RAPPORT D'ACTIVITÉS 2017
ACTIVITEITENVERSLAG 2017

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 renseignements 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.
15) Comité permanent R, *Rapport d'activités 2016*, 2017, 227 p.
16) Comité permanent R, *Rapport d'activités 2017*, 2018, 152 p.

RAPPORT D'ACTIVITÉS 2017

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 2017* a été approuvé par le Comité permanent de Contrôle des services de renseignements et de sécurité lors de la réunion du 5 septembre 2018.

(*soussignés*)
Guy Rapaille, Président
Pieter-Alexander De Brock, Conseiller
Laurent Van Doren, Conseiller
Wouter De Ridder, Greffier

Rapport d'activités 2017
Comité permanent de Contrôle des services de renseignements et de sécurité

ISBN 978-94-000-1003-1
D/2018/7849/116
NUR 823

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

A.M.	Arrêté ministériel
Ann. parl.	Annales parlementaires
ANS	Autorité nationale de sécurité
APD	Autorité de protection des données
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 FTF	Arrêté royal du 21 juillet 2016 relatif à la banque de données commune 'Foreign Terrorist Fighters' et portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police
AR OCAM	Arrêté royal du 28 novembre 2006 portant exécution de la Loi du 10 juillet 2006 relative à l'analyse de la menace
BELPIU	*Belgian Passenger Information Unit* (Unité belge d'information des passagers)
BISC	*Belgian Intelligence Studies Centre*
BNB	Banque nationale de Belgique
BNG	Banque de données nationale générale
CAC	*Conduct After Capture*
CEDH	Convention européenne des droits de l'homme
CHOD	*Chief of Defence*
CI	*Counterintelligence*
CIC	Code d'instruction criminelle
CICB	Centre Islamique et Culturel de Belgique
CNCIS	Commission nationale de contrôle des interceptions de sécurité
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNS	Conseil national de sécurité
C.O.C.	Organe de contrôle de l'information policière
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
CP	Code pénal
CPE	Commission d'enquête parlementaire
CPVP	Commission (de la protection de la) vie privée
CRIV	Compte Rendu Intégral – *Integraal Verslag*
CTIF	Cellule de Traitement des Informations Financières
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten*
C-Ops	Centre des opérations
DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
DG EPI	Direction générale des Établissements pénitentiaires
DGSE	Direction Générale de la Sécurité Extérieure
Doc. parl.	Documents parlementaires de la Chambre et du Sénat
EI	État islamique
FRA	Agence des droits fondamentaux de l'Union européenne – *European Agency for Fundamental Rights*
FTF	*Foreign terrorist fighters*
HTF	*Homegrown terrorist fighters*
HUMINT	*Human intelligence*
ICT	*Information and communications technology*
IMINT	*Image intelligence*
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
LFP	Loi du 5 août 1992 sur la fonction de police
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
LTF	*Local task forces*

M.B.	Moniteur belge
MoU	*Memorandum of Understanding*
MRD	Méthodes de recueil des données
NTF	*National Task Force*
OCAM	Organe de coordination pour l'analyse de la menace
OE	Office des étrangers
ONU	Organisation des Nations Unies
OSINT	*Open sources intelligence*
OTAN	Organisation du Traité de l'Atlantique Nord
PCC	Point de contact central
PES	Potentiel économique et scientifique
POC	*Point of contact*
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
SGRS	Service Général du Renseignement et de la Sécurité
SIGINT	*Signal intelligence*
SPF	Service public fédéral
TCCC	*Tactical Combat Casualty Care*
TF	*Terrorist fighters*
VSSE	Sûreté de l'État

PRÉFACE

Ces dernières années, le nombre de missions confiées au Comité permanent R n'a cessé de croître. Les missions existantes ont été étendues ou ont reçu un contenu pour la première fois. Le Comité s'est également vu confier plusieurs nouvelles tâches importantes. Cette inflation de missions a eu pour corollaire un alourdissement de la charge de travail, mais sans octroi de moyens supplémentaires.

L'extension des missions existantes est la conséquence indirecte de l'extension des compétences et des effectifs attribués aux services qui relèvent du contrôle du Comité. La VSSE et le SGRS bénéficient désormais d'un plus grand champ d'action, ce qui implique, par exemple, une augmentation du nombre de méthodes particulières de renseignement à contrôler ainsi que d'autres méthodes à contrôler. Le même phénomène se produit pour l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité : qui dit plus de secteurs soumis à un screening de sécurité obligatoire, dit plus de recours… Avec la nouvelle Loi du 23 février 2018, le nombre de screenings, et donc de recours, suivra inéluctablement une courbe ascendante.

En outre, l'attribution de nouvelles missions aux services de renseignement a des répercussions sur le Comité permanent R. À titre d'exemple, le SGRS s'est vu attribuer un rôle central dans le cadre de la cybersécurité. Un contrôle sérieux sur cette activité de renseignement est conditionné à la capacité du Comité d'investir dans du personnel doté d'expertises spécifiques.

Par ailleurs, le Comité est confronté au fait que les compétences existantes doivent être davantage assurées, voire que de nouvelles tâches doivent être exécutées. Ainsi, ces trois dernières années, le Comité a formulé, à la demande du Parlement ou d'un ministre, autant d'avis qu'au cours de ces quinze dernières années. Autre nouveauté : le Comité a été impliqué dans deux commissions d'enquête parlementaires. Il s'est considérablement investi, mais – hélas – au détriment d'autres missions…

Enfin, il convient de mentionner les nombreuses dispositions légales qui sont à l'origine de nouvelles missions pour le Comité : le contrôle des banques de données communes FTF (devenu *foreign fighters*) et 'prédicateurs de haine' qui sont gérées par l'OCAM, le contrôle de certaines missions du bataillon ISTAR, le contrôle de la manière dont le SGRS effectue des prises d'images et des intrusions dans des systèmes informatiques, un contrôle renforcé de certaines méthodes ordinaires, le contrôle de la manière dont les services de renseignement fonctionnent au sein de l'Unité d'information des passagers (BELPIU) et dont ils font usage de certaines images enregistrées par des caméras.

Alors que l'impact de toutes ces missions récentes n'était pas encore évalué, à la mi-2018, il est apparu qu'une nouvelle mission viendrait s'ajouter à la liste : le Comité fait office d'Autorité de protection des données pour presque toutes les données à caractère personnel qui ont un lien avec la 'sécurité nationale'. Dans ce cadre, le Comité devra non seulement tenir compte des demandes individuelles, mais il devra aussi rendre des avis et conclure des protocoles avec d'autres autorités de protection des données.

Les nouvelles et nombreuses initiatives législatives pèsent lourdement sur l'équilibre précaire entre, d'une part, les droits et les libertés des citoyens, et d'autre part, la limitation de ces droits et libertés, en raison des risques de sécurité qu'ils encourent. Mais le Comité doit lui aussi tenter de trouver cet équilibre. Le Comité a été institué pour remplir ses missions de contrôle de manière indépendante et impartiale, entre autres pour donner l'assurance aux citoyens que les droits qui leur sont conférés par la loi et la Constitution sont et demeurent garantis. La qualité du travail que peut fournir le Comité permanent R est non seulement essentielle pour garantir les droits des citoyens, mais elle constitue aussi un facteur nécessaire de la confiance que les diverses structures étatiques doivent pouvoir leur inspirer.

