het eerstvolgende boekjaar. Daardoor verminderen de door de Staat toegekende bedragen voor de financiering van de dotatie. De jaarrekeningen van 2014 en 2015 hebben evenwel aangetoond dat deze middelen de reële uitgaven van het Comité – waarvan circa 80% bestemd voor personeelsuitgaven – niet meer dekten. Met andere woorden, het verschil tussen de inkomsten enerzijds en de uitgaven anderzijds werd gecompenseerd door de boni van het vorige boekjaar.

De beslissing van de Ministerraad van 15 oktober 2014 om het dotatiebudget jaarlijks lineair met 2% te verminderen, versterkt deze negatieve spiraal. In die mate zelfs dat de goede werking van het Comité hierdoor op termijn mogelijk kan door worden aangetast.

VIII.5. 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.

142 Wet van 19 december 2014 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2015, *BS* 29 december 2014.

143 Omwille van andere prioriteiten kon de aanwervingsprocedure pas in 2016 worden opgestart.

DATUM	TITEL	ORGANISATIE	PLAATS
2014-2015	Hogere Studies Veiligheid en Defensie, een multi-sectorale opportuniteit	KHID	Brussel
16 februari 2015	Balancing Counter-Terrorism and Human Rights. Challenges and Opportunities	Global Network for Rights and Development (GNRD)	Genève
13 maart 2015	Meeting met André Vandoren	ECSA	Brussel
12 en 13 maart 2015	Surveillance, Privacy and Transnational Relations in the Digital Era	International Association of Constitutional Responses to Terrorism	Brussel
9 en 10 april 2015	Conférence sur le contrôle démocratique des services de renseignement	DCAF/Institut de la Défense Nationale Tunisien	Tunis
13 april 2015	Les services spéciaux dans le monde Arabo-Musulman	Métis	Parijs
16 en 17 april 2015	La réponse judiciaire au terrorisme en Europe	Ecole Nationale de la Magistrature	Parijs
28 en 29 mei 2015	Conference on the Democratic Oversight of Intelligence Services in the European Union	European Parliament, Committee on Civil Liberties, Justice and Home Affairs	Brussel
25 juni 2015	8ème Conférence de l'Association Francophone des Autorités de Protection des Données Personnelles	AFAPDP	Brussel
26 juni 2015	Organisation de la cyber défense face à la menace actuelle	Haut comité français pour la défense civile (HCFDC)	Brussel
29 juni 2015	Politie en inlichtingenactiviteiten tijdens de Groote Oorlog: parallellen naar vandaag	BISC	Sint-Pieters-Leeuw
21 september 2015	Le renseignement: planification, stratégie et prospective	Métis	Parijs
24 september 2015	ICT-Security II	4Instance	Brussel
30 september 2015	L'intelligence stratégique au service du Plan Marshall 4.0?	HEC/ULG	Luik
5 oktober 2015	2015 ECSA Diplomatic Security Conference	ECSA	Brussel
17 oktober 2015	Quand l'invasion technologique menace nos libertés!	Université de Namur, Faculté de Droit	Namen

DATUM	TITEL	ORGANISATIE	PLAATS
23 oktober 2015	Meeting with Mr. Wil van Gemert, Deputy Director Europol	ECSA	Brussel
10 november 2015	185 jaar Veiligheid van de Staat, 100 jaar militaire veiligheid, 70 jaar KUIAD en 5 jaar BISC: pasts and futures	BISC	Brussel
12 november 2015	Juridische actuele vragen rond defensie	die Keure opleidings-centrum	Brussel
13 november 2015	Digital Enlightenment Forum. Policy and Strategy Debate. Security, Surveillance and Civil Liberties in Cyber Space	TrustCore.EU	Brussel

HOOFDSTUK IX
AANBEVELINGEN

Op basis van de in 2015 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. VEILIGHEIDSONDERZOEKEN EN SOCIALE MEDIA

Het Comité beveelt aan dat personen die het voorwerp zijn van een veiligheidsonderzoek, uitdrukkelijk kennis zouden krijgen van het feit dat de raadpleging van open bronnen – met inbegrip van de publieke profielen op sociale media – een van de methoden voor het verzamelen van informatie is die in dat kader kan ingezet worden.[144]

IX.1.2. DE STRIJD TEGEN EXTREMISME IN HET LEGER *VERSUS* FUNDAMENTELE RECHTEN

Om een overhaast oordeel te vermijden, vereist de opvolging van het radicaal islamisme in het leger een kritische ingesteldheid en behoedzaamheid bij de analyse van de gedragingen van personen. De ADIV moet gedragingen die, gelet op de vrijheid van eredienst, in overeenstemming zijn met een normale geloofsbeleving,

144 Hierover 'Hoofdstuk II.5. De personeelsleden van de inlichtingendiensten en de sociale media' en 'Hoofdstuk II.6. De personeelsleden van het OCAD en de sociale media'.

kunnen onderscheiden van gedrag dat wijst op een radicale en sektarische ontsporing.[145]

IX.1.3. ACCURATE INFORMATIE EN DE RECHTEN VAN BURGERS[146]

Het Vast Comité I beveelt de inlichtingendiensten aan om bij verzoeken om informatie vanwege buitenlandse diensten of bij het plaatsen van personen op lijsten, bijzondere zorg te dragen voor de accuraatheid van hun inlichtingen en de juridische gegrondheid van de informatie-transmissie (zowel nationaal als internationaal), en dit met oog voor de mogelijke gevolgen voor de betrokkenen.

Daarenboven moet er getracht worden om een evenwicht te bereiken tussen enerzijds de collectieve veiligheidsvereisten en anderzijds de rechten van de burgers die op dergelijke lijsten voorkomen. Dit zou kunnen via multilaterale afspraken over bijvoorbeeld de creatie van een ombudsfunctie of van een extern toezicht op deze lijsten. Momenteel hebben nationale instanties zoals het Vast Comité I immers niet de bevoegdheid om de gegrondheid en rechtmatigheid van dergelijke lijsten en hun inhoud na te gaan.

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 *JOINT INFORMATION BOX*[147]

De Vast Comités I en P formuleerden diverse aanbevelingen om het systeem van de *Joint Information Box* (JIB) – een door het OCAD beheerde lijst met namen van personen en organisaties die een sleutelrol spelen in het radicaliseringsproces – fundamenteel te herbekijken:

– de rol van elke medewerkende dienst dient uitgeklaard te worden. Dit geldt ook voor het OCAD die, als analysedienst, zijn meerwaarde kan bewijzen ten aanzien van de informatie die wordt aangedragen door de ondersteunende diensten. Het OCAD vulde zijn rol als dreigingsanalyseorgaan in het kader

145 Deze aanbeveling vloeit voort uit het toezichtonderzoek naar de opsporing en opvolging van extremistische elementen bij het personeel van Defensie (Hoofdstuk II.3).

146 Zie 'Hoofdstuk II.8. Onterecht opgevolgd door de inlichtingendiensten'.

147 Zie 'Hoofdstuk II.1. Gemeenschappelijk toezichtonderzoek naar de Joint Information Box van het OCAD'.

van de JIB-lijst te minimalistisch in. Bij het coördineren van de analyse dient het OCAD een meer actieve rol te spelen. De dienst kan voor elke entiteit een inschatting maken van de specifieke dreiging die er van uitgaat op het vlak van de radicalisering;
- anderzijds lijkt het aangewezen dat een andere dienst (bijvoorbeeld de Algemene Directie Crisiscentrum) wordt aangewezen om de coördinatie van de uitvoering van de maatregelen op zich te nemen;
- het werken met parameters biedt de garantie dat de opname in de JIB niet willekeurig gebeurt. Een systeem van criteria is inderdaad noodzakelijk om de objectiviteit te handhaven;
- de Vaste Comités I en P onderlijnen de noodzaak om in de JIB informatie op te nemen die afkomstig is van lokale en nationale diensten op het terrein. De lokale niveaus dienen in de mogelijkheid te zijn hun vaststellingen in te brengen in het systeem en minstens *feedback* te krijgen over de al dan niet opname in de lijst en van de eventuele maatregelen. Het is inderdaad zo dat de eerste tekenen van radicalisering dikwijls op het lokale niveau (bijvoorbeeld via de wijkagent of de lokale antenne van de inlichtingendiensten) worden vastgesteld. De Comités zijn van oordeel dat grondig dient te worden uitgewerkt op welke wijze een zo adequaat mogelijke informatiestroom kan worden op gang gebracht, dit met respect voor de bestaande structuren;
- de informatie en analyses dienen zo snel én zo ruim mogelijk verspreid te worden bij de betrokken actoren, dit uiteraard rekening houdende met een eventuele classificatie en de *need to know*. Waar nodig, moeten bepaalde personen (bijvoorbeeld van het regionale of lokale niveau) over een veiligheidsmachtiging beschikken;
- gelet op de diversiteit en de specificiteit aan maatregelen die moeten of kunnen genomen worden ten aanzien van dragers van radicalisering[148] moet het voorstellen, het opleggen, het uitwerken en het opvolgen van maatregelen zo nodig worden toevertrouwd aan beter geplaatste instanties of werkgroepen, zodat de JIB-actoren zich kunnen toespitsen op hun kerntaak: inlichtingen aandragen en analyseren. In voorkomend geval dienen andere dan federale veiligheidsdiensten in het debat te worden betrokken. Het radicaliserend effect detecteren, neutraliseren of beperken van een persoon of een groepering, kan immers niet alleen op het federale niveau gebeuren.

De Vaste Comités I en P spraken hun steun uit voor alle in die zin gemaakte plannen zodat de JIB op korte termijn zou kunnen uitgroeien tot hét instrument bij uitstek om de dragers van alle vormen van de radicalisering in onze maatschappij zo ruim mogelijk in beeld te brengen en te beheersen. De Comités stelden tevens dat ze het door het OCAD aangekondigde gewijzigde werkproces van de JIB in een latere periode zullen onderzoeken.

148 Bedoeld wordt personen die een radicaliserend effect hebben op derden.

IX.2.2. AANBEVELINGEN INZAKE HET BEHEER VAN EN DE CONTROLE OP DE SPECIALE FONDSEN[149]

IX.2.2.1. Een wettelijk kader

Er moet een wettelijke of reglementaire bepaling worden opgesteld die het beheer van de speciale fondsen helder en nauwkeurig beschrijft. Voorts is het absoluut noodzakelijk dat voor beide inlichtingendiensten soortgelijke controles worden ingevoerd, zowel intern als extern. In de reglementaire bepaling moet onder meer worden vastgelegd volgens welke procedures de betrokken diensten eventuele jaarlijkse overschotten mogen behouden. Het is tevens aangewezen om de diensten voldoende te betrekken bij de begrotingscyclus.

IX.2.2.2. Specifieke aanbevelingen wat betreft speciale fondsen en de ADIV

- De bedragen die de ADIV ontvangt voor zijn gewone kredieten (die de personeels-, werkings- en investeringskosten omvatten) en het jaarlijks bedrag van de speciale fondsen, moeten duidelijk identificeerbaar zijn in de begrotingswet van Defensie die het Parlement elk jaar goedkeurt.
- De ADIV moet de organisatie van de 'subkassen' aanpassen. Dit moet gebeuren rekening houdend met de finaliteit van sommige kassen (bijvoorbeeld operationele autonomie voor bepaalde secties). Wat betreft de andere kassen acht het Comité het aangewezen om het beheer ervan te centraliseren.
- De ADIV moet een eenvormig en geïntegreerd normerend kader opstellen van de (vernieuwde) kassen. Meer bepaald moeten de procedures voor uitgaven worden geformaliseerd opdat de controle door de hiërarchie efficiënt zou verlopen en een toegevoegde waarde zou bieden. Tevens komt het erop aan de boekhouding van deze fondsen te gebruiken als een beheerinstrument door gebruik te maken van een eenvormig en betrouwbaar informaticasysteem.
- Voor uitgaven waarvoor de criteria van 'geheimhouding' en 'hoogdringendheid' niet van toepassing zijn, moet de ADIV in samenwerking met andere diensten van Defensie op zoek gaan naar gewone financieringsmiddelen. Zo komen er meer middelen vrij voor operationele uitgaven.

Het Comité wees erop dat een wijziging van de reglementering niet mag inhouden dat de opdrachten van de ADIV in gevaar worden gebracht. Het benadrukte dat deze fondsen absoluut noodzakelijk zijn voor de werking van ADIV. De aanbevelingen van het Comité mogen niet tot gevolg hebben dat deze dienst het gebruik van een deel van de fondsen verliest. Volgens het Comité moet de optimalisatie van het beheer van de fondsen van de ADIV gebeuren in overleg met de dienst. Tevens stelde het Comité dat de ADIV enerzijds op zoek moet gaan naar

[149] Zie 'Hoofdstuk II.2. Het beheer, het gebruik en de controle van de 'speciale fondsen''.

alternatieve financiering in samenwerking met andere diensten van Defensie, en anderzijds, op basis van de actueel beschikbare fondsen, er naar moet streven om het gebruik van die fondsen te integreren in zijn veiligheidsstrategie.

IX.2.2.3. Specifieke aanbevelingen wat betreft de speciale fondsen en de VSSE

- De VSSE moet de uitoefening van de functie van buitengewoon rekenplichtige meer valoriseren door een precieze functiebeschrijving op te stellen, door personeel op te leiden in deze functie en door voortgezette opleidingen hieromtrent te organiseren.
- De VSSE moet erover waken dat de continuïteit van de functie van buitengewoon rekenplichtige wordt verzekerd. Dit vereist meer bepaald dat een adjunct wordt aangesteld[150] en dat er werkprocessen worden opgesteld.

IX.2.2.4. Regelmatige informatiesessies

Het Comité dringt er op aan om voor het voltallige personeel van zowel de ADIV als van de VSSE regelmatig informatiesessies te organiseren over de voorwaarden inzake het gebruik van de fondsen.