Ces dernières années, le Comité n'a laissé passer aucune occasion de rappeler aux autorités compétentes qu'il ne suffit pas de voter des lois instituant un contrôle, encore faut-il investir dans l'organe de contrôle. Ainsi, en octobre 2016, le Comité a exprimé ses préoccupations à la Commission Justice de la Chambre, et ce, à l'occasion des discussions sur la modification de la loi sur les services de renseignément, qui se voyaient attribuer de nouvelles compétences soumises au contrôle du Comité. En outre, un courrier commun a été rédigé avec toutes les institutions à dotation qui sont confrontées au même problème, et la problématique de la réduction des moyens a fait l'objet de discussions approfondies lors de l'audit mené au sein de ces institutions à la demande du Président de la Chambre. Dans le cadre de cet audit, des réserves ont été émises sur le nombre de membres du personnel auxiliaire. Le Comité permanent R ne partage pas cet avis. Certaines missions – comme par exemple le fonctionnement de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité dont le greffe est assuré par le Comité – requièrent un large appui administratif qui est entièrement supporté par le Comité.

Comme président sortant du Comité permanent R, je ne peux qu'espérer que cet appel à mobiliser davantage de moyens sera entendu, afin que les restrictions budgétaires annoncées, combinées à l'accroissement des compétences et de la charge de travail, n'aient pas un effet négatif sur la qualité du fonctionnement d'un organe qui joue un rôle fondamental dans notre État de droit démocratique.

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

5 septembre 2018

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'Organe de coordination pour l'analyse de la menace et, dans une moindre mesure, de ses services d'appui. Les recommandations émises par le Comité en 2017 figurent au dernier chapitre du présent rapport d'activités.

Ces dernières années, le premier chapitre énumérait les principales initiatives prises l'année précédente par les différents acteurs, dans la lignée des recommandations du Comité permanent R, et une attention particulière était portée aux recommandations que le Comité estimait essentielles, mais qui n'avaient pas encore été mises en œuvre.

Le *Rapport d'activités 2006*[1] avait offert un aperçu des recommandations les plus importantes que le Comité permanent R et ses Commissions de suivi avaient formulées entre 1994 et 2005, et de la suite qui leur avait été réservée.

Le Comité permanent R a procédé au même exercice pour la période 2006-2016, répondant en même temps à une demande de la Commission parlementaire de suivi. Dans le cadre de la discussion sur le *Rapport d'activités 2015*, il avait en effet été suggéré que le Comité dresse *'une liste des recommandations non encore exécutées et que la Commission consacre une réunion aux recommandations afin de voir quelles initiatives elle pourrait prendre'*.[2]

Le Comité a initié ce projet en 2016. Dans le courant de l'année 2017, la mission assignée par la Commission de suivi a été reprise et affinée. Le Comité a examiné quelles recommandations avaient déjà été concrétisées pour cette période et a vérifié si les recommandations qui ne l'avaient pas été étaient toujours d'actualité. Ces recommandations ont été reformulées si cela s'avérait

---

1 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 1-20 ('Chapitre I. Les recommandations antérieures du Comité permanent R et des Commissions de suivi').

2 *Doc. parl.*, Chambre 2016-17, n° 54-2185/1 (Rapport d'activités 2015 du Comité permanent de Contrôle des services de renseignement et de sécurité, Rapport fait au nom de la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de Contrôle des services de renseignement et de sécurité), 7.

nécessaire et utile. Ce travail a abouti à un document conséquent, qui a été transmis à la Commission de suivi en décembre 2017 et qui a été discuté en février 2018. En raison du volume de ce document, il a été décidé de le reprendre à l'"Annexe D' du présent rapport d'activités.

CHAPITRE II
LES ENQUÊTES DE CONTRÔLE

En 2017, le Comité permanent R a finalisé cinq rapports d'enquête, dont un conjointement avec le Comité permanent P (II.1 à II.5). Le Comité a également ouvert trois nouvelles enquêtes de contrôle, dont une avec le Comité permanent P. Deux enquêtes ont été ouvertes d'initiative. Dans une enquête, le Comité permanent R était saisi par le ministre de la Défense (art. 32 L. Contrôle).[3] Les trois enquêtes qui ont été initiées sont brièvement décrites au point II.6.

Au total, le Comité a reçu 35 plaintes ou dénonciations en 2017. Depuis 2016, le processus de travail 'plaintes et dénonciations' fait l'objet d'un assouplissement, d'une 'déformalisation' et d'une standardisation.[4] Après la vérification de plusieurs données objectives, le Comité a rejeté 34 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 griefs. Dans ces derniers cas, les plaignants ont été renvoyés, si possible, vers les instances compétentes (le Comité permanent P, la Police fédérale, le procureur du Roi). Une des plaintes introduites en 2017 a donné lieu à l'ouverture d'une enquête de contrôle.

En plus des enquêtes de contrôle, le Comité permanent R a ouvert ce que l'on appelle des 'dossiers d'information'. Ceux-ci doivent permettre de répondre à des questions relatives au fonctionnement des services de renseignement et de l'OCAM.[5] Si de tels dossiers font apparaître des indices de dysfonctionnement ou des aspects du fonctionnement des services de renseignement qui requièrent un examen approfondi, le Comité peut procéder, dans un deuxième temps, à

---

3 Il est plutôt rare que le Comité soit saisi par un membre du pouvoir exécutif. Voir à ce propos : VAN LAETHEM, W. et VANDERBORGHT, J., 'Torture numbers, and they'll confess to anything. Een analyse van twintig jaar toezichtonderzoeken, studies en adviezen' dans VAN LAETHEM, W. et VANDERBORGHT, J. (eds.), *Regards sur le contrôle. Vingt ans de contrôle sur les services de renseignement*, Antwerpen, Intersentia, 2013, 266.

4 Dans un premier temps, la recevabilité de la plainte est examinée avant que le Service d'Enquêtes n'en assure le traitement. Dans le cas d'une problématique générique, le Comité peut décider d'ouvrir une enquête de contrôle, sinon l'enquête reste limitée à la plainte (une enquête relative à une plainte).

5 Le Comité permanent R peut ouvrir un dossier d'information pour des raisons très diverses : une plainte a été déposée et le Comité permanent R souhaite exclure le plus rapidement possible l'absence manifeste de fondement ; la direction d'un service de renseignement fait état d'un incident et le Comité souhaite vérifier comment cet incident a été traité ; les médias signalent un événement et le Comité souhaite déterminer si ces faits sont conformes à la réalité et s'ils relèvent d'une problématique plus générale….

l'ouverture d'une enquête de contrôle formelle. Si toutefois il apparaît que ce genre d'enquête n'apporterait aucune plus-value au regard des finalités du Comité permanent R, aucune suite n'est donnée au dossier d'information. En 2017, un dossier d'information a notamment été ouvert sur le déploiement d'une capacité de renseignement du SGRS en zone de conflit, ce qui a abouti à l'ouverture d'une enquête de contrôle en 2018.

Enfin, des briefings sont très régulièrement organisés, rencontres au cours desquelles des membres des services de renseignement informent le Comité sur des thématiques actuelles et importantes au sein de la communauté du renseignement (p. ex. le fonctionnement de l'Unité belge d'information des passagers BELPIU, la mise en œuvre de la directive en matière de collaboration avec des services partenaires étrangers, la manière dont certains pays tentent d'exercer une influence sur les intérêts belges, le fonctionnement de la section SIGINT, les nouveautés technologiques dans le cadre des méthodes particulières de renseignement, le *risk-assessment* et la lutte contre le terrorisme…). Ces briefings doivent promouvoir une discussion approfondie sur le fonctionnement, les compétences et le contrôle des services de renseignement et de sécurité et de l'OCAM, ainsi que sur le travail de renseignement. Ils peuvent également donner lieu à l'ouverture d'une enquête.