IX.2.3. HET GEBRUIK VAN SOCIALE MEDIA DOOR PERSONEELSLEDEN VAN DE VSSE EN DE ADIV[151]

Het Vast Comité I beveelt aan dat de directies van de inlichtingendiensten initiatieven zouden nemen om het normerende kader (wetten, Koninklijke besluiten, interne richtlijnen, deontologische code…) dat toepasselijk is op de leden van de inlichtingendiensten, te expliciteren wat betreft de algemene houding inzake loyaliteit en voorzichtigheid op sociale netwerken en wat betreft de controlemiddelen die daartoe kunnen worden aangewend.

Het Comité had eerder[152] reeds aanbevolen dat de VSSE, in uitvoering van artikel 17 van het KB van 13 december 2006 houdende het statuut van de ambtenaren van de buitendiensten van de Veiligheid van de Staat, een (voorstel van) deontologische code zou opstellen en ter goedkeuring zou overleggen aan de minister van Justitie. Het Comité beval aan dat deze code zou beschrijven waarin de neutraliteits- en discretieplicht van de agenten van de VSSE bestaat. Bovendien vroeg het Comité toe te zien op de strikte inachtneming van deze code door een snelle en stelselmatige toepassing van de tuchtprocedure in geval van overtredin-

150 Deze aanbeveling is ondertussen achterhaald door de aanstelling van een plaatsvervangend buitengewoon rekenplichtige.

151 Hierover 'Hoofdstuk II.5. De personeelsleden van de inlichtingendiensten en de sociale media'.

152 VAST COMITÉ I, *Activiteitenverslag 2011*, 113 ('IX.2.8. Een deontologische code voor de agenten van de VSSE').

gen. Het Vast Comité I herhaalt deze aanbeveling en is van mening dat een dergelijke deontologische code gedragsregels moet stellen voor het 'goed gebruik' van sociale media.[153]

Het Comité beveelt de directie van de diensten verder ook aan om bijzondere maatregelen te treffen die aangeven op welke proactieve wijze het ICT-gebruik en het gedrag van de agenten op sociale netwerkdiensten, zowel voor professionele als persoonlijke doeleinden, kunnen worden gecontroleerd. Die maatregelen moeten natuurlijk rekening houden met de beginselen inzake finaliteit, proportionaliteit en transparantie en dit in functie van de bijzondere opdrachten van de diensten.

Tevens moet er een procedure worden ingevoerd die toelaat in geval van een incident de eventuele schade voor de betrokkene en de dienst te beoordelen, op passende wijze te reageren en corrigerende maatregelen te nemen om herhaling te voorkomen.

Onverminderd de eventuele intrekking van de veiligheidsmachtiging moeten de hiërarchische overheden overwegen om eventuele tuchtstraffen te nemen in geval van bewezen inbreuk op de veiligheidsregels en op de discretieplicht.

Ten slotte moeten de diensten hun agenten preventief wijzen op de risico's die gepaard gaan met hun aanwezigheid op sociale media en moeten ze algemene aanbevelingen kunnen formuleren en veiligheidsmaatregelen kunnen vaststellen die aangeven welke voorzorgsmaatregelen moeten worden getroffen en welke gedragingen moeten worden vermeden op de betrokken netwerken.

IX.2.4. HET GEBRUIK VAN SOCIALE MEDIA DOOR PERSONEELSLEDEN VAN HET OCAD[154]

Wat betreft het gebruik van sociale netwerkdiensten door de personeelsleden van het OCAD, formuleerden de Vaste Comités I en P volgende aanbevelingen:

- de inspanningen die de leiding van het OCAD al heeft geleverd om de veiligheidsrisico's die gepaard gaan met de aanwezigheid van zijn personeelsleden op sociale netwerksites aan te pakken (meer bepaald in het kader van het stuurcomité), moeten worden voortgezet;
- er moeten initiatieven worden genomen om het normatief raamwerk van het OCAD (wetten, Koninklijke besluiten, interne richtlijnen, deontologische code) te expliciteren met betrekking tot de algemene houding van loyaliteit en voor-

153 Het Comité is hierbij van oordeel dat de adviezen en voorschriften in de charters voor het gebruik van sociale netwerken zoals voorgesteld door de Federale Politie, de *Belgian Cyber Security Guide* of de Franse en Amerikaanse militaire overheden een nuttige inspiratiebron kunnen vormen bij het opmaken van die deontologische code, mits rekening wordt gehouden met de bijzondere opdrachten waarmee de leden van de inlichtingendiensten zijn belast en met de voorwaarden inzake vertrouwelijkheid en geheimhouding waaronder zij moeten werken.

154 Hierover 'Hoofdstuk II.6. De personeelsleden van het OCAD en de sociale media'.

zichtigheid die wordt verwacht van zijn medewerkers op sociale media en met betrekking tot de controlemiddelen die daartoe kunnen worden aangewend;
- de Nationale Veiligheidsoverheid (NVO) moet aan iedereen die het voorwerp uitmaakt van een veiligheidsonderzoek uitdrukkelijk meedelen dat de raadpleging van open bronnen, met inbegrip van openbare profielen op sociale media, een van de methoden vormt om daartoe bruikbare informatie te vergaren;
- er dienen regels voor 'goed gebruik' te worden uitgewerkt voor de personeelsleden die zich bedienen van die nieuwe communicatiemiddelen;
- er dienen in het raam van de bestaande regels[155], gerichte opzoekingsmiddelen te worden ingevoerd om na te gaan of die regels – die nog altijd kunnen worden aangepast aan de evolutie van de communicatiemiddelen – goed worden toegepast, zowel preventief door steekproeven als reactief in geval van incidenten of aanwijzingen van disfuncties gelinkt aan risicogedrag van personeelsleden op sociale media;
- de personeelsleden van het OCAD moeten worden geïnformeerd over hoe het gebruik van ICT en het gedrag van de medewerkers op sociale netwerksites, weze het voor beroeps- of voor privédoeleinden, proactief kunnen worden gecontroleerd. Die bepalingen zullen uiteraard rekening moeten houden met de beginselen van finaliteit, proportionaliteit en transparantie, in onderhavig geval aangepast aan de specifieke opdracht van de diensten;
- er moet een procedure worden ingevoerd om de schade te ramen en om te reageren teneinde een ongepaste verspreiding van informatie die schadelijk is voor de medewerker, en bij uitbreiding voor zijn dienst, te kunnen ondervangen en/of beheren. Naar het voorbeeld van de OPSEC[156]-methodologie, zou die procedure ook moeten voorzien in corrigerende maatregelen die moeten worden genomen om herhaling van een dergelijk incident te vermijden en de gevolgen ervan te beperken;
- de medewerkers van het OCAD moeten duidelijk worden ingelicht over het feit dat de volgende maatregelen kunnen worden genomen indien bewezen is dat de veiligheidsregels en de discretieplicht geschonden zijn:
  a) de intrekking van de veiligheidsmachtiging;
  b) een tuchtvervolging overeenkomstig het tuchtstelsel van de analisten van het OCAD;

---

155 Meer bepaald CAO nr. 81 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-line-communicatiegegevens (mails, internetgebruik, internet, intranet, extranet, SMS, chat, discussiefora…).

156 OPSEC of 'Operations Security' wordt gedefinieerd als *'a process that involves the identification and protection of generally unclassified critical information or processes that can be used by a competitor or adversary to gain real information when pieced together. Although the information sought under OPSEC isn't classified, it could give a competitor or other adversary advantage. OPSEC focuses on the identification and protection of information that could give enemies clues or capabilities to put one in a disadvantage*', in www.techopedia.com.

c) een einde maken aan de detachering van de betrokken medewerker en hem verwijzen naar de overheid van de dienst van oorsprong wanneer het gaat om een gedetacheerde medewerker;

– de toepassing van de voornoemde beginselen en maatregelen moet beoordeeld worden rekening houdend met de specifieke opdrachten waarmee de betrokkenen bekleed zijn binnen de inlichtingengemeenschap en met de voorwaarden van vertrouwelijkheid en geheimhouding waarin zij moeten werken.

IX.2.5. DE INTERNATIONALE RELATIES VAN HET OCAD[157]

Rekening houdend met de respectieve politieke en bestuurlijke verantwoordelijkheden van elke instantie die betrokken is bij het aanknopen van internationale contacten, formuleren de Vaste Comités I en P de volgende aanbevelingen:

– de contacten die het OCAD legt met (al dan niet) gelijkaardige buitenlandse diensten moeten transparant en traceerbaar zijn ten aanzien van de bevoegde ministers, de FOD Buitenlandse Zaken en de Belgische politie- en inlichtingendiensten;
– de Nationale Veiligheidsraad moet een richtlijn uitvaardigen om de specifieke internationale contacten van het OCAD met gelijkaardige buitenlandse of internationale diensten te verzekeren overeenkomstig het artikel 8, 3° W. OCAD.[158] In dat opzicht lijkt het nodig dat de richtlijn verduidelijkt welke de strategische partnerdiensten van het OCAD kunnen zijn, welke types van samenwerking kunnen worden aangegaan met die diensten en hoe kan worden bepaald of ze al dan niet 'gelijkaardig' zijn.[159]

Volgens de Vaste Comités I en P zou deze richtlijn minstens de volgende voorschriften moeten bevatten:

– dat het OCAD een lijst *up-to-date* houdt van de buitenlandse diensten waarmee het internationale contacten onderhoudt of wenst te onderhouden; dat die lijst wordt voorgelegd aan de Nationale Veiligheidsraad en wordt gepubliceerd in de halfjaarlijkse verslagen van het OCAD;

---

157 Hierover 'Hoofdstuk II.7. De internationale contacten van het OCAD'.

158 Er werden reeds akkoorden gesloten tussen het OCAD en de VSSE om een oplossing te bieden voor de problemen die veroorzaakt zijn door bepaalde internationale contacten van het OCAD. De Comités waren echter van oordeel dat een structurele oplossing vereist dat de Nationale Veiligheidsraad ter zake een richtlijn uitvaardigt.

159 De aanbeveling is ondertussen achterhaald in de zin dat de Nationale Veiligheidsraad in de loop van 2016 een dergelijke richtlijn uitvaardigde. Er werd evenwel nog niet afgetoetst of de richtlijn rekening hield met alle hieronder geformuleerde voorschriften.

- dat daartoe de betrokken ondersteunende diensten en klanten van het OCAD worden ingelicht en geraadpleegd voordat er contact wordt gelegd met een buitenlandse dienst, al dan niet gelijkaardig, meer bepaald de VSSE, de ADIV, de Federale Politie maar ook de FOD Buitenlandse Zaken. Dergelijke contacten en vormen van samenwerking die de politieke verantwoordelijkheid van de regering en/of de reputatie van het land in de internationale gemeenschap op het spel kunnen zetten, vereisen immers een politieke evaluatie en dekking. Met andere woorden, de bevoegde ministers moeten voldoende ingelicht zijn, zodat ze te allen tijde hun politieke verantwoordelijkheid kunnen nemen[160];
- dat de eventuele contacten die het OCAD zou willen aanknopen met bepaalde buitenlandse inlichtingendiensten voortaan worden gelegd via het kanaal van de VSSE of de ADIV;
- dat de eventuele contacten die het OCAD zou willen aanknopen met bepaalde buitenlandse politiediensten voortaan worden gelegd via het kanaal van het Commissariaat-generaal, Directie van de internationale politiesamenwerking (CGI) van de Federale Politie;
- dat de deskundigen die uit de politie- of inlichtingendiensten gedetacheerd zijn bij het OCAD, bij die contacten worden betrokken;
- dat elke aanknoping van een bilateraal contact met een buitenlandse dienst het voorwerp uitmaakt van een voorafgaande SWOT-analyse;
- dat elke aldus aangegane samenwerking met een buitenlandse dienst het voorwerp uitmaakt van een periodieke evaluatie op basis van de SWOT-criteria;
- dat, op zijn minst, over elke buitenlandse missie door een lid van het OCAD een schriftelijk en gedetailleerd verslag wordt opgesteld over de gelegde contacten en hun aard; dat die verslagen worden toegezonden aan de betrokken politie- of veiligheidsdiensten;
- dat elke mededeling van informatie aan een derde dienst wordt genoteerd in een *ad-hoc*-register;
- dat een overzicht van de internationale contacten van het OCAD en van de deelnames van zijn personeelsleden aan evenementen in het buitenland wordt opgenomen in elk halfjaarlijks verslag dat die dienst moet opstellen krachtens het artikel 10 § 4 W.OCAD;
- dat het OCAD een interne richtlijn opstelt om te bepalen welke praktische en veiligheidsregels er moeten worden gevolgd bij verplaatsingen naar het buitenland door leden van zijn directie en/of personeel in het kader van hun beroepsactiviteit;

[160] Zie in die zin ook een eerdere aanbeveling: VAST COMITÉ I, *Activiteitenverslag 2014*, 113 ('IX.1.3. De nood aan een politieke dekking voor samenwerkingsverbanden').

– dat het OCAD gebruik maakt van de beveiligde internationale verbindingen van de inlichtingendiensten om te corresponderen met buitenlandse diensten;
– dat het OCAD zelf geen verslag meer stuurt noch verspreidt aan buitenlandse ambassades.

Anderzijds achtten de Comités het wenselijk dat zowel de VSSE als de ADIV het OCAD zouden uitnodigen op overlegvergaderingen met buitenlandse inlichtingendiensten, zeker wanneer die handelen over informatie betreffende dreigingen die vallen onder de bevoegdheid van het OCAD. Bovendien zou het OCAD van de gelegenheid gebruik kunnen maken om hypotheses te toetsen, informatie uit de eerste hand te krijgen… Zo zouden de betrokken diensten hun wederzijds vertrouwen kunnen versterken met het oog op een betere samenwerking.