II.1. UNE PLAINTE CONCERNANT TROIS OPÉRATIONS DU SGRS

II.1.1. CONTEXTE

En mai 2017, un officier du SGRS a introduit une plainte concernant une série d'opérations qui ont ou auraient été effectuées par la Section I/H[6] du SGRS. Selon lui, des irrégularités, voire des illégalités, devaient être signalées. Le Comité permanent R a alors décidé d'ouvrir une enquête de contrôle.[7, 8] Cette enquête a été menée parallèlement à une enquête judiciaire, l'officier s'étant également adressé au Parquet.[9]

---

6 La Section I/H est une composante de la Division I du SGRS. Elle a pour mission de constituer des réseaux de sources et d'informateurs afin de permettre au SGRS de collecter des renseignements sur des phénomènes étrangers. Le plaignant a été actif dans cette section pendant environ deux ans.

7 Le ministre de la Défense et le Parlement ont été informés de l'ouverture de l'enquête de contrôle le 10 mai 2017. L'enquête a été clôturée le 14 juillet 2017.

8 En 2018, il a été décidé que la Section I/H ferait l'objet d'une enquête de contrôle élargie. La présente enquête se limite à la plainte.

9 Il a été fait appel à des enquêteurs du Service d'Enquêtes R dans le cadre de l'enquête pénale. Ces enquêteurs n'étaient pas impliqués dans l'enquête de contrôle.

La plainte se déclinait en trois volets :
- La Section I/H aurait eu l'intention de créer une 'cellule action' sur le territoire belge ;
- Un envoi de membres de la Section I/H dans une zone de conflit était problématique ;
- Le SGRS entretenait des contacts en Belgique avec une personne liée à un groupement qui serait étroitement impliqué dans une organisation terroriste.

II.1.2. UNE NOUVELLE 'CELLULE ACTION' AU SEIN DU SERVICE DE RENSEIGNEMENT MILITAIRE ?

II.1.2.1. Éléments communiqués par le plaignant

Le plaignant affirmait qu'il existait, au sein de la Section I/H, un embryon de 'service action'. Celui-ci collecterait des renseignements, mais, à l'instar des cellules actions de la DGSE française, monterait également des 'actions'. Alors que ce genre de service ne mène en principe ses opérations qu'à l'étranger, l'idée aurait germé d'en mener également sur le territoire belge.

Le plaignant avançait divers éléments démontrant que les préparatifs étaient en cours : un collaborateur de la Section I/H aurait loué un stand de tir privé pour y former au tir une personne externe (un non-militaire) avec des armes de guerre ; le plaignant faisant mention d'un échange de SMS entre le commandant de I/H et son chef de division, dans lequel il serait question de l'activation d'un 'service action' sur le territoire belge. Une formation *survival training* aurait été organisée à l'étranger pour des externes, et des membres de la section ont suivi une formation *Conduct After Capture* (CAC).[10]

II.1.2.2. Constatations du Comité permanent R

La Section I/H a effectivement loué, à trois moments différents, un stand de tir privé, qui disposait toutefois des autorisations officielles requises. Cette opération a reçu l'approbation formelle de la hiérarchie de la Division I. La location d'un stand de tir privé est une pratique courante depuis longtemps déjà, y compris pour les membres de la Section I/Ops et de la Division CI. Il apparaît que l'utilisation d'un stand de tir militaire est effectivement soumise à toutes sortes de limitations.[11] La personne ayant reçu une initiation était une source qui s'était

[10] Il s'agit d'une formation qui est organisée en priorité pour les pilotes de Composante Air de l'Armée belge pour les préparer au cas où ils seraient abattus derrière des lignes ennemies.

[11] Il faut s'y prendre très longtemps l'avance, ce qui n'est pas toujours possible lorsque les membres de la Section I/H doivent partir à l'étranger. De plus, le propriétaire du stand de tir pouvait mettre à disposition d'autres armes que les armes standards de l'Armée belge auxquelles les membres de la Section I/H pourraient être confrontés au cours de leurs missions à l'étranger.

déjà retrouvée, par le passé, dans une situation très dangereuse à l'étranger. La Section I/H estimait qu'il était opportun de lui expliquer les manipulations de base d'une arme à feu. La cellule formation au sein de la Section I/H n'avait pas apparemment pas été informée de la location du stand de tir. Inutile, selon l'officier formateur, puisqu'il s'agissait d'une formation technique.

Par ailleurs, le Comité a pu constater que dans un échange de SMS entre le Commandant de la Section I/H et le Chef de la Division I, l'engagement de la section I/H sur le territoire belge avait bien été abordé et qu'un 'service action' avait bien été mentionné. Le Comité estime toutefois que le contenu de cet échange doit être remis dans son contexte : il a eu lieu au lendemain des attentats de Paris, lorsque la Belgique était placée au niveau 4 de la menace. Il n'était pas question de déployer un 'service action' en Belgique, mais le Commandant de la Section I/H proposait que les membres de cette section assistent, si nécessaire, leurs collègues de la Division CI sur le territoire belge, mais seulement pour collecter des renseignements. Cependant, dans la pratique, les membres de la Section I/H n'ont pas été sollicités pour intervenir en Belgique.

Début janvier 2015, la Section I/H a envoyé une personne de nationalité belge, mais qui ne faisait pas partie du SGRS, à un *survival training* de plusieurs jours à l'étranger. Le Comité a pu constater qu'il s'agissait d'une nouvelle source de la Section I/H, qui, pour sa propre sécurité pendant les missions, avait besoin de développer sa confiance en lui et sa résistance. La formation avait été élaborée en collaboration avec la cellule formation interne de la Section I/H, qui, après avoir dressé un profil psychologique de l'intéressé, avait conclu que cette formation était effectivement adaptée pour lui permettre d'acquérir de nouvelles compétences.

En ce qui concerne la formation CAC à laquelle des membres de la Section I/H auraient participé, le Comité a pu dresser les constats suivants : deux membres – dont le responsable de la cellule formation – de la Section I/H ont suivi la version 'light' de la formation. L'objectif était d'évaluer l'intérêt de cette formation pour les membres de la section. La conclusion s'est révélée être négative.

Au vu de ce qui précède, le Comité permanent R est arrivé à la conclusion qu'il n'y avait aucune raison de supposer qu'il y a ou avait une intention de développer la Section I/H en 'service action' ou de l'activer sur le territoire belge. De plus, toutes les formations se sont déroulées dans le respect des règles en vigueur à la Défense.

II.1.3. LA MISSION DANS UNE ZONE DE CONFLIT ET L'APPUI À UNE ORGANISATION SUR PLACE

II.1.3.1. Éléments communiqués par le plaignant

Cette question portait sur une mission menée en juillet 2015 par quelques membres de la Division I dans une zone de conflit. Au cours de cette mission, un contact a été pris avec un service de renseignement d'une organisation sur place.

Du matériel médical a également été livré, et des instructions de tir ont apparemment été données à des troupes locales.

II.1.3.2. Les constatations du Comité permanent R

En février 2015, des militaires de la Division I se sont rendus dans une zone de conflit. Le but de l'opération consistait à développer des contacts avec des acteurs (militaires) et d'y installer sur place une connexion informatique sécurisée, qui permettrait une transmission des renseignements vers la Belgique. Des *foreign terrorist fighters* (FTF) belges qui se sont ralliés à l'EI étaient susceptibles de se trouver dans cette région ou d'y transiter. L'espoir était de pouvoir recueillir des renseignements sur les FTF par le biais de ces acteurs locaux. L'idée était également d'établir des contacts amicaux avec les milices et les troupes présentes, au cas où un F-16 belge serait abattu dans cette région et que le pilote devrait ensuite être exfiltré.[12]

L'opération a été initiée à la demande du Chef du SGRS de l'époque. La chaîne classique de commandement a été suivie[13], et une concertation régulière a été organisée concernant des démarches à entreprendre et des missions à effectuer. À leur retour, les membres de la Section I/H qui ont mené ces missions ont systématiquement établi des rapports circonstanciés.

La mission de février 2015 avait déjà débuté en septembre 2014 via un contact avec l'ambassade concernée en Belgique. Les premiers contacts à l'étranger ont eu lieu en octobre et décembre 2014. Une autre mission est partie en juillet 2015 : la délégation belge (des membres de la Section I/H) a visité un camp d'entraînement des troupes locales, et des sacs à dos contenant du matériel médical ont été offerts, en contrepartie des renseignements livrés au SGRS par les services de renseignement locaux. Ce matériel médical devait permettre de dispenser les premiers soins dans des conditions de combat.[14] Un membre du SGRS, formé à cet effet, a réalisé sur place une démonstration de l'utilisation de l'équipement.

---

12 En ce sens, cette opération de renseignement se situait dans le droit fil de la décision gouvernementale de fin 2014 d'engager les F-16 belges et de participer au *Building Partner Capacity Program*.

13 L'existence de l'opération a également été révélée au CHOD en fonction à ce moment-là, lors d'un briefing qui a eu lieu le 29 mars 2015.

14 Il s'agit de l'entraînement *Tactical Combat Casualty Care* (TCCC). Le matériel est utilisé dans des conditions 'réalistes', c'est-à-dire partiellement dans un véritable camp d'entraînement, avec des participants équipés pour le combat, et parfois même sous le feu des balles. Cela peut être considéré, à tort, comme une 'instruction de tir', mais il s'agit d'une des situations dans lesquelles des blessés peuvent être évacués sous le feu. Ce type de mission fait normalement partie des interventions ou des missions d'entraînement des unités opérationnelles de la Défense (Special Forces ou OPS/Trn). Dans le cas présent, la mission relevait du renseignement. La brève initiation qui a été donnée lors de la livraison du matériel ne constituait qu'une modalité pratique de la mission.

II.1.3.3. Le cadre général de l'engagement de militaires à l'étranger

Selon le CHOD, ce type de mission s'inscrit dans un double cadre. D'une part, la mission est couverte par le 'Plan d'opération' de la Défense, qui est élaboré au niveau du CHOD et approuvé par le Gouvernement. Ce plan prévoit une capacité permettant au SGRS d'engager plusieurs militaires pour effectuer des missions à l'étranger, sans autre spécification. D'autre part, un Plan Directeur du Renseignement (PDR) est approuvé par le ministre de la Défense, plan qui fait de la collecte de renseignements sur la région concernée une priorité (vu qu'il s'agit d'une zone d'opération de la Défense belge).

Au moment où l'opération a débuté, il n'y avait pas encore de directive (politique) officielle émanant du Conseil national de sécurité et fixant les critères permettant de déterminer avec quels services de renseignement externes une collaboration était possible et dans quelle mesure elle l'était.[15]

II.1.3.4. Les informations communiquées aux échelons militaire et politique

La chaîne de commandement classique a été suivie au sein de la Section I/H et du SGRS : I/H a reçu l'approbation formelle d'exécuter la mission et a tenu la hiérarchie parfaitement informée des opérations. Le CHOD a, il est vrai, reçu un briefing après la mission de février 2015, et le chef de la Composante Air de l'Armée belge a lui aussi été informé (mais pas des détails opérationnels).

En dehors des chaînes militaires, le Comité permanent R et la VSSE ont été briefés (avril 2016), mais les détails opérationnels ne leur ont pas non plus été communiqués.

Lors d'une précédente enquête de contrôle[16], le Comité avait affirmé que dans des cas spécifiques de collaboration au niveau international, une évaluation et une couverture politiques s'imposaient. Le Comité avait recommandé, à l'époque, que les ministres compétents soient suffisamment informés pour pouvoir assumer leur responsabilité politique à l'égard du Parlement. Dans le cas présent, le ministre de la Défense et son Cabinet ont été mis au courant. Plusieurs éléments y ont contribué : le fait que l'opération et la mission ont été exécutées par un bureau spécial de la Section I/H ; le fait qu'il s'agissait d'une opération dans une zone de conflit et, plus encore, dans une zone d'opération aérienne de la Défense belge (qui plus est au centre de l'intérêt militaire et politique belge, si bien que les opérations menées sur place pouvaient avoir des répercussions politiques) ; et qu'il y avaient des risques opérationnels spécifiques pour les membres du SGRS impliqués. Ces éléments peuvent être considérés comme des

---

15 Ce n'est que plus tard que cette directive a été émise (Directive du 26 septembre 2016 concernant les relations des services de renseignement belges avec les services de renseignement étrangers).

16 Voir notamment COMITÉ PERMANENT R, *Rapport d'activités 2014,* 32-33 et 117-118.

risques dont il convient de tenir compte lorsque la décision de mener une opération est prise : plus le risque est élevé, plus vite le ministre doit être informé.

Compte tenu de tous ces éléments, le Comité permanent R a donc estimé que briefer le ministre de la Défense relevait de l'évidence. Il revenait au dirigeant du service de choisir le moment opportun. Le SGRS a agi comme il se doit à cet égard.

Toutefois, dans ce cas-ci, le Comité permanent R a constaté l'absence de cadre structuré et de formalisation de l'analyse des risques stratégico-politiques *et* militaires.[17] Plusieurs moments ont pourtant été consacrés à l'évaluation.

Le Comité a par ailleurs constaté que c'est un service d'expédition privé qui a acheminé sur place le matériel médical dont il est question. Cette opération présentait un risque particulier pour la personne impliquée, mais cet aspect n'a apparemment pas été examiné au préalable.

II.1.4. LES CONTACTS AVEC UN GROUPEMENT ÉVENTUELLEMENT LIÉ À UNE ORGANISATION TERRORISTE NON ISLAMISTE

II.1.4.1. Éléments communiqués par le plaignant

Un troisième grief formulé par le plaignant concernait les contacts du SGRS et de la Section I/H avec une personne qui appartiendrait à un groupement actif dans une zone de conflit. Ce groupement ferait partie d'une organisation terroriste non islamiste ou, à tout le moins, aurait des liens étroits avec celle-ci. Le SGRS aurait non seulement entretenu des contacts avec ce service de renseignement non gouvernemental, mais il aurait aussi joué un rôle de facilitateur lors de contacts entre ce groupement non gouvernemental (ou la personne qui en est issue) et une firme belge. Le groupement tentait, en effet, de se procurer du matériel, certes non létal, par le biais de leur représentant.

II.1.4.2. Constatations du Comité permanent R

Le Comité permanent R a constaté que le SGRS avait effectivement eu des contacts avec un groupement, que ce soit en Belgique ou, par la suite, dans la zone de conflit dans laquelle ce groupement était actif. Le but de l'opération était de renforcer le réseau de renseignement du SGRS. En effet, ce groupement était un acteur important dans cette région et représentait une source potentielle de renseignements sur les *foreign terrorist fighters* belges. D'autres accès à des sources dans d'autres zones de conflit étaient même envisagés par ce canal.