Deze aanbevelingen van de Vaste Comités I en P liggen in de lijn van het destijds geformuleerde gezamenlijke standpunt[161]:
– het OCAD is geen inlichtingendienst;
– het komt het OCAD niet toe om inlichtingen te verzamelen, in België noch in het buitenland, al was het maar om zelf de leemten te vullen die de inlichtingendiensten of ondersteunende diensten in zijn ogen zouden laten vallen;
– het is van belang dat dit orgaan erop toeziet dat er niet de minste ambiguïteit ontstaat over zijn wettelijke opdracht, zowel in zijn communicatie als in zijn contacten met andere Belgische of buitenlandse diensten.

IX.2.6. DE STRIJD TEGEN EXTREMISME IN HET LEGER[162]

De ADIV moet bijzondere aandacht besteden aan alle tekenen van bekering tot de radicale islam, zowel bij het burgerlijke personeel als bij het militaire personeel van Defensie. Een zelfde waakzaamheid is geboden voor extreemrechtse neigingen en criminele motorbendes, die in de eenheden soms als minder problematisch worden beschouwd.

Het Comité raadt daarom aan dat het ADIV-commando op dat vlak duidelijke instructies geeft aan de bevoegde secties en hen de opdracht geeft om ondubbelzinnige indicatoren van radicalisering te identificeren met het oog op het samenstellen van documentatie over deze problematiek.

Daartoe moet de ADIV ervoor zorgen dat alle nuttige informatiekanalen worden geoptimaliseerd. Zo moet er ruime aandacht worden besteed aan de kwaliteit van de contacten met de verschillende eenheden en andere diensten van Defensie.

---

161 VAST COMITÉ I, *Activiteitenverslag 2011*, 33-34 ('II.5. Een gepland werkbezoek in het buitenland door het OCAD').

162 Deze aanbevelingen vloeien voort uit het toezichtonderzoek naar de opsporing en opvolging van extremistische elementen bij het personeel van Defensie (Hoofdstuk II.3).

De verantwoordelijken en korpschefs van de eenheden moeten worden bewust gemaakt van de problematiek, meer bepaald via regelmatige informatiebriefings.

Ten slotte is het aan te raden om de communicatiekanalen en –procedures, zowel met de tuchtrechtelijke overheden binnen Defensie als met de politiediensten en gerechtelijke overheden, te evalueren. De ADIV moet steeds tijdig op de hoogte worden gebracht van administratieve maatregelen, sancties of veroordelingen met betrekking tot een personeelslid van Defensie. Dit soort communicatie moet systematischer gebeuren zodat te nemen maatregelen kunnen worden onderzocht, meer bepaald met betrekking tot veiligheidsmachtigingen. Bij problemen in de informatiestroom moet de minister op de hoogte worden gebracht zodat hij deze kan verhelpen.

IX.2.7. DE HERZIENING VAN HET VEILIGHEIDS-REGLEMENT VAN DE ADIV[163]

Het Comité beveelt aan dat de ADIV alle bepalingen betreffende de militaire veiligheid (met inbegrip van de INFOSEC-richtlijnen) zou bundelen in één enkel document (IF5). De ADIV verklaarde in 2015 dat zij hiermee een aanvang had genomen.

IX.2.8. EEN UITVOERIGE VERSLAGGEVING BIJ VEILIGHEIDSINCIDENTEN[164]

Van ieder veiligheidsincident dient de ADIV een uitvoerig verslag op te maken dat alle dimensies (niet alleen technisch, maar ook op vlak van het gedrag) onderzoekt en analyseert, vooral wanneer een van de betrokkenen houder is van een veiligheidsmachtiging. Dit verslag moet worden bezorgd aan de bevoegde veiligheidsautoriteit, eventueel samen met een voorstel van besluit.

IX.2.9. FINALISEREN VAN HET ARBEIDSREGLEMENT[165]

Het Vast Comité I beveelt aan dat de VSSE haar arbeidsreglement snel afwerkt en goedkeurt. Dit document moet ten minste de aspecten van de arbeidsduur, van ziekteverloven en van preventie omvatten. In het kader van de preventie is het

163 Zie 'Hoofdstuk II.9. Klacht over et verstrekken van persoonlijke informatie door een inlichtingenagent aan een derde'.

164 Zie 'Hoofdstuk II.9. Klacht over et verstrekken van persoonlijke informatie door een inlichtingenagent aan een derde'.

165 Hierover: 'Hoofdstuk II.10. De VSSE en de toepassing van de reglementering met betrekking tot ziekteverloven'.

aanbevelenswaardig dat de VSSE snel een *ad hoc* structuur creëert teneinde haar wettelijke verplichtingen na te komen. De VSSE moet onder andere een preventieadviseur aanwerven en een netwerk van vertrouwenspersonen instellen.

IX.2.10. OVERZENDEN VAN ALLE RELEVANTE INFORMATIE AAN HET OCAD[166]

Het Vast Comité I beveelt aan dat de inlichtingendiensten alle relevante informatie evenals de resultaten van onderzoeken die ze voeren in het kader van lopende dossiers stelselmatig bezorgen aan het OCAD, ook wanneer een dergelijk onderzoek geen bewijskrachtige resultaten oplevert.

IX.3. AANBEVELING IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

IX.3.1. DE INTERNATIONALE RELATIES VAN HET OCAD

De Vaste Comités I en P drongen er op aan dat de contacten die het OCAD legt met (al dan niet) gelijkaardige buitenlandse diensten, ook transparant en traceerbaar zouden zijn voor beide toezichtorganen. Tevens bevelen de Comités aan dat bepaalde elementen van die contacten zouden opgenomen worden in de activiteitenverslagen, die het OCAD via de Nationale Veiligheidsraad moet overzenden aan beide Comités (art. 10, § 4, W.OCAD).

166 Zie: 'Hoofdstuk II.8. Onterecht opgevolgd door de inlichtingendiensten'.

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 2015 TOT 31 DECEMBER 2015)

Wet 10 april 2014 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* 11 februari 2015

Wet 30 juli 2015 houdende eerste aanpassing van de algemene uitgavenbegroting voor het begrotingsjaar 2015, *BS* 30 juli 2015

Wet 10 augustus 2015 tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen om beter rekening te houden met de bedreigingen voor de samenleving en de nationale veiligheid in de aanvragen tot internationale bescherming, *BS* 24 augustus 2015

Wet 10 augustus 2015 houdende wijziging van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *BS* 28 augustus 2015

Wet 3 september 2015 houdende instemming met de Overeenkomst tussen de lidstaten van de Europese Unie, in het kader van de Raad bijeen, betreffende de bescherming van in het belang van de Europese Unie uitgewisselde gerubriceerde informatie, gedaan te Brussel op 25 mei 2011, *BS* 30 november 2015

Wet 14 december 2015 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 wat betreft het mandaat van de plaatsvervangende leden van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de inlichtingendiensten, *BS* 24 december 2015

Uittreksel uit arrest nr. 84/2015 van 11 juni 2015 (rolnummers 5856 en 5859) inzake de beroepen tot gedeeltelijke (artikel 5) of gehele vernietiging van de wet van 30 juli 2013 'houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering', ingesteld respectievelijk door de 'Ordre des barreaux francophones et germanophones' de door de vzw 'Liga voor Mensenrechten' en de vzw 'Ligue des Droits de l'Homme', *BS* 11 augustus 2015

K.B. 19 december 2014 houdende gedeeltelijke verdeling van het provisioneel krediet ingeschreven op het programma 14-53-5 van de algemene uitgavenbegroting voor het begrotingsjaar 2014 en bestemd voor de looncompensatie en de terugbetaling van vergoedingen en van kosten verbonden aan de ontplooiing en het functioneren van leden van de Federale Politie, van vertegenwoordigers van de Magistratuur en van personeelsleden van Justitie, van Buitenlandse Zaken, van Binnenlandse Zaken, van Financiën, van het Coördinatie Orgaan voor de Dreigings Analyse, van Defensie en andere overheidsdiensten belast met zendingen in het buitenland, *BS* 7 januari 2015

K.B. 28 januari 2015 tot oprichting van de Nationale Veiligheidsraad, *BS* 30 januari 2015

K.B. 2 juni 2015 tot oprichting van het Strategisch Comité en het Coördinatiecomité voor inlichting en veiligheid, *BS* 5 juni 2015

K.B. 23 augustus 2015 houdende samenstelling van de bestuurlijke Commissie door de inlichtingen- en veiligheidsdiensten belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, *BS* 31 augustus 2015

K.B. 8 september 2015 tot wijziging van verschillende koninklijke besluiten wat de benaming 'Nationale Veiligheidsraad' betreft, *BS* 17 september 2015

K.B. 27 september 2015 tot wijziging van het koninklijk besluit van 23 januari 2007 betreffende het personeel van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 2 oktober 2015

K.B. 27 september 2015 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, veiligheidsattesten en veiligheidsadviezen, *BS* 2 oktober 2015

K.B. 2 oktober 2015 houdende gedeeltelijke verdeling van het provisioneel krediet ingeschreven in het programma 03-41-1 van de algemene uitgavenbegroting voor het begrotingsjaar 2015 en bestemd tot het dekken van niet structurele uitgaven wat betreft de veiligheid, *BS* 8 oktober 2015

K.B. 30 oktober 2015 betreffende de rechtstreekse toegang van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten en de Dienst Enquêtes ervan tot de gegevens en de informatie van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt, *BS* 20 november 2015

K.B. 9 december 2015 betreffende de specifieke taken van de leden van het college van procureurs-generaal, *BS* 28 december 2015

M.B. 1 april 2015 betreffende de uitvoering van een veiligheidsverificatie bij de personeelsleden van het autonoom overheidsbedrijf Belgocontrol en derden, *BS* 15 april 2015

M.B. 29 juni 2015 tot wijziging van het ministerieel besluit van 5 december 2006 houdende aanwijzing van een selectiecomité belast met de evaluatie van de kandidaturen van de ondersteunende cel van de Veiligheid van de Staat, *BS* 8 juli 2015

Werving – uitslag – vergelijkende selectie van Nederlandstalige analist. Er zijn 20 geslaagden, *BS* 27 maart 2015

Oproep tot kandidaten voor de bestuurlijke Commissie voor de inlichtingen- en veiligheidsdiensten belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, *BS* 7 april 2015

Vergelijkende selectie van Franstalige Cyber Risk Prevention Specialisten (m/v) (niveau B) voor het Ministerie van Defensie, *BS* 1 juni 2015

Vergelijkende selectie van Nederlandstalige Cyber Risk Prevention Specialisten (m/v) (niveau B) voor het Ministerie van Defensie, *BS* 1 juni 2015

Vergelijkende selectie van Franstalige Cyber Risk Prevention Experts (m/v) (niveau A2) voor het Ministerie van Defensie, *BS* 1 juni 2015

Vergelijkende selectie van Nederlandstalige Cyber Risk Prevention Expert (m/v) (niveau A2) voor het Ministerie van Defensie, *BS* 1 juni 2015

Vergelijkende selectie van Franstalige Cyber Security Experts (m/v) (niveau A2) voor het Ministerie van Defensie, *BS* 1 juni 2015

Vergelijkende selectie van Nederlandstalige Cyber Security Expert (m/v) (niveau A2) voor het Ministerie van Defensie, *BS* 1 juni 2015

Vergelijkende selectie van Franstalige Cyber Security Specialist (m/v) (niveau B) voor het Ministerie van Defensie, *BS* 1 juni 2015

Vergelijkende selectie van Nederlandstalige Cyber Security Specialisten (m/v) (niveau B) voor het Ministerie van Defensie, *BS* 1 juni 2015

Oproep tot kandidaten voor de bestuurlijke Commissie door de inlichtingen- en veiligheidsdiensten belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, *BS* 5 juni 2015

Vergelijkende selectie van Nederlandstalige Cyber Risk Prevention Specialist (m/v) (niveau B) voor de Ministerie van Defensie werd afgesloten op 29 september 2015, *BS* 12 oktober 2015

Vergelijkende selectie van Nederlandstalige Cyber Security Specialist (m/v) (niveau B) voor de Ministerie van Defensie werd afgesloten op 29 september 2015, *BS* 12 oktober 2015

Bij koninklijk besluit van 29 oktober 2015 is, op verzoek van de heer Vandoren A., een einde gesteld aan de aanwijzing tot directeur bij het Coördinatieorgaan voor de dreigingsanalyse, met ingang van 31 december 2015 's avonds, *BS* 6 november 2015

Openstaande betrekking van directeur van het Coördinatieorgaan voor de dreigingsanalyse (wet van 10 juli 2006, *BS* 20 juli 2006) – oproep tot kandidaten, *BS* 19 november 2015

Vergelijkende selectie van Nederlandstalige systeembeheerders (m/v) (niveau B) voor de Veiligheid van de Staat, *BS* 24 november 2015

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 2015 TOT 31 DECEMBER 2015)

Senaat

Mededeling van de eerste minister, *Hand.* Senaat 2014-2015, 16 januari 2015, nr. 6-8, 10

Overzicht van de wetten die voor de hoven en de rechtbanken moeilijkheden bij de toepassing of de interpretatie ervan hebben opgeleverd – VERSLAG 2013-2014, *Parl. St.* Senaat 2014-15, nr. 6-0039/2

Kamer van Volksvertegenwoordigers

Beleidsverklaring – Defensie en Ambtenarenzaken, *Parl. St.* Kamer 2014-15, nr. 54K0020/024

Overzicht van de wetten die voor de hoven en de rechtbanken moeilijkheden bij de toepassing of de interpretatie ervan hebben opgeleverd – VERSLAG 2013-2014, *Parl. St.* Kamer 2014-15, nr. 54K0435/002

Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, aangaande het toezicht op de activiteiten van de buitenlandse inlichtingendiensten in België, *Parl. St.* Kamer 2014-15, nr. 54K0553/002