[17] Pour les missions dans ces zones de conflit, la Section I/H a utilisé pour la première fois en mars et en avril 2017 un document spécifique afin de déterminer les risques opérationnels.

La question qui se posait était de savoir ce que le SGRS pouvait donner au groupement en échange des renseignements (*do-ut-des*). Lors d'une réunion préparatoire, il avait été question de matériel non létal.

En ce qui concerne la qualification du groupement ('terroriste' ou 'lié à une organisation terroriste'), le Comité a constaté qu'en 2015, les services d'analyse de la Division I avaient décrit le groupement comme étant une 'franchise' d'une organisation terroriste non islamiste. Cette organisation terroriste non islamiste est également mentionnée dans plusieurs rapports de la Section I/H, lorsqu'il est question du représentant en Belgique du groupement qui y est lié. Enfin, une puissance régionale considère le groupement comme étant l'aile d'une organisation terroriste et donc – par définition – comme étant lui-même un groupement terroriste.

D'autre part, le groupement ne figure pas sur une liste internationale d'organisations terroristes, même si ses agissements dans la zone de guerre étaient clairement controversés. Par ailleurs, le SGRS n'était pas le seul service à être en relation avec ce groupement ; l'armée d'une puissance alliée lui déjà apporté son soutien en septembre 2014 et lui livrait des armes depuis mai 2017.

Le Comité en a dès lors conclu que, formellement, le groupement n'était pas, jusqu'à nouvel ordre, une organisation terroriste, mais qu'il était plus qu'évident que les contacts avaient un caractère sensible.

Le Comité permanent R a constaté qu'il s'agissait d'une opération de renseignement conforme au Plan Directeur du Renseignement, mais que certains éléments particuliers appelaient à la prudence.

II.1.4.3. Les informations communiquées aux échelons militaire et politique

La hiérarchie de la Section I/H était systématiquement informée des contacts, que ce soit au sein de la Division I ou au niveau du Commandement. Le Département CI de la Division SI était lui aussi informé.[18] D'autres autorités militaires ne l'étaient pas, pas même le CHOD[19], qui n'a été mis au courant que fin avril 2017.

Dès le début de l'opération, la Section I/H avait pris contact avec les autorités judiciaires (d'abord avec la Police judiciaire fédérale et en suite avec le magistrat fédéral) pour l'/les informer que la personne concernée participait à une opération de renseignement. Un représentant de la VSSE était également présent à la réunion. À partir du moment où l'opération a été lancée, les différents services sont restés en contact.

---

18 Au début de l'opération, la Section I/H a été informée par CI que la personne concernée était citée dans un dossier judiciaire du Parquet fédéral, qui est compétent en matière de terrorisme.

19 Selon le CHOD, il serait utile de porter ce genre d'opération à la connaissance de C-Ops en priorité, avant même le CHOD, de sorte que C-Ops soit conscient que des militaires belges sont secrètement présents dans la zone.

Le ministre de la Défense n'a pas été briefé avant l'opération et n'a été informé que fin avril 2017. Pourtant, on retrouvait les mêmes éléments que lors de l'opération précédente (*supra*) : l'opération a été menée par la Section I/H et était par définition très délicate ; il s'agissait d'une mission en zone de conflit avec des risques opérationnels accrus, qui plus est dans une région d'influence d'un partenaire de l'OTAN dont on connaissait le peu d'engouement pour ce groupement. Ce genre d'éléments devait être pris en considération quand il s'agissait pour le service de renseignement d'apprécier la nécessité et le moment d'avertir le ministre. En outre, un lien existait entre l'organisation concernée et un groupe terroriste (même si l'organisation ne figurait pas sur une liste terroriste internationale), il y avait également un lien avec une enquête judiciaire en cours. Par ailleurs, on savait que les contacts avec le groupe terroriste pouvaient avoir un impact négatif sur les relations que la VSSE entretenait avec un service partenaire et que l'opération pouvait s'en trouver compromise. Compte tenu de l'intérêt de l'opération pour le SGRS, mais aussi du caractère sensible (voire risqué) de celle-ci pour les relations de la Belgique au niveau international, le Chef du SGRS aurait dû en informer l'Administrateur général de la VSSE afin de parvenir à une position commune au plus haut niveau.

Étant donné qu'il s'agissait d'une opération à haut risque, le Comité permanent R était d'avis que le ministre de la Défense devait impérativement être briefé. Et le Comité d'estimer qu'il appartenait au dirigeant du service de choisir le moment opportun. Interrogé à ce propos, le Chef du service a répondu qu'il considérait que l'opération était encore à un stade embryonnaire et que le ministre de la Défense (et le CHOD) aurai(en)t bien été informé(s) à la première avancée concrète. Selon le Comité permanent R, informer ou non le ministre à temps est un choix d'opportunité qui, en définitive, ne peut être apprécié que par l'intéressé. Compte tenu du fait que le Cabinet du ministre a affirmé à ce propos que le ministre (qui a effectivement eu connaissance des faits après la divulgation de l'opération) couvrait entièrement l'opération, il y avait lieu de considérer que le ministre estimait que le SGRS avait agi de manière conforme.

Enfin, il est vrai que des éléments d'une analyse de risques ont été repris dans divers documents – il a par exemple été décidé de ne pas rencontrer ce groupement en Belgique au vu du danger de compromission par un pays partenaire – mais il n'y a eu aucune appréciation globale du risque. Le fait qu'une telle analyse aurait pu faire apparaître le rôle de la VSSE revêt un intérêt spécifique. En effet, le SGRS savait que la VSSE était en relation avec un service partenaire au sein de l'OTAN et que ce service n'apprécierait pas les contacts belges avec ce groupement.

II.2. LA DEMANDE POTENTIELLEMENT INJUSTIFIÉE DE TRANSACTIONS BANCAIRES ET LE SECRET PROFESSIONNEL

II.2.1. UNE PLAINTE EN DEUX VOLETS

À la mi-août 2017, le Comité permanent R a reçu, par l'intermédiaire d'un avocat, une plainte de l'administratrice déléguée d'un cabinet comptable. La plainte visait un inspecteur de la VSSE et se composait de deux parties : il était mentionné, d'une part, que l'inspecteur avait fait pression sur l'administratrice déléguée, ce qui l'avait contrainte à violer le secret professionnel auquel elle est tenue[20] et, d'autre part, que les informations demandées auraient dû faire l'objet d'une méthode particulière de renseignement (art.18/15 L.R&S).

II.2.2. RÉSUMÉ DES FAITS

À la mi-juillet 2017, l'inspecteur de la VSSE a contacté par téléphone le cabinet comptable. L'administratrice déléguée étant absente, l'inspecteur a laissé ses coordonnées. Il a déclaré s'être présenté comme étant un membre du personnel du SPF Justice qui souhaitait obtenir des renseignements dans le cadre d'une enquête pour blanchiment.

À son retour, l'administratrice déléguée a pris contact avec l'inspecteur et a finalement marqué son accord pour une rencontre début août 2017. Dès son arrivée au cabinet comptable, l'inspecteur s'est identifié comme étant un membre de la Sûreté de l'État, en montrant sa carte de légitimation officielle (carte de service), et a expliqué les circonstances réelles entourant sa visite (une enquête sur d'éventuelles activités d'espionnage). La VSSE manifestait un intérêt pour un client du cabinet comptable. Des informations ont été demandées sur la manière dont les contacts avaient été établis, ainsi qu'une consultation des livres d'achats et de ventes et des copies d'e-mails… Une copie des comptes annuels du target a également été remise.