Wetsontwerp met betrekking tot geautomatiseerde verwerkingen van persoonsgegevens die noodzakelijk zijn voor de Belgische paspoorten en reisdocumenten, *Parl. St.* Kamer 2014-15, nrs. 54K0731/002 tot 54K0731/004

Huishoudelijk reglement van de commissie bedoeld in artikel 66*bis*, § 1, eerste lid, 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 2014-15, nrs. 54K0859/001 en 54K0859/002

Voorstel van resolutie tot het instellen van een onderzoek naar de mogelijkheid om te komen op een verbod op de financiering van moskeeën en islamitische instituten door middel van internationale geldstromen uit moslimfundamentalistische hoek, *Parl. St.* Kamer 2014-15, nr. 54K0868/001

Voorstel van resolutie betreffende de toekomst van het Belgisch leger, *Parl. St.* Kamer 2014-15, nr. 54K0908/001

Voorstel van resolutie over het Europees beleid tegen radicalisme en terrorisme, *Parl. St.* Kamer 2014-15, nr. 54K0915/001

Wetsvoorstel tot wijziging van de wet van 2 juni 1998 houdende oprichting van een Informatie- en Adviescentrum inzake de schadelijke sektarische organisaties en van een Administratieve coördinatiecel inzake de strijd tegen schadelijke sektarische organisaties, teneinde het toepassingsveld ervan te verruimen tot de therapeutische sekten, *Parl. St.* Kamer 2014-15, nr. 54K0968/001

Hoorzittingen – De Belgische Defensie in de toekomst, *Parl. St.* Kamer 2014-15, nr. 54K0975/001

Voorstel van resolutie inzake de toekomst van Defensie, *Parl. St.* Kamer 2014-15, nrs. 54K0988/001, 54K0988/002, 54K0988/006 en 54K0988/007 en *Hand.* Kamer 2014-15, 2 april 2015, CRIV54PLEN037, 43

Voorstel tot wijziging van het Reglement van de Kamer van Volksvertegenwoordigers, teneinde te waarborgen dat de bijzondere commissie Legeraankopen de wapenhandel daadwerkelijk controleert, *Parl. St.* Kamer 2014-15, nr. 54K0994/001

De Europese Raad van staatshoofden en regeringsleiders van 12 februari 2015 (debriefing), *Parl. St.* Kamer 2014-15, nr. 54K0995/001

Bespreking van het Justitieplan, *Parl. St.* Kamer 2014-15, nr. 54K1019/001

Commentaar en opmerkingen bij de ontwerpen van aanpassing van staatsbegroting voor het begrotingsjaar 2015, *Parl. St.* Kamer 2014-15, nr. 54K1026/002

Wetsontwerp houdende eerste aanpassing van de Algemene uitgavenbegroting voor het begrotingsjaar 2015, *Parl. St.* Kamer 2014-15, nr. 54K1027/001

Wetsontwerp tot wijziging van de wet van 1 augustus 1979 betreffende diensten bij een vreemde leger- of troepenmacht die zich op het grondgebied van een vreemde Staat bevindt, *Parl. St.* Kamer 2014-15, nr. 54K1078/001

Stand van zaken van de veiligheid van de Belgische kerncentrales, *Parl. St.* Kamer 2014-15, nr. 54K1105/001

Urgentieverzoeken vanwege de regering: 1. Wetsontwerp tot wijziging van de wet van 21 maart 1991 betreffende de hervorming van sommige economische overheidsbedrijven (1187/1) 2. Wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen om beter rekening te houden met de bedreigingen voor de samenleving en de nationale veiligheid in de aanvragen tot internationale bescherming (1197/1) 3. Wetsontwerp tot versterking van de strijd tegen het terrorisme (1198/1) 4. Wetsontwerp tot wijziging van de wet van 16 januari 2013 houdende diverse maatregelen betreffende de strijd tegen maritieme priaterij (1199/1), *Hand.* Kamer 2014-15, 1 juli 2015, CRIV54PLEN059, 3

Wetsontwerp tot wijziging van het Consulair Wetboek (1200/1-3) – Wetsontwerp houdende wijziging van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen (1170/1-6) – Wetsvoorstel tot intrekking van een identiteitskaart, paspoort en reisdocumenten van minderjarigen die in het buitenland willen gaan strijden (768/1) – Wetsvoorstel betreffende de intrekking van de identiteits- en reisdocumenten van wie naar het buitenland wil vertrekken om er te gaan strijden en er terroristische daden te plegen (797/1) – Wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen om beter rekening te houden met de bedreigingen voor de samenleving en de nationale veiligheid in de aanvragen tot internationale bescherming (1197/1-4) – Wetsontwerp tot versterking van de strijd tegen het terrorisme (1198/1-4) – Wetsvoorstel ertoe strekkende jihadisten de Belgische nationaliteit en alle sociale voordelen te ontnemen (658/1) – Wetsvoorstel betreffende de bestraffing en de vervallenverklaring van de Belgische nationaliteit van Belgen die zich vrijwillig aansluiten bij of taken vervullen voor bepaalde jihadistische groeperingen, verenigingen of entiteiten (781/1) – Wetsvoorstel tot wijziging van de wet van 1 augustus 1979 betreffende diensten bij een vreemde leger- of troepenmacht die zich op het grondgebied van een vreemde Staat bevindt, teneinde het vertrek van strijders naar Syrië of Irak te verbieden (795/1) – Wetsvoorstel tot wijziging van het Wetboek van de Belgische nationaliteit, teneinde de mogelijkheden tot vervallenverklaring van de nationaliteit uit te breiden (796/1) – Wetsvoorstel tot wijziging van de wet van 1 augustus 1979 betreffende diensten bij een vreemde leger- of troepenmacht die zich op het grondgebied van een vreemde Staat bevindt 11078/1), Algemene bespreking, *Hand.* Kamer 2014-15, 15 juli 2015, CRIV54PLEN063, 14

Wetsontwerp houdende wijziging van de wet van 19 juli 1991 betreffende de bevolkingsregisters, de identiteitskaarten, de vreemdelingenkaarten en de verblijfsdocumenten en tot wijziging van de wet van 8 augustus 1983 tot regeling van een Rijksregister van de natuurlijke personen, *Parl. St.* Kamer 2014-15, nr. 54K1170/007

Wetsontwerp tot wijziging van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen om beter rekening te houden met de bedreigingen voor de samenleving en de nationale veiligheid in de aanvragen tot internationale bescherming, *Parl. St.* Kamer 2014-15, nr. 54K1197/005

Wetsontwerp tot versterking van de strijd tegen het terrorisme (1198/4), *Hand.* Kamer 2014-15, 16 juli 2015, CRIV54PLEN065, 34

Wetsontwerp tot wijziging van het Consulair Wetboek, *Parl. St.* Kamer 2014-15, nr. 54K1200/002

Gedachtewisseling met de minister van Financiën over het Beleidsplan van de Algemene Administratie Douane en Accijnzen, *Parl. St.* Kamer 2014-15, nr. 54K1212/001

Voorstel van resolutie betreffende de toekomst van de Belgische Defensie, *Parl. St.* Kamer 2014-15, nr. 54K1261/001

Wetsontwerp houdende diverse bepalingen Binnenlandse Zaken, *Parl. St.* Kamer 2014-15, nr. 54K1298/001

Wetsontwerp houdende instemming met de Overeenkomst tussen het Koninkrijk België en het Groothertogdom Luxemburg inzake de uitwisseling en wederzijdse bescherming van geclassificeerde informatie, gedaan te Luxemburg op 9 februari 2012, *Parl. St.* Kamer 2014-15, nrs. 54K1299/001 en 54K1299/002

Hoorzitting met de heer Wim De Clercq, Chief Nuclear Officer van Electrabel, betreffende de analyse van de recente incidenten in de centrale van Tihange en het plan van aanpak voor de verbetering van de veiligheidscultuur in de centrales, *Hand.* Kamer 2014-15, 21 september 2015, CRIV54COM231, 1

Wetsontwerp tot wijziging van diverse wetten wat de benaming "Nationale Veiligheidsraad" betreft, *Parl. St.* Kamer 2014-15, nrs. 54K1330/001 tot 54K1330/004

Activiteitenverslag 2014 van het Vast comité van toezicht op de inlichtingen- en veiligheidsdiensten, *Parl. St.* Kamer 2014-15, nr. 54K1340/001

Ontwerp van algemene uitgavenbegroting voor het begrotingsjaar 2016, *Parl. St.* Kamer 2015-16, nr. 54K1352/001

Verantwoording van de algemene uitgavenbegroting voor het begrotingsjaar 2016, *Parl. St.* Kamer 2015-16, nrs. 54K1353/002, 54K1353/007 en 54K1353/008

Wetsontwerp houdende wijzigingen van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie, *Parl. St.* Kamer 2015-16, nrs. 54K1418/001, 54K1418/002 en 54K1418/004

Algemene beleidsnota – deel Fiscale fraude van de minister van Financiën, *Parl. St.* Kamer 2015-16, nrs. 54K1428/002, 54K1428/004, 54K1428/013, 54K1428/019 en 54K1428/022

Mededeling van de regering over de terroristische aanslagen, *Hand.* Kamer 2015-16, 19 november 2015, CRIV54PLEN081, 2

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 wat betreft het mandaat van de plaatsvervangende leden van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de inlichtingendiensten, *Parl. St.* Kamer 2015-16, nrs. 54K1446/001 tot 54K1446/004

Rekenhof, Grondwettelijk Hof, Hoge Raad voor de Justitie, Vaste Comités van toezicht op de politie- en inlichtingendiensten, Federale Ombudsmannen, Commissie voor de bescherming van de persoonlijke levenssfeer, Benoemingscommissies voor het nota-

riaat, BIM-Commissie en Controleorgaan politionele informatie – rekeningen van het begrotingsjaar 2014 – begrotingsaanpassingen 2015 – begrotingsvoorstellen voor het begrotingsjaar 2016, *Parl. St.* Kamer 2015-16, nrs. 54K1497/001 en 54K1497/002

Ontwerp van Algemene Uitgavenbegroting voor het begrotingsjaar 2016 – Advies over sectie 16 – ministerie van Landsverdediging, *Parl. St.* Kamer 2015-16, nr. 54K1352/027

Ontwerp van Algemene Uitgavenbegroting voor het begrotingsjaar 2016 – Advies over sectie 12 – FOD Justitie, *Parl. St.* Kamer 2015-16, nr. 54K1352/037

Rekeningen van het begrotingsjaar 2014 het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten (1497/1), *Hand.* Kamer 2015-16, 17 december 2015, CRIV54PLEN090, 78

Rekeningen van het begrotingsjaar 2014 van de BIM-Commissie (1497/1), *Hand.* Kamer 2015-16, 17 december 2015, CRIV54PLEN090, 80

Begrotingsvoorstellen voor het begrotingsjaar 2016 van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten (1497/1), *Hand.* Kamer 2015-16, 17 december 2015, CRIV54PLEN090, 84

Begrotingsvoorstellen voor het begrotingsjaar 2016 van de BIM-Commissie (1497/1), *Hand.* Kamer 2015-16, 17 december 2015, CRIV54PLEN090, 85

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 2015 TOT 31 DECEMBER 2015)

Senaat

Vraag van J.-J. De Gucht aan de minister van Binnenlandse Zaken over 'wahabisme – radicale scholen – Staatsveiligheid – handhaving – samenwerking met de Gemeenschappen' (Senaat 2014-15, 21 januari 2015, Vr. nr. 6-404)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over 'persoonsgegevens verwerkt door de inlichtingendiensten – archiefwet – bewaartermijn' (Senaat 2014-15, 13 februari 2015, Vr. nr. 6-441)

Schriftelijke vraag van Ch. Defraigne aan de minister van Binnenlandse Zaken over de 'politiediensten – plattelandsgebieden en grootstedelijke gebieden – OCAD – veiligheidsmaatregelen – begroting en operationele moeilijkheden' (Senaat 2014-15, 17 februari 2015, Vr. nr. 6-451)

Kamer van Volksvertegenwoordigers

Vraag van S. Smeyers aan de staatsecretaris voor Asiel en Migratie over 'de hervestiging van Syrische vluchtelingen' (*Hand.* Kamer 2014-15, 7 januari 2015, CRIV54COM045, 7, Vr. nr. 776)

Vraag van J. Fernandez Fernandez aan de minister van Defensie over 'de mogelijke politieopdrachten van het leger' (*Hand.* Kamer 2014-15, 7 januari 2015, CRIV54COM046, 4, Vr. nr. 673)

Vraag van F. Demon aan de minister van Binnenlandse Zaken over 'de werking van de lokale taskforce radicalisme' (*Hand*. Kamer 2014-15, 7 januari 2015, CRIV54COM050, 38, Vr. nr. 566)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over 'de herstart van Doel 4' (*Hand*. Kamer 2014-15, 7 januari 2015, CRIV54COM050, 49, Vr. nr. 629)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over 'de vlucht van een drone over de site van Doel' (*Hand*. Kamer 2014-15, 7 januari 2015, CRIV54COM050, 64, Vr. nr. 1045)

Samengevoegde vragen van P. Dewael, V. Matz, L. Onkelinx, K. Temmerman, S. Verherstraeten, H. Vuye, D. Ducarme, M. Almaci, R. Hedebouw, J.-M. Nollet, F. Dewinter, K. Metsu en O. Maingain aan de eerste minister over 'de terroristische aanslag op de redactie van Charlie Hebdo' (*Hand*. Kamer 2014-15, 8 januari 2015, CRIV54PLEN026, 4, Vr. nrs. 160 tot 172)

Samengevoegde vragen van G. Dallemagne en P. Buysrogge aan de eerste minister over 'de Belgische cybersecuritystrategie' (*Hand*. Kamer 2014-15, 13 januari 2015, CRIV-54COM051, 6, Vr. nrs. 984 en 1093)