Les déclarations divergeaient quant à l''obligation' de coopérer : selon l'administratrice déléguée, l'inspecteur avait affirmé qu'elle était 'obligée' de coopérer. L'inspecteur affirmait quant à lui n'avoir pas parlé explicitement d'une 'obligation', mais avoir fait référence à la Loi sur les services de renseignement.

Il n'y a plus eu d'autres contacts entre la VSSE et le cabinet comptable.

---

[20] Visé à l'art. 58, alinéa 4 de la Loi du 22 avril 1999 relative aux professions comptables et fiscales et à l'art. 458 CP.

II.2.3. ÉVALUATION

De l'avis du Comité permanent R, l'intervention de l'inspecteur de la VSSE n'est en rien inadmissible. Il a pris contact par téléphone pour demander un rendez-vous. Il s'est identifié comme étant un membre du personnel de la Justice, ce qui est exact. Il a certes invoqué 'des pratiques de blanchiment' (ce qui ne correspondait pas à la réalité), mais il ne pouvait pas donner d'informations classifiées par téléphone. L'utilisation d'une *coverstory* lors d'un premier contact, certainement un contact téléphonique, est acceptable, mais ce qui ne l'est pas, c'est de laisser entendre qu'on dispose de compétences spécifiques.

L'enquête n'a pas pu déterminer si l'intéressé avait réellement évoqué une 'obligation', et si tel était le cas, ce qu'il aurait pu sous-entendre.[21] Le Comité permanent R n'était pas en mesure de constater les termes exacts employés lors de l'entretien, mais il n'a pas constaté, dans le chef de l'inspecteur, un comportement inconvenant, intimidant ou impoli.

L'administratrice déléguée affirmait par ailleurs être tenue de respecter un secret professionnel spécifique, y compris dans ses contacts avec la VSSE. Elle aurait été amenée à violer le secret professionnel de manière tout à fait injustifiée. L'article 16 L.R&S, tel que modifié par la Loi du 30 mars 2017 (loi qui était donc d'application en août 2017, lorsque l'entretien entre la VSSE et l'administratrice déléguée a eu lieu), dispose que les personnes et les organisations privées peuvent communiquer aux services de renseignement des informations et des données à caractère personnel qu'elles jugeraient utiles à l'exercice des missions de ces services, et inversement, que les services de renseignement peuvent demander de telles données. Cette disposition n'impose pas de restrictions au secret professionnel des personnes ou des instances privées, sauf en ce qui concerne le secret professionnel des avocats et des médecins, ainsi que le secret des sources des journalistes. On peut donc conclure *a contrario* que d'autres formes de secret professionnel ne s'appliquent pas aux relations avec la VSSE. Le Comité estime toutefois qu'il serait indiqué que le législateur détermine plus explicitement si et dans quels cas il est permis d'écarter d'autres formes de secret professionnel. Il convient également de tenir compte du potentiel impact direct sur la vie privée des personnes, tel que visé à l'article 8 CEDH.

Reste à savoir si une méthode particulière de renseignement aurait dû être mise en œuvre. L'article 18/15 L.R&S stipule que les services de renseignement peuvent demander à une banque ou à un organisme financier la liste des comptes bancaires ou d'instruments financiers, les transactions financières qui ont été réalisées pendant une période déterminée, ou des données concernant les titulaires ou mandataires de coffres bancaires. Il est vrai que l'administratrice déléguée a remis les livres d'achats et de ventes de la société, dans lesquels figurent, en toute logique, des transactions financières et des comptes bancaires.

21 Obligation 'morale', obligation légale qui est punissable, 'devoir' d'un bon citoyen ….

Néanmoins, ce n'est pas ce qui est visé à l'article 18/15 L.R&S. Le fait que des données bancaires figuraient parmi les données communiquées par le cabinet comptable ne signifie pas que la VSSE aurait dû employer une méthode particulière de renseignement. Les données bancaires ne sont apparues que de manière accidentelle dans les données demandées, et la VSSE n'a en tout cas pas demandé une 'liste de comptes bancaires ou de transactions bancaires', ce que la société n'aurait d'ailleurs pas pu fournir.[22]

II.3. USAGE ABUSIF DE SA CARTE DE SERVICE PAR UN MEMBRE DE LA VSSE

En mai 2017, un membre de la Sûreté de l'État a déposé une plainte auprès du Comité permanent R contre un collègue. Ce dernier aurait abusé de son statut de membre du service de renseignement en présentant sa carte de service à un fournisseur d'hébergement, et ce, en vue d'obtenir des informations concernant le plaignant. Depuis un certain temps déjà, un conflit personnel opposait les deux protagonistes.

Au préalable, le plaignant avait pris contact avec la hiérarchie de la VSSE, qui avait alors ouvert une enquête interne. La hiérarchie de la VSSE avait également préconisé le dépôt d'une plainte, ce que le plaignant n'avait pas fait.

Le Comité permanent R a constaté que la personne visée par la plainte avait elle-même reconnu les faits dans un document faisant partie d'une procédure civile entre les deux intéressés.

Le Service d'Enquêtes estimait qu'il était donc effectivement préférable que la plainte soit traitée par les autorités judiciaires en raison du caractère

[22] En marge de ce cas, se pose la question de savoir si la 'nature' de l'instance à laquelle la VSSE demande une liste de données bancaires est déterminante pour établir si l'article 18/15 L.R&S s'applique ou non. En effet, la loi parle de 'banques et d'organismes financiers'. Le Comité permanent R a décidé, dans le cadre d'un cas qui s'était présenté, qu'il était question d'une méthode telle que visée à l'article 18/15 L.R&S lorsqu'il s'agissait d'une demande de données au Point de contact central (PCC) de la Banque nationale de Belgique. Le Comité a examiné 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. 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 (à savoir la méthode prévue à l'article 14 L.R&S). Mais le Comité n'était pas de cet avis. Si le Comité voyait dans l'initiative de la VSSE une implication dans la recherche active de canaux d'informations utiles, il a néanmoins attiré l'attention sur l'article 18/15 § 1er, 1° L.R&S. Cet article considère la demande de listes de comptes bancaires comme une méthode exceptionnelle. Et aucune réserve n'est émise sur l'instance qui fournit les informations. Dès lors, si la BNB ne devait pas être considérée comme une 'banque' ou comme 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 donc, si la VSSE souhaite obtenir des listes de comptes bancaires via le PCC, elle doit d'abord demander l'autorisation d'utiliser 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 adressée au PCC.

éventuellement punissable des faits (usage abusif de son statut officiel de fonctionnaire/de sa carte de service à des fins personnelles).

Le Comité permanent R a pris deux initiatives. D'une part, il a informé la VSSE de l'introduction de la plainte, dans laquelle il était signalé que des menaces avaient manifestement été proférées par la personne visée par la plainte. Le Comité a appris par la suite que la VSSE lui avait retiré son arme de service et qu'une procédure disciplinaire avait été lancée. D'autre part, en application de l'article 29 CIC, le Comité a informé le procureur du Roi. Celui-ci a demandé au Service d'Enquêtes R d'effectuer plusieurs devoirs d'enquête (art. 40 L.Contrôle).

Le Parquet a classé le dossier sans suite.