Vraag van V. Yüksel aan de minister van Binnenlandse Zaken over 'het inzetten van het leger bij dreigingsniveau 3 (*Hand*. Kamer 2014-15, 13 januari 2015, CRIV54COM053, 46, Vr. nr. 1255)

Vraag van H. Bonte aan de minister van Binnenlandse Zaken over 'de dramatische aanslag op de redactie van Charlie Hebdo en de lessen voor het Belgische veiligheidsbeleid' (*Hand*. Kamer 2014-15, 13 januari 2015, CRIV54COM053, 48, Vr. nr. 1256)

Vraag van S.Smeyers aan de staatssecretaris voor Bestrijding van de sociale fraude, over 'terreurscreening bij bedrijven' (*Hand*. Kamer 2014-15, 14 januari 2015, CRIV-54COM055, 15, Vr. nr. 1340)

Vraag van R. Bellens aan de minister van Justitie over 'de uitwisseling van ISIS-strijders en Turkse gijzelaars door Turkije en de impact op de binnenlandse veiligheid' (*Hand*. Kamer 2014-15, 14 januari 2015, CRIV54COM055, 19, Vr. nr. 1075)

Samengevoegde vragen van H. Bonte, K. Metsu, V. Yüksel, F. Dewinter, S. Smeyers, L. Onkelinx en S. De Wit aan de minister van Justitie over 'het indijken van radicalisme in gevangenissen' (*Hand*. Kamer 2014-15, 14 januari 2015, CRIV54COM055, 35, Vr. nrs. 1278, 1282, 1311, 1333, 1339, 1348 en 1356)

Vraag van L. Onkelinx aan de minister van Justitie over 'de budgetten van de Veiligheid van de Staat en de strijd tegen fundamentalisme en terrorisme' (*Hand*. Kamer 2014-15, 14 januari 2015, CRIV54COM055, 48, Vr. nr. 1347)

Samengevoegde vragen van F. Dewinter, H. Bonte, V. Matz, M. Van Hees, B. Hellings en F. Demon aan de eerste minister over 'het beleid en de concrete maatregelen inzake terreur en radicalisme' (*Hand*. Kamer 2014-15, 15 januari 2015, CRIV54PLEN027, 22, Vr. nrs. 187 tot 192)

Vraag van S. Smeyers aan de staatsecretaris voor Asiel over de 'medische regularisatie' (*Vr. en Ant*. Kamer 2014-15, 19 januari 2015, QRVA 008, 223, Vr. nr. 21)

Samengevoegde vragen van K. Temmerman en S. Crusnière aan de minister van Begroting over 'het gebruik van de interdepartementale provisie voor de strijd tegen radicalisme en terrorisme' (*Hand*. Kamer 2014-15, 21 januari 2015, CRIV54COM060, 18, Vr. nrs. 1365 en 1403)

Gedachtewisseling en samengevoegde vragen van A. Top, G. Dallemagne, C. Van Cauter, S. De Wit, K. Degroote, J. Fernandez Fernandez, W. Demeyer, F. Demon, M. Wathelet, V. Matz, K. Metsu, P. Buysrogge, W. De Vriendt, S. Van Hecke, O. Maingain, L. Onkelinx, V. Yüksel en Ch. Brotcorne aan de minister van Binnenlandse Zaken over 'de strijd tegen terrorisme en radicalisme' (*Hand*. Kamer 2014-15, 21 januari 2015, CRIV54COM066, 1, Vr. nrs. 1321, 1364, 1379, 1382, 1447, 1449, 1451, 1452, 1456, 1460, 1461, 1467, 1474, 1475, 1484, 1508, 1513, 1514, 1522, 1523, 1528, 1529, 1530, 1537, 1541 en 1552)

Vraag van K. Lalieux aan de minister van Justitie over 'de veilgheid in het Justitiepaleis te Brussel' (*Hand*. Kamer 2014-15, 28 januari 2015, CRIV54COM070, 13, Vr. nr. 1747)

Vraag van S. Van Hecke aan de minister van Justitie over 'de openbaarheid van de archieven van de Veiligheid van de Staat' (*Hand*. Kamer 2014-15, 28 januari 2015, CRIV54COM070, 16, Vr. nr. 1594)

Vraag van S. Van Hecke aan de minister van Justitie over 'de 23 extra analisten voor de Veiligheid van de Staat en het invullen de bestaande kaders' (*Hand*. Kamer 2014-15, 28 januari 2015, CRIV54COM070, 22, Vr. nr. 1739)

Vraag van K. Temmerman aan de minister van Binnenlandse Zaken over 'het toekennen van verblijfspapieren aan imams door de Staatveiligheid' (*Hand*. Kamer 2014-15, 28 januari 2015, CRIV54COM073, 19, Vr. nr. 1535)

Samengevoegde vragen van H. Bonte en K. Degroote aan de eerste minister over 'de nood aan coördinatie en samenwerking inzake de aanpak van terrorisme en radicalisme' (*Hand*. Kamer 2014-15, 29 januari 2015, CRIV54PLEN029, 11, Vr. nrs. 226 en 227)

Vraag van S. Van Hecke aan de eerste minister over 'de politieke gevolgen van de hacking van Belgacom' (*Hand*. Kamer 2014-15, 3 februari 2015, CRIV54COM077, 1, Vr. nr. 865)

Vraag van K. Temmerman aan de minister van Justitie over 'het toekennen van verblijfspapieren aan imams door de Staatsveiligheid' (*Hand*. Kamer 2014-15, 4 februari 2015, CRIV54COM081, 3, Vr. nr. 1840)

Samengevoegde vragen van R. Deseyn en G. Dallemagne aan de eerste minister over 'de cyberveiligheid' (*Hand*. Kamer 2014-15, 5 februari 2015, CRIV54PLEN030, 7, Vr. nrs. 243 en 244)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de verminderde activiteiten van de lokale politie ten gevolge van haar inzet in het kader van de terreurbestrijding' (*Hand*. Kamer 2014-15, 5 februari 2015, CRIV54PLEN030, 23, Vr. nr. 251)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'steunbetuigingen aan Daesh op sociale netwerken in België' (*Vr. en Ant*. Kamer 2014-15, 9 februari 2015, QRVA 011, 47, Vr. nr. 136)

Vraag van M. Wathelet aan de minister van Energie over 'de fysieke bescherming van kerninstallaties en strategische infrastructuur' (*Hand*. Kamer 2014-15, 10 februari 2015, CRIV54COM084, 39, Vr. nr. 1600)

Samengevoegde vragen van J. Fernandez Fernandez en S. Pirlot aan de minister van Defensie over 'de begroting van de ADIV' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV54COM087, 31, Vr. nrs. 1232 en 1833)

Vraag van M. Wathelet aan de minister van Binnenlandse Zaken over 'de fysieke bescherming van kerninstallaties en strategische infrastructuur' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV54COM088, 1, Vr. nr. 1601)

Vraag van V. Matz aan de minister van Binnenlandse Zaken over 'de maatregelen van de federale overheid ter ondersteuning van de lokale overheden in de strijd tegen het radicalisme' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV54COM088, 13, Vr. nr. 1789)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'de beschermingsmaatregelen voor de Koerdische televisiezender ROJ TV' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV54COM088, 18, Vr. nr. 1801)

Vraag van F. Demon aan de minister van Binnenlandse Zaken over 'de OCAD-risicoanalyse van evenementen' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV54COM088, 39, Vr. nr. 1974)

Vraag van P.-O. Delannois aan de minister van Binnenlandse Zaken over 'de reacties op het afgelasten van het filmfestival Ramdam' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV54COM088, 41, Vr. nr. 2008)

Vraag van E. Kir aan de minister van Binnenlandse Zaken over 'het toezicht op imams uit het buitenland' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV54COM088, 59, Vr. nr. 2108)

Samengevoegde vragen van W. Demeyer en N. Ben Hamou aan de minister van Binnenlandse Zaken over 'de wijkspolitie en het dreigingsniveau 3' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV54COM088, 61, Vr. nrs. 2120 en 2187)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over 'de impact van het dreigingsniveau 3 op de politiezones' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV-54COM088, 68, Vr. nr. 2201)

Vraag van N. Lanjri aan de staatsecretaris voor Bestrijding van de sociale fraude over 'de mogelijke sociale fraude door Syriëstrijders' (*Hand*. Kamer 2014-15, 11 februari 2015, CRIV54COM091, 14, Vr. nr. 84)

Vraag van H. Bonte aan de minister van Binnenlandse Zaken over 'de rondzendbrief van 25 september 2014 inzake het informatiebeheer en de maatregelen voor de opvolging van de foreign fighters die in België verblijven' (*Vr. en Ant*. Kamer 2014-15, 16 februari 2015, QRVA 012, 139, Vr. nr. 127)

Vraag van P. Buysrogge aan de eerste minister over 'de samenwerking met Google en andere internetbedrijven om radicalisering tegen te gaan' (*Hand*. Kamer 2014-15, 24 februari 2015, CRIV54COM095, 8, Vr. nr. 1645)

Vraag van A. Top aan de minister van Defensie over 'het BINII-systeem' (*Hand*. Kamer 2014-15, 25 februari 2015, CRIV54COM096, 3, Vr. nr. 1493)

Vraag van S. Pirlot aan de minister van Defensie over 'de Belgian Intelligence Academy' (*Hand*. Kamer 2014-15, 25 februari 2015, CRIV54COM096, 27, Vr. nr. 1782)

Vraag van E. Willaert aan de staatssecretaris voor Bestrijding van de sociale fraude over 'het beroepsgeheim van sociaal-assistenten' (*Hand*. Kamer 2014-15, 25 februari 2015, CRIV54COM097, 14, Vr. nr. 2240)

Vraag van L. Onkelinx aan de minister van Justitie over 'het toezicht op buitenlandse imams' (*Hand*. Kamer 2014-15, 25 februari 2015, CRIV54COM097, 16, Vr. nr. 2099)

Vraag van S. Lahaye-Battheu aan de minister van Justitie over 'de toekomst van de rechtbank te Veurne' (*Hand.* Kamer 2014-15, 25 februari 2015, CRIV54COM097, 25, Vr. nr. 2342)

Vraag van S. Van Hecke aan de minister van Justitie over 'de samenwerking tussen de NSA en de Belgische inlichtingendienst' (*Hand.* Kamer 2014-15, 25 februari 2015, CRIV54COM097, 43, Vr. nr. 2256)

Samengevoede vragen van P. Vanvelthoven en W. Demeyer aan de minister van Binnenlandse Zaken over 'de beveiliging van bepaalde politici en hun gezinsleden' (*Hand.* Kamer 2014-15, 25 februari 2015, CRIV54COM100, 49, Vr. nrs. 2295 en 2487)

Samengevoegde vragen van P. Dewael en W. Demeyer aan de minister van Binnenlandse Zaken over 'de gevolgen van het aanhouden van dreigingsniveau 3' (*Hand.* Kamer 2014-15, 26 februari 2015, CRIV54PLEN032, 18, Vr. nrs. 297 en 298)

Vraag van N. Lijnen aan de minister van Defensie over de 'administraties en diensten – cyberaanvallen' (*Vr. en Ant.* Kamer 2014-15, 2 maart 2015, QRVA 014, 252, Vr. nr. 123)

Vraag van K. Grosemans aan de minister van Defensie over de 'attritie bij kandidaat-militairen' (*Vr. en Ant.* Kamer 2014-15, 2 maart 2015, QRVA 014, 258, Vr. nr. 124)

Vraag van S. Van Hecke aan de minister van Defensie over de 'inzet van BIM-methoden in het buitenland' (*Vr. en Ant.* Kamer 2014-15, 2 maart 2015, QRVA 014, 262, Vr. nr. 127)

Vraag van Ö. Özen aan de minister van Justitie over 'de lijst van potentiële jihadstrijders' (*Hand.* Kamer 2014-15, 3 maart 2015, CRIV54COM103, 21, Vr. nr. 2602)

Vraag van Ph. Goffin aan de minister van Justitie over 'de mogelijkheden inzake samenwerking tussen de Veiligheid van de Staat en het Terrorist Screening Center' (*Hand.* Kamer 2014-15, 3 maart 2015, CRIV54COM103, 35, Vr. nr. 2520)

Vraag van S. Van Hecke aan de minister van Justitie over 'de hacking van gegevens bij een producent van chips voor bank- en simkaarten' (*Hand.* Kamer 2014-15, 3 maart 2015, CRIV54COM103, 34, Vr. nr. 2612)

Vraag van R. Hufkens aan Binnenlandse Zaken over 'de terugkeer van Syriëstrijders' (*Vr. en Ant.* Kamer 2014-15, 9 maart 2015, QRVA 015, 68, Vr. nr. 68)

Vraag van K. Gabriëls aan de minister van Defensie over de 'ADIV – burgerpersoneel en analisten – aantastingen van de "fysieke integriteit"' (*Vr. en Ant.* Kamer 2014-15, 9 maart 2015, QRVA 015, 206, Vr. nr. 131)

Vraag van R. Hedebouw aan de minister van Defensie over de 'inzet van het leger' (*Vr. en Ant.* Kamer 2014-15, 9 maart 2015, QRVA 015, 210, Vr. nr. 134)

Vraag van J. Fernandez Fernandez aan de minister van Defensie over de 'evaluatie van de aanwezigheid van militairen op straat' (*Vr. en Ant.* Kamer 2014-15, 9 maart 2015, QRVA 015, 218, Vr. nr. 138)

Vraag van D. Ducarme aan de staatssecretaris voor Asiel en Migratie over de 'controle op radicale imams' (*Vr. en Ant.* Kamer 2014-15, 9 maart 2015, QRVA 015, 236, Vr. nr. 63)

Samengevoegde vragen van V. Yüksel, S. Pirlot en G. Dallemagne aan de minister van Defensie over 'jihadisten binnen het leger' (*Hand.* Kamer 2014-15, 10 maart 2015, CRIV54COM108, 35, Vr. nrs. 2383, 2467 en 2856)