II.4. PLAINTE RELATIVE À UNE DÉCISION NÉGATIVE DANS LE CADRE D'UNE HABILITATION DE SÉCURITÉ

II.4.1. OBJET DE LA PLAINTE

En février 2017, une plainte a été introduite par déposition orale contre le SGRS.[23] La plainte portait sur la manière dont le service de renseignement militaire avait effectué une enquête de sécurité en vue d'octroyer au plaignant une habilitation de sécurité du niveau 'Secret', nécessaire pour l'exercice de ses fonctions à la Défense et à la Police fédérale.[24] Les griefs du plaignant étaient les suivants :

- l'absence de transparence dans la procédure d'octroi de l'habilitation de sécurité et le manque de professionnalisme dont auraient fait preuve les agents chargés du dossier ;
- un traitement discriminatoire à son égard ainsi qu'à l'égard de sa compagne ;
- une attitude jugée humiliante et vexatoire de la part des agents qui l'ont auditionné.

II.4.2. CONSTATATIONS

II.4.2.1. Sur l'absence de transparence dans la procédure d'octroi de l'habilitation de sécurité

La manière dont une enquête de sécurité est effectuée est réglée par la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&HS), et plus particulièrement par les articles 16 à 22.

---

23 La Commission de suivi a été informée le 14 décembre 2017 des résultats de la présente enquête relative à la plainte.

24 Pour l'octroi d'une habilitation de sécurité au sein de la Police fédérale, c'est l'Autorité nationale de sécurité (ANS) qui est l'autorité de sécurité, tandis qu'à la Défense, c'est le Chef du SGRS.

La personne qui doit obtenir une habilitation de sécurité est informée du niveau et de l'objet de l'habilitation, ainsi que des types de données qui pourront être examinées ou vérifiées lors de l'enquête de sécurité, des modalités de celle-ci et de la durée de validité de l'habilitation de sécurité (art. 16 L.C&HS). L'accord de l'intéressé est requis pour pouvoir procéder à l'enquête de sécurité. Ces informations figurent dans le formulaire prévu par l'Arrêté royal du 24 mars 2000. Il s'agit du document que le demandeur de l'habilitation de sécurité doit signer pour marquer son accord.[25, 26]

Pour le reste, la loi ne prévoit pas le respect d'un quelconque principe de transparence, invoqué par le plaignant, lors du déroulement des enquêtes de sécurité, ni d'ailleurs la nécessité d'un débat contradictoire avec le demandeur de l'habilitation avant la prise de décision par l'autorité de sécurité.[27]

Le plaignant avait été averti, comme l'exige la loi, et avait marqué son accord. Par conséquent, l'enquête de sécurité, pour cet aspect, s'est déroulée conformément aux prescrits de la L.C&HS. Le premier grief relatif à l'absence de transparence de la procédure n'était donc pas fondé.

II.4.2.2. Sur le manque de professionnalisme dont auraient fait preuve les agents chargés du dossier

L'examen du dossier a montré que les délais fixés par l'article 25 de l'Arrêté royal du 24 mars 2000 portant exécution de la L.C&HS n'avaient pas été respectés. Un délai anormalement long s'était écoulé entre la première demande d'habilitation de sécurité (en novembre 2012) et la première décision prise par le SGRS de refuser au plaignant l'octroi d'une habilitation de sécurité (mai 2016).

Plusieurs raisons expliquaient ce retard conséquent. Le Comité permanent R a constaté que le premier recours introduit par le plaignant devant de l'Organe de recours pour absence de décision concernant son habilitation de sécurité datait d'avril 2016, alors que sa première demande avait été déposée en novembre 2012. Par ailleurs, des retards et des dysfonctionnements ont effectivement été relevés tant dans la communication interne d'informations au sein du SGRS que dans l'échange de correspondance entre ce service et d'autres services. Le deuxième grief était dès lors partiellement fondé.

---

25 Le plaignant a signé un premier formulaire le 13 décembre 2012 et un second le 27 octobre 2015.

26 L'ampleur de l'enquête de sécurité est déterminée par le Conseil national de sécurité, et ce, pour chaque niveau d'habilitation. Seuls les agents des services de renseignement, l'Autorité nationale de sécurité et le Comité permanent R sont informés de la décision prise par le Conseil national de sécurité sur l'ampleur des enquêtes (art. 18 L.C&HS).

27 Néanmoins, en cas de recours devant l'Organe de recours, le requérant et son avocat peuvent consulter le dossier ou le rapport d'enquête (à l'exception de certaines informations qui doivent rester secrètes, en application de l'art. 5, § 3 de la Loi portant création d'un Organe de recours) au greffe de l'Organe de recours, ce que le plaignant a fait en octobre 2016 et en janvier 2017.

II.4.2.3. Sur le traitement discriminatoire à l'égard du plaignant ainsi qu'à l'égard de sa compagne

Le plaignant jugeait 'discriminatoire' que sa compagne, avec qui il ne cohabitait pas, ait dû se soumettre à une enquête de sécurité, et que lui-même ait dû subir plusieurs entretiens.

L'audition d'un(e) partenaire d'un(e) demandeur d'habilitation de sécurité n'est pas prévu dans la L.C&HS lorsque ces personnes ne vivent pas sous le même toit. Mais le législateur n'interdit pas aux services chargés de mener une enquête de sécurité et, s'ils l'estiment nécessaire, de recueillir des renseignements sur les fréquentations d'un demandeur d'une habilitation de sécurité.

Au vu du dossier de sécurité du plaignant, le Comité a estimé que les motifs de la demande d'audition de sa compagne étaient justifiés et ne traduisaient aucune intention discriminatoire, que ce soit à son égard et/ou de sa compagne. Le Comité a par ailleurs estimé que cette audition aurait sans doute permis au plaignant d'apporter les explications que le service souhaitait obtenir sur certains éléments de sa vie privée. Le refus de la partenaire du plaignant de se présenter à une audition ne pouvait toutefois, à lui seul, justifier la décision négative qui a été prise à l'égard du plaignant.

Le troisième grief n'était donc pas fondé.

II.4.2.4. Sur une attitude humiliante et vexatoire de la part des agents

Il ressortait clairement du rapport de l'audition incriminée que celle-ci avait débuté dans un climat tendu, mais on n'y trouvait aucune mention ou appréciation pouvant être considérée comme humiliante ou vexatoire à l'égard de quiconque.

De même, les rapports internes de l'enquête de sécurité concernant le plaignant et sa partenaire ne contiennent aucun commentaire qui tendrait à laisser supposer que sa demande d'habilitation de sécurité aurait été traitée avec partialité. Bien au contraire, chacun des renseignements recueillis par le SGRS paraissait, selon le Comité, avoir été examiné avec beaucoup de circonspection et évalué avec impartialité. Au final, c'était l'absence de renseignements sur certains aspects de la vie privée du plaignant qui avait entretenu la suspicion du SGRS et motivé la décision négative.

Le quatrième grief n'était pas fondé.

II.4.3. L'OCTROI D'UNE HABILITATION, MALGRÉ TOUT…

Après l'enquête de sécurité effectuée par la section 'Habilitations de sécurité' du SGRS, le Chef du SGRS a refusé, en mai 2016, l'octroi de l'habilitation de sécurité. Le plaignant a alors a introduit un recours devant l'Organe de recours en matière d'habilitations de sécurité, qui, en janvier 2017, a ordonné qu'une habilitation de sécurité du niveau 'Secret' lui soit octroyée.