Vraag van V. Yüksel aan de minister van Defensie over de 'diefstal van materiaal van Defensie in Landen' (*Vr. en Ant.* Kamer 2014-15, 16 maart 2015, QRVA 016, 251, Vr. nr. 149)

Vraag van M. De Coninck aan de staatssecretaris voor Asiel en Migratie over 'de procedure voor de verblijfsvergunning voor imams' (*Vr. en Ant.* Kamer 2014-15, 16 maart 2015, QRVA 016, 255, Vr. nr. 68)

Vraag van E. Kir aan de staatssecretaris voor Asiel en Migratie over 'het bezoek van de Belgische delegatie aan een kamp voor Syrische vluchtelingen' (*Hand.* Kamer 2014-15, 18 maart 2015, CRIV54COM118, 34, Vr. nr. 2825)

Samengevoegde vragen van A. Top, P. Buysrogge en J. Fernandez Fernandez aan de minister van Defensie over 'cyberdefence' (*Hand.* Kamer 2014-15, 18 maart 2015, CRIV-54COM119, 10, Vr. nrs. 2722, 2731 en 2867)

Samengevoegde vragen van S. Pirlot, A. Top en V. Yüksel aan de minister van Defensie over 'de verlaging van het dreigingsniveau op maandag 9 maart 2015' (*Hand.* Kamer 2014-15, 18 maart 2015, CRIV54COM119, 17, Vr. nrs. 2945, 3083 en 3090)

Vraag van N. Ben Hamou aan de minister van Binnenlandse Zaken over 'de organisatie van de politieopdrachten bij een verhoogd dreigingsniveau' (*Hand.* Kamer 2014-15, 18 maart 2015, CRIV54COM124, 3, Vr. nr. 2647)

Vraag van K. Temmerman aan de minister van Binnenlandse Zaken over 'de transparentie met betrekking tot ons veiligheidsbeleid' (*Hand.* Kamer 2014-15, 18 maart 2015, CRIV54COM124, 38, Vr. nr. 2764)

Samengevoegde vragen van E. Thiébaut en F. Demon aan de minister van Binnenlandse Zaken over 'de verlaging van het dreigingsniveau' (*Hand.* Kamer 2014-15, 18 maart 2015, CRIV54COM124, 46, Vr. nrs. 2895 en 2982)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over 'de overvliegen van de Belgische kerncentrales – overleg tussen het FANC en het OCAD' (*Vr. en Ant.* Kamer 2014-15, 23 maart 2015, QRVA 017, 113, Vr. nr. 93)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over 'de uitbreiding van de militaire taken' (*Vr. en Ant.* Kamer 2014-15, 23 maart 2015, QRVA 017, 117, Vr. nr. 131)

Vraag van S. De Wit aan de minister van Justitie over 'het voornemen om aparte afdelingen op te richten in de gevangenissen voor geradicaliseerde gevangenen' (*Hand.* Kamer 2014-15, 25 maart 2015, CRIV54COM127, 20, Vr. nr. 3100)

Vraag van E. Thiébaut aan de eerste minister over 'het Centrum voor Cybersecurity België' (*Hand.* Kamer 2014-15, 25 maart 2015, CRIV54COM130, 1, Vr. nr. 2481)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'de hacking van websites door IS' (*Hand.* Kamer 2014-15, 1 april 2015, CRIV54COM141, 1, Vr. nr. 2868)

Vraag van V. Yüksel aan de minister van Binnenlandse Zaken over 'een schema voor het drreigingsniveau en te nemen maatregelen' (*Hand.* Kamer 2014-15, 1 april 2015, CRIV54COM141, 24, Vr. nr. 3052)

Vraag van V. Matz aan de minister van Binnenlandse Zaken over 'bestrijding van de economische en financiële criminaliteit' (*Hand.* Kamer 2014-15, 1 april 2015, CRIV-54COM141, 43, Vr. nr. 3199)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'mogelijke feiten van radicalisering in Belgische overheidsbedrijven' (*Hand.* Kamer 2014-15, 1 april 2015, CRIV54COM141, 74, Vr. nr. 3447)

Vraag van W. De Vriendt aan de minister van Buitenlandse Zaken over 'de verhuis van het Afrika-archief van de FOD Buitenlandse Zaken naar het Rijksarchief' (*Vr. en Ant.* Kamer 2014-15, 7 april 2015, QRVA 019, 153, Vr. nr. 120)

Vraag van Ph. Goffin aan de minister van Binnenlandse Zaken over 'de raming van het aantal Belgische jihadi's in Syrië en Irak' (*Vr. en Ant.* Kamer 2014-15, 13 april 2015, QRVA 020, 29, Vr. nr. 196)

Vraag van R. Hedebouw aan de minister van Binnenlandse Zaken over 'de parlementaire controle op antiterreurbeleid en inlichtingendiensten' (*Vr. en Ant.* Kamer 2014-15, 13 april 2015, QRVA 020, 31, Vr. nr. 200)

Vraag van M. Van Hees aan de minister van Binnenlandse Zaken over 'de deelname aan buitenlandse conflicten' (*Vr. en Ant.* Kamer 2014-15, 13 april 2015, QRVA 020, 38, Vr. nr. 207)

Vraag van F. Demon aan de minister van Binnenlandse Zaken over de 'carnavalstoeten – veiligheidsaspect' (*Vr. en Ant.* Kamer 2014-15, 13 april 2015, QRVA 020, 41, Vr. nr. 212)

Vraag van P. Luykx aan de minister van Buitenlandse Zaken over 'de aanpak van de terreurdreiging in samenwerking met moslimlanden' (*Vr. en Ant.* Kamer 2014-15, 20 april 2015, QRVA 021, 134, Vr. nr. 55)

Samengevoegde vragen van P. Buysrogge en C. Cassart-Mailleux aan de minister van Defensie over 'het gebruik van computersimulaties en virtuele realiteit bij Defensie' (*Hand.* Kamer 2014-15, 22 april 2015, CRIV54COM143, 23, Vr. nrs. 3443 en 3791)

Samengevoegde vragen van S. Pirlot en G. Dallemagne aan de minister van Defensie over 'de bevoegdheden van de ADIV op het stuk van bescherming van het wetenschappelijke en economische potentieel' (*Hand.* Kamer 2014-15, 22 april 2015, CRIV-54COM143, 48, Vr. nrs. 3792 en 3819)

Vraag van K. Temmerman aan de minister van Binnenlandse Zaken over 'het hernieuwen van badges voor werknemers op de luchthaven van Zaventem' (*Hand.* Kamer 2014-15, 22 april 2015, CRIV54COM145, 15, Vr. nr. 3440)

Vraag van V. Matz aan de minister van Binnenlandse Zaken over 'het in praktijk brengen door de regering van haar twaalf maatregelen tegen radicalisme' (*Hand.* Kamer 2014-15, 22 april 2015, CRIV54COM146, 13, Vr. nr. 3504)

Vraag van G. Foret aan de minister van Binnenlandse Zaken over 'het gebruik van technieken van 'predictive profiling' door de ordediensten bij veiligheidsopdrachten' (*Hand.* Kamer 2014-15, 22 april 2015, CRIV54COM146, 35, Vr. nr. 3621)

Vraag van F. Demon aan de minister van Binnenlandse Zaken over 'de Veiligheid van de Staat en de federale politie' (*Hand.* Kamer 2014-15, 23 april 2015, CRIV54PLEN042, 23, Vr. nr. 435)

Samengevoegde vragen van P. Buysrogge en Ch. Brotcorne aan de minister van Justitie over 'de werking van de Veiligheid van de Staat' (*Hand.* Kamer 2014-15, 23 april 2015, CRIV54PLEN042, 26, Vr. nrs. 433 en 434)

Vraag van W. De Vriendt aan de staatssecretaris voor Armoedebestrijding over 'de verhuis van het Afrika-archief van de FOD Buitenlandse Zaken naar het Rijksarchief' (*Vr. en Ant.* Kamer 2014-15, 27 april 2015, QRVA 022, 165, Vr. nr. 57)

Vraag van K. Temmerman aan de minister van Binnenlandse Zaken over 'de implementatie van de twaalf maatregelen in de strijd tegen radicalisme en terrorisme' (*Vr. en Ant.* Kamer 2014-15, 4 mei 2015, QRVA 023, 13, Vr. nr. 257)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'kosten die door Binnenlandse Zaken werden gemaakt ten behoeve van het koningshuis' (*Vr. en Ant.* Kamer 2014-15, 4 mei 2015, QRVA 023, 83, Vr. nr. 110)

Vraag van F. Demon aan de minister van Binnenlandse Zaken, over 'de voorjaarskoersen – lokale politiekorpsen – ondersteuning door federale politie' (*Vr. en Ant.* Kamer 2014-15, 4 mei 2015, QRVA 023, 127, Vr. nr. 256)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken, over 'het inlichtingenbeleid – Nationale Veiligheidsraad' (*Vr. en Ant.* Kamer 2014-15, 4 mei 2015, QRVA 023, 136, Vr. nr. 276)

Vraag van P. Dedecker aan de minister van Telecommunicatie over 'de herziening van de dataretentiewet' (*Hand.* Kamer 2014-15, 5 mei 2015, CRIV54COM155, 1, Vr. nr. 3102)

Vraag van D. Geerts aan de minister van Telecommunicatie over 'de verdubbeling van het aantal cyberincidenten in België' (*Hand.* Kamer 2014-15, 5 mei 2015, CRIV54COM155, 12, Vr. nr. 3013)

Samengevoegde vragen van O. Maingain en W. Demeyer aan de minister van Binnenlandse Zaken over 'de Nationale Veiligheidsraad' (*Hand.* Kamer 2014-15, 5 mei 2015, CRIV54COM159, 6, Vr. nrs. 3907 en 4126)

Vraag van V. Matz aan de minister van Binnenlandse Zaken over 'de terreurdreiging tegen christelijke kerken in België' (*Hand.* Kamer 2014-15, 6 mei 2015, CRIV-54COM165, 12, Vr. nr. 4119)

Vraag van O. Maingain aan de minister van Binnenlandse Zaken over 'het bestrijden van cyberaanvallen' (*Hand.* Kamer 2014-15, 6 mei 2015, CRIV54COM165, 13, Vr. nr. 3739)

Vraag van S. Van Hecke aan de minister van Binnenlandse Zaken, over 'de juridische basis om de krijgsmacht in te zetten bij dreigingsniveau 3' (*Vr. en Ant.* Kamer 2014-15, 11 mei 2015, QRVA 024, 95, Vr. nr. 242)

Vraag van F. Demon aan de minister van Binnenlandse Zaken, over de 'permanentie van politieposten' (Vr. en Ant. Kamer 2014-15, 11 mei 2015, QRVA 024, 99, Vr. nr. 259)

Vraag van R. Hedebouw aan de eerste minister over 'het onderzoek naar de moord op Julien Lahaut' (*Hand.* Kamer 2014-15, 13 mei 2015, CRIV54PLEN046, 27, Vr. nr. 490)

Vraag van F. Schepmans aan de minister van Justitie over de 'informatie-uitwisseling in het kader van de strijd tegen terrorisme en radicalisme – nationaal niveau – werkgroep' (*Vr. en Ant.* Kamer 2014-15, 18 mei 2015, QRVA 025, 117, Vr. nr. 235)

Vraag van S. Van Hecke aan de minister van Justitie over 'de Russische spionagezaak' (*Vr. en Ant.* Kamer 2014-15, 18 mei 2015, QRVA 025, 120, Vr. nr. 297)

Vraag van R. Deseyn aan de minister van Energie over de 'inspectiedienst kritieke infrastructuur' (*Vr. en Ant.* Kamer 2014-15, 18 mei 2015, QRVA 025, 165, Vr. nr. 49)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over 'de vraag of onze kerncentrales bestand zijn tegen de impact van een neerstortende jumbojet' (*Hand.* Kamer 2014-15, 20 mei 2015, CRIV54COM176, 31, Vr. nr. 4328)

Vraag van A. Carcaci aan de minister van Binnenlandse Zaken over 'de grenscontrole' (*Hand.* Kamer 2014-15, 21 mei 2015, CRIV54PLEN047, 13, Vr. nr. 514)

Vraag van H. Bonte aan de minister van Binnenlandse Zaken over 'de pijnlijke administratieve praktijken in de strijd tegen radicalisme' (*Hand.* Kamer 2014-15, 21 mei 2015, CRIV54PLEN047, 18, Vr. nr. 516)

Samengevoegde vragen van B. Hellings, J.J. Flahaux en V. Matz aan de minister van Defensie over 'de structurele banden tussen de ADIV en de NSA in het licht van de door het hoofd van de militaire inlichtingendienst verspreide foute informatie over drie verijdelde aanslagen' (*Hand.* Kamer 2014-15, 27 mei 2015, CRIV54COM182, 35, Vr. nrs. 4195, 4259 en 4595)

Samengevoegde vragen van W. De Vriendt, V. Yüksel, S. Crusnière en K. Grosemans aan de minister van Defensie over 'Burundi' (*Hand.* Kamer 2014-15, 27 mei 2015, CRIV-54COM182, 46, Vr. nrs. 4387, 4392, 4511 en 4591)

Vraag van A. Top aan de minister van Defensie over 'de situatie over de inlichtingendiensten' (*Hand.* Kamer 2014-15, 27 mei 2015, CRIV54COM182, 61, Vr. nr. 4526)

Vraag van K. Jadin aan de eerste minister over de 'inlichtingenbeleid – Nationale Veiligheidsraad' (*Vr. en Ant.* Kamer 2014-15, 2 juni 2015, QRVA 027, 41, Vr. nr. 30)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over de 'stagiair met IS-sympathieën bij de Federale Politie' (*Vr. en Ant.* Kamer 2014-15, 2 juni 2015, QRVA 027, 123, Vr. nr. 359)

Vraag van V. Scourneau aan de minister van Defensie over de 'verbintenis in het kader van het cyberbeveiligingsprogramma' (*Vr. en Ant.* Kamer 2014-15, 2 juni 2015, QRVA 027, 243, Vr. nr. 221)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over 'de groep NATION en de strijd tegen extremisten' (*Hand.* Kamer 2014-15, 4 juni 2015, CRIV54PLEN050, 22, Vr. nr. 559)

Samengevoegde vragen van P. Buysrogge, A. Frédéric en B. Hellings aan de eerste minister over 'de nieuwe Belgacomhacking door de Duitse inlichtingendiensten' (*Hand.* Kamer 2014-15, 9 juni 2015, CRIV54COM186, 7, Vr. nrs. 4802, 4910 en 4915)

Vraag van K. Grosemans aan de minister van Buitenlandse Zaken over 'de afgifte van veiligheidscertificaten door de Nationale Veiligheidsoverheid' (*Vr. en Ant.* Kamer 2014-15, 9 juni 2015, QRVA 028, 126, Vr. nr. 171)

Vraag van S. Van Hecke aan de minister van Defensie over 'de juridische basis om de krijgsmacht in te zetten bij dreigingsniveau 3' (*Vr. en Ant.* Kamer 2014-15, 9 juni 2015, QRVA 028, 257, Vr. nr. 235)

Vraag van V. Yüksel aan aan de minister van Defensie over de 'ontslagen om medische redenen bij het Belgische leger' (*Vr. en Ant.* Kamer 2014-15, 9 juni 2015, QRVA 028, 264, Vr. nr. 236)

Vraag van A. Top aan de minister van Defensie over 'de extra veiligheidsmaatregelen na het uitlekken van foto's bij een autopsie' (*Hand.* Kamer 2014-15, 10 juni 2015, CRIV-54COM189, 7, Vr. nr. 4813)

Vraag van N. Ben Hamou aan de minister van Binnenlandse Zaken over 'de daling van de criminaliteit door de aanwezigheid van militairen op straat' (*Hand.* Kamer 2014-15, 10 juni 2015, CRIV54COM192, 3, Vr. nr. 4436)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over 'de vraag of onze kerncentrales bestand zijn tegen de inslag van een jumbojet' (*Hand.* Kamer 2014-15, 10 juni 2015, CRIV54COM192, 23, Vr. nr. 4777)

Vraag van A. Top aan de eerste minister over de 'aankoop van beveiligde gsm's' (*Vr. en Ant.* Kamer 2014-15, 15 juni 2015, QRVA 029, 73, Vr. nr. 32)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over de 'Imam Van Ael – Stopzetting publieke werkzaamheden' (*Vr. en Ant.* Kamer 2014-15, 15 juni 2015, QRVA 029, 99, Vr. nr. 407)

Vraag van S. Van Hecke aan de minister van Buitenlandse Zaken over de 'toename van Russische spionnen' (*Vr. en Ant.* Kamer 2014-15, 15 juni 2015, QRVA 029, 102, Vr. nr. 167)

Vraag van R. Deseyn aan de minister van Mobiliteit over de 'inspectiedienst kritieke infrastructuur' (*Vr. en Ant.* Kamer 2014-15, 15 juni 2015, QRVA 029, 283, Vr. nr. 344)

Samengevoegde vragen van S. Van Hecke en G. Dallemagne aan de minister van Justitie over 'de spionageactiviteiten van de Duitse inlichtingendiensten op het telefoon- en dataverkeer van en naar België op vraag van de NSA' (*Hand.* Kamer 2014-15, 16 juni 2015, CRIV54COM193, 12, Vr. nrs. 4693 en 4988)

Samengevoegde vragen van S. Van Hecke aan de minister van Justitie over 'de organisatie van vergaarde informatie door de Veiligheid van de Staat' (*Hand.* Kamer 2014-15, 16 juni 2015, CRIV54COM193, 23, Vr. nrs. 4806 tot 4810)

Vraag van P. Buysrogge aan de minister van Justitie over 'de infrastructuur bij de VSSE' (*Vr. en Ant.* Kamer 2014-15, 22 juni 2015, QRVA 030, 106, Vr. nr. 346)

Vraag van K. Gabriëls aan de minister van Justitie over 'de transparantie bij de Staatsveiligheid' (*Vr. en Ant.* Kamer 2014-15, 22 juni 2015, QRVA 030, 108, Vr. nr. 368)

Vraag van K. Jadin aan de minister van Defensie over 'de omvangrijke Defensiestaf' (*Vr. en Ant.* Kamer 2014-15, 22 juni 2015, QRVA 030, 146, Vr. nr. 250)

Vraag van J.-M. Nollet aan de minister van Defensie over 'de opdrachten van de heer André Moyen' (*Vr. en Ant.* Kamer 2014-15, 22 juni 2015, QRVA 030, 156, Vr. nr. 257)

Vraag van K. Temmerman aan de minister van Binnenlandse Zaken over 'de implementatie van de twaalf maatregelen in de strijd tegen radicalisme en terrorisme' (*Vr. en Ant.* Kamer 2014-15, 29 juni 2015, QRVA 031, 212, Vr. nr. 257)

Vraag van V. Yüksel aan de minister van Binnenlandse Zaken over de 'overuren bij de politie in het kader van de verhoogde terrorismedreiging' (*Vr. en Ant.* Kamer 2014-15, 29 juni 2015, QRVA 031, 213, Vr. nr. 284)

Vraag van W. Demeyer aan de minister van Binnenlandse Zaken over 'de antiterreuroperatie van maandag 8 juni op verscheidene plekken in België' (*Hand.* Kamer 2014-15, 1 juli 2015, CRIV54COM208, 1, Vr. nr. 4970)

Samengevoegde vragen van F. Demon en K. Metsu aan de minister van Binnenlandse Zaken over 'de gevolgen van het vernietigen van de dataretentiewet' (*Hand.* Kamer 2014-15, 1 juli 2015, CRIV54COM209, 30, Vr. nrs. 5100 en 5188)

Vraag van R. Hufkens aan de minister van Binnenlandse Zaken over 'de bewaking van ambassades en internationale instellingen door private beveiligingsondernemingen' (*Vr. en Ant.* Kamer 2014-15, 6 juli 2015, QRVA 032, 116, Vr. nr. 376)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'de verkiezingscampagne van president Erdogan in de Ethias Arena van Hasselt' (*Vr. en Ant.* Kamer 2014-15, 6 juli 2015, QRVA 032, 117, Vr. nr. 387)

Vraag van B. Pas aan de minister van Justitie over de 'Veiligheid van de Staat – actuele stand van zaken met betrekking tot de invulling van de taalkaders' (*Vr. en Ant.* Kamer 2014-15, 6 juli 2015, QRVA 032, 177, Vr. nr. 318)

Samengevoegde vragen van A. Top, G. Dallemagne et V. Yüksel aan minister van Defensie over 'de gelekte documenten bij Defensie' (*Hand.* Kamer 2014-15, 8 juli 2015, CRIV-54COM219, 10, Vr. nrs. 5162, 5373 en 5690)

Vraag van J. Fernandez Fernandez aan minister van Defensie over 'de aanwerving van 24 specialisten in cyberveiligheid' (*Hand.* Kamer 2014-15, 8 juli 2015, CRIV54COM219, 19, Vr. nr. 5400)

Vraag van B. Hellings aan minister van Binnenlandse Zaken over 'het onderbrengen van speciale spionage-eenheden in een aantal Amerikaanse ambassades over de hele wereld' (*Hand.* Kamer 2014-15, 8 juli 2015, CRIV54COM219, 20, Vr. nr. 5404)

Vraag van N. Lijnen aan minister van Buitenlandse Zaken over 'de operatie in Aleppo' (*Hand.* Kamer 2014-15, 9 juli 2015, CRIV54PLEN062, 38, Vr. nr. 690)

Vraag van R. Hedebouw aan de minister van Binnenlandse Zaken over de 'toepassing protocolakkoord 17 januari 2015 over de inzet van het leger' (*Vr. en Ant.* Kamer 2014-15, 13 juli 2015, QRVA 033, 109, Vr. nr. 199)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'afgelasting van een congres op 3 juni wegens terreurdreiging' (*Vr. en Ant.* Kamer 2014-15, 13 juli 2015, QRVA 033, 139, Vr. nr. 479)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'Islamistische organisatie te Antwerpen' (*Vr. en Ant.* Kamer 2014-15, 13 juli 2015, QRVA 033, 141, Vr. nr. 480)

Vraag van B. Hellings aan de minister van Binnenlandse Zaken over 'de uitwijzing an EU-staatsburgers' (*Hand.* Kamer 2014-15, 14 juli 2015, CRIV54COM225, 10, Vr. nr. 5569)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'de screening van imams' (*Hand.* Kamer 2014-15, 14 juli 2015, CRIV54COM225, 13, Vr. nr. 5595)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'de uitzetting van radicale imams' (*Hand.* Kamer 2014-15, 14 juli 2015, CRIV54COM225, 23, Vr. nr. 5728)

Vraag van V. Matz aan de minister van Binnenlandse Zaken over 'het verzoek van de vakbonden om het defilé van de politieagenten op 21 juli 2015 af te gelasten' (*Hand.* Kamer 2014-15, 16 juli 2015, CRIV54PLEN065, 8, Vr. nr. 700)

Vraag van F. Dewinter aan de minister van Justitie over de 'terugkerende Syriëstrijders en/of leden van ISIS' (*Vr. en Ant.* Kamer 2014-15, 22 juli 2015, QRVA 034, 198, Vr. nr. 162)

Vraag van K. Temmerman aan de eerste minister over de 'implementatie van de twaalf maatregelen in de strijd tegen radicalisme en terrorisme' (*Vr. en Ant.* Kamer 2014-15, 27 juli 2015, QRVA 035, 17, Vr. nr. 53)

Vraag van S. Van Hecke aan de minister van Justitie over de 'toenemende Russische spionage' (*Vr. en Ant.* Kamer 2014-15, 27 juli 2015, QRVA 035, 59, Vr. nr. 365)

Vraag van L. Van Biesen aan de minister van Justitie over het 'nieuwe personeelsevaluatiesysteem federale overheidsdiensten' (*Vr. en Ant.* Kamer 2014-15, 27 juli 2015, QRVA 035, 63, Vr. nr. 374)

Vraag van E. Kir aan de minister van Binnenlandse Zaken over het 'Europees actieplan tegen terrorisme' (*Vr. en Ant.* Kamer 2014-15, 3 augustus 2015, QRVA 036, 68, Vr. nr. 413)

Vraag van V. Yüksel aan de minister van Defensie over 'de opslag van digitale informatie' (*Vr. en Ant.* Kamer 2014-15, 3 augustus 2015, QRVA 036, 206, Vr. nr. 300)

Vraag van V. Yüksel aan de minister van Defensie over 'de piloten bij de Luchtcomponent' (*Vr. en Ant.* Kamer 2014-15, 3 augustus 2015, QRVA 036, 209, Vr. nr. 302)

Vraag van V. Yüksel aan de minister van Defensie over 'de Divisie Veiligheid van ADIV' (*Vr. en Ant.* Kamer 2014-15, 3 augustus 2015, QRVA 036, 214, Vr. nr. 303)

Vraag van V. Yüksel aan de minister van Defensie over 'militairen die voor andere ministeries werken' (*Vr. en Ant.* Kamer 2014-15, 10 augustus 2015, QRVA 037, 160, Vr. nr. 329)

Vraag van P. Buysrogge aan de minister van Defensie over 'de infrastructuur bij de VSSE' (*Vr. en Ant.* Kamer 2014-15, 17 augustus 2015, QRVA 038, 249, Vr. nr. 333)

Vraag van R. Deseyn aan de minister van Binnenlandse Zaken over de 'inspectiediensten kritieke infrastructuur' (*Vr. en Ant.* Kamer 2014-15, 31 augustus 2015, QRVA 040, 81, Vr. nr. 297)

Vraag van G. Gilkinet aan de minister van Binnenlandse Zaken over de 'evolutie van het aantal politieagenten' (*Vr. en Ant.* Kamer 2014-15, 31 augustus 2015, QRVA 040, 114, Vr. nr. 383)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over de 'aanslagen in Lyon, Sousse en Koeweit' (*Vr. en Ant.* Kamer 2014-15, 31 augustus 2015, QRVA 040, 289, Vr. nr. 566)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'controle door de Vaste Commissie voor Taaltoezicht van de naleving van de taalkaders door de Veiligheid van de Staat' (*Vr. en Ant.* Kamer 2014-15, 31 augustus 2015, QRVA 040, 301, Vr. nr. 575)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over de 'inlichtingendiensten – opvolging' (*Vr. en Ant.* Kamer 2014-15, 7 september 2015, QRVA 041, 99, Vr. nr. 619)

Vraag van R. Deseyn aan de minister van Binnenlandse Zaken over 'spionage door Russische diplomaten' (*Vr. en Ant.* Kamer 2014-15, 7 september 2015, QRVA 041, 124, Vr. nr. 269)

Vraag van B. Pas aan de minister van Justitie over 'de verkiezingscampagne van president Erdogan in de Ethias Arena van Hasselt' (*Vr. en Ant.* Kamer 2014-15, 16 september 2015, QRVA 042, 165, Vr. nr. 357)

Vraag van B. Pas aan de minister van Justitie over 'benoemingen door de federale regering' (*Vr. en Ant.* Kamer 2014-15, 16 september 2015, QRVA 042, 182, Vr. nr. 427)

Vraag van Ph. Blanchart aan de minister van Binnenlandse Zaken over 'praktijken van anarchisten in Brussel' (*Vr. en Ant.* Kamer 2014-15, 21 september 2015, QRVA 043, 20, Vr. nr. 405)

Vraag van Ph. Pivin aan de minister van Justitie over 'confessionele scholen, eredienstaangelegenheden en het toezicht erop' (*Hand.* Kamer 2014-15, 7 oktober 2015, CRIV-54COM240, 27, Vr. nr. 6143)

Vraag van A. Top aan de minister van Justitie over 'informatieveiligheid' (*Hand.* Kamer 2014-15, 7 oktober 2015, CRIV54COM240, 52, Vr. nr. 6614)

Vraag van E. Burton aan de minister van Binnenlandse Zaken over 'ANPR-camera's' (*Vr. en Ant.* Kamer 2015-16, 9 oktober 2015, QRVA 046, 40, Vr. nr. 491)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over het 'Europees politieteam op zoek naar IS op sociale media' (*Vr. en Ant.* Kamer 2015-16, 9 oktober 2015, QRVA 046, 55, Vr. nr. 567)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over de 'uitkeringen Syriëstrijders' (*Vr. en Ant.* Kamer 2015-16, 9 oktober 2015, QRVA 046, 61, Vr. nr. 594)

Vraag van K. Degroote aan de minister van Binnenlandse Zaken over de 'detachering buiten de geïntegreerde politie' (*Vr. en Ant.* Kamer 2015-16, 9 oktober 2015, QRVA 046, 72, Vr. nr. 615)

Vraag van K. Metsu aan de minister van Defensie over de 'radicalisering bij militairen' (*Vr. en Ant.* Kamer 2015-16, 9 oktober 2015, QRVA 046, 259, Vr. nr. 375)

Vraag van J. Penris aan de minister van Defensie over 'de mogelijke gevolgen van militaire overlopers in de strijd tegen het moslimextremisme' (*Vr. en Ant.* Kamer 2015-16, 9 oktober 2015, QRVA 046, 261, Vr. nr. 377)

Vraag van R. Deseyn aan de minister van Defensie over de 'spionage door Russische diplomaten' (*Vr. en Ant.* Kamer 2015-16, 19 oktober 2015, QRVA 047, 214, Vr. nr. 380)

Vraag van S. De Wit aan de minister van Justitie over 'de oplossing die de minister aankondigde naar aanleiding van de vernietigde dataretentiewet' (*Hand.* Kamer 2015-16, 21 oktober 2015, CRIV54COM250, 28, Vr. nr. 5823)

Vraag van S. Van Hecke aan de minister van Justitie over 'de rol van de Staatsveiligheid bij het staatsbezoek van president Erdogan' (*Hand.* Kamer 2015-16, 21 oktober 2015, CRIV54COM250, 47, Vr. nr. 6817)

Samengevoegde vragen van B. Hellings en A. Top aan de minister van Defensie over 'de velleïteit van het hoofd van de militaire inlichtingendienst om alle digitale communicatie die via glasvezelkabels door België loopt, af te tappen' (*Hand.* Kamer 2015-16, 28 oktober 2015, CRIV54COM256, 4, Vr. nrs. 5720 en 5863)

Vraag van S. Pirlot aan de minister van Defensie over 'de strategie van de ADIV inzake de strijd tegen het terrorisme' (*Hand.* Kamer 2015-16, 28 oktober 2015, CRIV54COM256, 21, Vr. nr. 5950)

Samengevoegde vragen van P. Dedecker, Ö. Özen, Ph. Goffin en D. Geerts aan de staatsecretaris voor Bestijding van de sociale fraude over 'het standpunt van de regering inzake de bescherming van Europese persoonsgegevens in de VS' (*Hand.* Kamer 2015-16, 28 oktober 2015, CRIV54COM257, 4, Vr. 6455, 6480, 6635 en 7116)

Vraag van O. Maingain aan de minister van Justitie over 'de strijd tegen het toenemende radicalisme in de gevangenissen' (*Hand.* Kamer 2015-16, 28 oktober 2015, CRIV-54COM259, 6, Vr. nr. 6777)

Vraag van W. Demeyer aan de minister van Binnenlandse Zaken over 'de omzendbrief betreffende de informatie-uitwisseling over en de opvolging van de 'foreign terrorist fighters' uit België' (*Hand.* Kamer 2015-16, 28 oktober 2015, CRIV54COM259, 19, Vr. nr. 7029)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over 'de inventarisering van wapens' (*Hand.* Kamer 2015-16, 28 oktober 2015, CRIV54COM261, 30, Vr. nr. 6003)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over 'de bescherming van de Belgische luchtvaart- en binnenvaartinfrastructuur tegen mogelijke terreuraanslagen' (*Hand.* Kamer 2015-16, 28 oktober 2015, CRIV54COM261, 41, Vr. nr. 6142)

Vraag van A. Top aan de minister van Binnenlandse Zaken over 'het bezoek van de minister aan Noord-Afrika' (*Hand.* Kamer 2015-16, 28 oktober 2015, CRIV54COM261, 57, Vr. nr. 6531)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'de moslimbeurs' (*Hand.* Kamer 2015-16, 29 oktober 2015, CRIV54PLEN079, 29, Vr. nr. 760)

Vraag van E. Kir aan de minister van Binnenlandse Zaken over 'de evaluatie van de terreurdreiging in België na de aanslagen in Frankrijk en in Tunesië op 26 juni 2015' (*Vr. en Ant.* Kamer 2015-16, 9 november 2015, QRVA 049, 93, Vr. nr. 722)

Vraag van F. Schepmans aan de minister van Justitie over 'de huiszoekingen in het Tsjetsjeense jihadistische milieu' (*Vr. en Ant.* Kamer 2015-16, 9 november 2015, QRVA 049, 132, Vr. nr. 410)

Vraag van B. Pas aan de minister van Justitie over 'de extra bezoldigingen of vergoedingen van vakbondsafgevaardigden in beheerscomités en andere raden/commissies' (*Vr. en Ant.* Kamer 2015-16, 9 november 2015, QRVA 049, 140, Vr. nr. 536)

Vraag van S. Lahaye-Battheu aan de minister van Financiën over de 'verkeersveroordelingen – verbeurdverklaringen van auto's (Vr. en Ant. Kamer 2015-16, 9 november 2015, QRVA 049, 198, Vr. nr. 223)

Vraag van F. Demon aan de minister van Defensie over 'het online plaatsen van grondplannen van overheidsgebouwen' (*Vr. en Ant.* Kamer 2015-16, 9 november 2015, QRVA 049, 358, Vr. nr.389)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de maatregelen van de regering om de infiltratie van mogelijke IS-militanten in het kielzog van de asielstroom tegen te gaan' (*Hand.* Kamer 2015-16, 12 november 2015, CRIV54PLEN080, 37, Vr. nr. 793)

Mededeling van de minister van Defensie gedachtewisseling en samengevoegde vragen van S. Pirlot, B. Hellings, G. Dallemagne, V. Yüksel, A. Top, W. De Vriendt en K. Grosemans over 'de nieuwe missie van de Leopold I' (*Hand.* Kamer 2015-16, 18 november 2015, CRIV54COM270, 1, Vr. nrs. 7356, 7361, 7462, 7478, 7480, 7481, 7493, 7463 en 7479)

Vraag van B. Vermeulen aan de eerste minister over 'de bescherming van de kritieke infrastructuur' (*Hand.* Kamer 2015-16, 24 november 2015, CRIV54COM274, 10, Vr. nr. 7616)

Samengevoegde vragen van A. Top, S. Pirlot en G. Dallemagne aan de minister van Defensie over 'de Belgische deelname aan MINUSMA in 2016' (*Hand.* Kamer 2015-16, 25 november 2015, CRIV54COM277, 25, Vr. nrs. 6417, 7571 en 7632)

Vraag van A. Top aan de minister van Defensie over 'de gelekte documenten met gevoelige informatie' (*Hand.* Kamer 2015-16, 25 november 2015, CRIV54COM277, 30, Vr. nr. 6420)

Samengevoegde vragen van S. Pirlot, A. Top, G. Dallemagne en K. Jadin aan de minister van Defensie over 'de kosten van de inzet van militairen op straat' (*Hand.* Kamer 2015-16, 25 november 2015, CRIV54COM277, 40, Vr. nrs. 6546, 6684, 6977, 7128, 7611 en 7631)

Samengevoegde vragen van W. De Vriendt, A. Top, G. Dallemagne en S. Pirlot aan de minister van Defensie over 'het strategisch plan Defensie' (*Hand.* Kamer 2015-16, 25 november 2015, CRIV54COM277, 58, Vr. nrs. 7252, 7313, 7464 en 7567)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'de aanwezigheid van terroristen in Belgische asielcentra' (*Hand.* Kamer 2015-16, 25 november 2015, CRIV54COM278, 1, Vr. nr. 7650)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'de taskforce over radicalisering' (*Hand.* Kamer 2015-16, 25 november 2015, CRIV54COM278, 4, Vr. nr. 7652)

Samengevoegde vragen van L. Onkelinx, R. Hedebouw, P. Dewael, F. Dewinter, M. Kitir, G. Dallemagne, O. Maingain, S. Verherstraeten, K. Metsu, D. Ducarme, en J.-M. Nollet aan de eerste minister over 'het terrorisme' (*Hand.* Kamer 2015-16, 26 november 2015, CRIV54PLEN083, 1, Vr. nrs. 816 tot 826)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'Belgische jihadstrijders' (*Vr. en Ant.* Kamer 2015-16, 29 november 2015, QRVA 048, 111, Vr. nr. 400)

Vraag van S. Pirlot aan de minister van Justitie over de 'samenwerking tussen de Veiligheid van de Staat en de ADIV inzake terreurbestrijding' (*Vr. en Ant.* Kamer 2015-16, 29 november 2015, QRVA 048, 252, Vr. nr. 599)

Vraag van K. Metsu aan de minister van Defensie over de 'inlichtingendiensten – opvolging' (*Vr. en Ant.* Kamer 2015-16, 29 november 2015, QRVA 048, 322, Vr. nr. 384)

Vraag van F. Schepmans aan de minister van Binnenlandse Zaken over 'huiszoekingen in het Tsjetsjeense jihadistische milieu' (*Vr. en Ant.* Kamer 2015-16, 30 november 2015, QRVA 052, 77, Vr. nr. 719)

Vraag van S. Van Hecke aan de minister van Binnenlandse Zaken over 'het Staatsbezoek president Erdogan – controle wapens veiligheidsteam' (*Vr. en Ant.* Kamer 2015-16, 30 november 2015, QRVA 052, 99, Vr. nr. 794)

Gedachtewisseling met de minister van Binnenlandse Zaken en de minister van Justitie over de strijd tegen het terrorisme en het radicalisme en samengevoegde vragen van O. Maingain, W. Demeyer, E. Thiébaut, K. Jadin, K. Metsu, E. Kir, N. Ben Hamou, G. Vanden Burre, V. Matz, F. Demon, S. Van Hecke, K. Van Vaerenbergh, Ph. Pivin, A. Top, Ph. Blanchart, J.-M. Nollet, G. Dallemagne, Ph. Goffin, H. Bonte, F. Schepmans, I. De Coninck, D. Ducarme en S. De Wit over 'de omzendbrief betreffende de opvolging van de 'foreign terrorist fighters'' (*Hand.* Kamer 2015-16, 2 december 2015, CRIV54COM285, 1, Vr. nrs. 6645, 7029, 7208, 7384, 7610, 7466, 7487, 7488, 7518, 7519, 7527, 7530, 7547, 7566, 7568, 7573, 7607, 7620, 7640, 7641, 7655, 7702, 7707, 7722, 7730, 7740, 7751, 7761, 7762, 7763, 7764, 7766, 7770, 7771, 7776, 7777, 7778, 7780, 7781, 7782, 7788, 7789, 7790, 7791, 7806 en 7807)

Samengevoegde vragen van K. Jadin en G. Dallemagne aan de minister van Defensie over 'de toenadering tussen de ADIV en de Veiligheid van de Staat' (*Hand.* Kamer 2015-16, 9 december 2015, CRIV54COM288, 1, Vr. nrs. 7385 en 7461)

Samengevoegde vragen van A. Top, R. Hufkens en V. Yüksel aan de minister van Defensie over 'de brandbom in de kazerne van Heverlee' (*Hand.* Kamer 2015-16, 9 december 2015, CRIV54COM288, 16, Vr. nrs. 7795, 7799 en 7888)

Vraag van V. Yüksel aan de minister van Defensie over 'het rapport van het Comité I over radicalisering binnen Defensie' (*Hand.* Kamer 2015-16, 9 december 2015, CRIV-54COM288, 20, Vr. nr. 7887)

Vraag van R. Hufkens aan de minister van Defensie over 'de blootstelling van gevoelige informatie via open sourcekanalen' (*Hand.* Kamer 2015-16, 9 december 2015, CRIV-54COM288, 26, Vr. nr. 7925)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de erfpachtregeling en de eventuele sluiting van de Saudische grote Moskee in het Jubelpark te Brussel' (*Hand.* Kamer 2015-16, 10 december 2015, CRIV54PLEN085, 8, Vr. nr. 867)

Vraag van Ph. Goffin aan de minister van Justitie over 'de contacten van de vermoedelijke terrorist Salah Abdeslam in de gevangenis van Namen' (*Hand.* Kamer 2015-16, 10 december 2015, CRIV54PLEN085, 12, Vr. nr. 870)

Samengevoegde vragen van Ö. Özlen, V. Matz, G. Vanden Burre, O. Maingain, D. Ducarme, H. Bonte en C. Van Cauter aan de minister van Justitie over 'het onderzoek naar Salah Abdelsam' (*Hand.* Kamer 2015-16, 17 december 2015, CRIV54PLEN090, 16, Vr. nrs. 885 tot 891)

Vraag van S. Van Hecke aan de minister van Justitie over 'het protocolakkoord tussen de Nationale Bank en de Staatsveiligheid' (*Hand.* Kamer 2015-16, 6 januari 2016, CRIV-54COM301, 3, Vr. nr. 8170)