II.5. LA POSITION D'INFORMATION DE L'OCAM AVANT LES ATTENTATS DE PARIS

Presque immédiatement après les attentats de Paris en novembre 2015, le Comité permanent R a ouvert une enquête de contrôle sur la position d'information des deux services de renseignement belges.[28] Le Comité permanent P a pour sa part initié une enquête de contrôle sur le fonctionnement des services de police. À la demande de la Commission parlementaire de suivi et en application de l'article 53, 6° L.Contrôle, les Comités permanents R et P ont décidé, fin janvier 2016, de réaliser une enquête commune sur *'la position d'information de l'OCAM sur les individus ou groupes ayant perpétré les attentats de Paris ou liés à ces attentats, avant le 13 novembre au soir'*. Il s'agissait de vérifier de quelles informations l'OCAM disposait en ce qui concerne les attentats terroristes, et d'examiner si, avant ces attentats, l'organe de coordination avait demandé et/ou reçu des informations des divers services d'appui et services partenaires étrangers.

L'enquête a été suspendue, étant donné qu'à la mi-2016, les Comités se sont vu confier d'autres missions d'enquête (plus prioritaires) par la Commission d'enquête parlementaire 'Attentats terroristes'. En outre, vu que le directeur de l'OCAM a par la suite été entendu à plusieurs reprises par la Commission d'enquête parlementaire, qui a *de facto* repris les questions de l'enquête, les Comités n'ont pas jugé pertinent de reprendre les devoirs d'enquête. Lors de leur réunion commune du 13 juin 2017, les deux Comités ont décidé de clôturer l'enquête de contrôle et de ne pas établir de rapport définitif. Le président de la Commission de suivi en a été informé le 15 juin 2017 et n'a émis aucune objection.

II.6. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ EFFECTUÉS EN 2017 ET QUI ONT DÉBUTÉ EN 2017

II.6.1. L'ÉCHANGE DE DONNÉES SUR LES *FOREIGN TERRORIST FIGHTERS* AU NIVEAU INTERNATIONAL

En 2016 déjà, à l'occasion d'une réunion internationale à laquelle participaient plusieurs organes de contrôle européens[29], il a été décidé d'initier, dans tous les

---

28 À ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2016*, 18-36 ('II.3. La position d'information des deux services de renseignement avant les attentats de Paris').

29 Le Comité permanent de contrôle des services de renseignement et de sécurité, la *Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten* (CTIVD) néerlandaise, la *Strategic Intelligence Service Supervision* suisse, ainsi que des délégations venues de Suède (*Commission on Security and Integrity Protection*), de Norvège (*Parliamentary Oversight Committee*) et du Danemark (*Intelligence Oversight Board*). Voir à ce propos COMITÉ PERMANENT R, *Rapport d'activités 2015*, 80-81.

pays participants, une enquête de contrôle similaire portant sur la coopération internationale entre les différents services de renseignement en matière de lutte contre les *foreign terrorist fighters* (FTF). 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 sur une approche commune.

Le volet belge de l'enquête[30] consiste à avoir la vision la plus précise et complète possible de l'échange d'informations bilatéral ou international, tant formel qu'informel, entre la VSSE et le SGRS, d'une part, et les services étrangers, les groupes de travail ou les structures de coopération, d'autre part, et ce, concernant la problématique des FTF.

La finalité ultime de l'enquête est d'évaluer l'échange d'informations et, le cas échéant, de formuler des recommandations pour l'optimaliser. L'objectif est d'améliorer la position d'information des services concernés, sans pour autant éroder les droits des citoyens.

En 2017, diverses missions d'enquête ont été effectuées par la VSSE et le SGRS, que ce soit au niveau national ou international. Les résultats de l'enquête de contrôle belge viendront enrichir l'enquête internationale, en tenant compte évidemment des restrictions en matière de classification. Une réunion d'expert a eu lieu dans ce cadre en mai 2017 à Oslo.

II.6.2. ENQUÊTE DE CONTRÔLE SUR LE FONCTIONNEMENT DE LA DIRECTION COUNTERINTELLIGENCE (CI) DU SGRS

En application de l'article 32 L.Contrôle, le ministre de la Défense a demandé au Comité permanent R, fin décembre 2016, d'effectuer une enquête sur le fonctionnement de la Direction Counterintelligence (CI) du SGRS. En effet, selon le ministre, *'een disfunctionele dienst roept vragen op die een onafhankelijk onderzoek noodzakelijk maakt'*.[31] C'est un courrier de la mi-décembre 2016, envoyé par une grande partie des cadres de CI, qui est à l'origine de cette déclaration. Le ministre était ainsi informé des préoccupations liées au fonctionnement du service et aux conditions dans lesquelles le personnel devait remplir ses missions légales.

Le Comité permanent R a ouvert son enquête de contrôle le 13 janvier 2017.[32]

---

30 L'enquête a démarré fin août 2016, après l'approbation par la Commission de suivi de la Chambre des Représentants de l'initiative qui lui avait été soumise.

31 Face à un service dysfonctionnel, se pose la question de la nécessité de mener une enquête indépendante (traduction libre).

32 En 2010, le Comité avait mené un audit similaire, avec l'appui de la Commission sénatoriale de suivi de l'époque. Cet 'audit de performance' avait permis de se faire une idée de la

L'enquête s'est déroulée de janvier 2017 à avril 2018. Un rapport intermédiaire a été envoyé en juillet 2017 au président de la Chambre et au ministre de la Défense. Ce premier rapport mettait l'accent sur la situation du personnel du service (y compris la problématique du statut), sur le manque d'infrastructures, l'ICT et les conditions matérielles, et, enfin, sur les procédures, l'organisation et la perte graduelle d'autonomie. Le rapport définitif a été finalisé en mai 2018.

Il est clair qu'au cours de son enquête de contrôle, le Comité permanent R a été confronté à une organisation en transition : le Plan Stratégique National du Renseignement était en pleine préparation, la structure était (de nouveau) redéfinie, du personnel supplémentaire était recruté, et les recommandations de la Commission d'enquête parlementaire sur les attentats terroristes devaient être mises en œuvre… Le Comité permanent R posait comme principe que la sécurité nationale nécessitait un service de renseignement militaire fort et fiable. C'est aussi la raison pour laquelle le Comité est convaincu de l'intérêt, pour la Direction CI, d'être organisée et gérée conformément aux standards d'un service efficace et efficient. Le rapport intermédiaire relevait que le service ne répondait pas à ces standards.

II.6.3. LA RÉALISATION DE VÉRIFICATIONS DE SÉCURITÉ PAR LES SERVICES DE RENSEIGNEMENT

Chaque année, la VSSE et le SGRS passent au crible quelques milliers de personnes qui veulent obtenir l'une ou l'autre licence ou autorisation, ou qui souhaitent exercer une fonction déterminée. Ce faisant, ils veulent vérifier si les intéressés offrent des garanties suffisantes en termes de fiabilité.

Le rôle des services de renseignement dans le cadre des enquêtes de fiabilité n'est pas toujours identique. Parfois, le rôle de ces services se limite à transmettre à d'autres autorités les données à caractère personnel dont ils disposent, tandis que dans d'autres circonstances, ils sont amenés à chercher activement des informations complémentaires. Il arrive aussi qu'ils rendent un avis motivé et, dans quelques cas spécifiques, qu'ils prennent également la décision finale (seuls ou comme section d'une autorité de sécurité) d'octroi ou de retrait de la licence ou de l'autorisation.

Dans le cas présent, une plainte était à l'origine de l'enquête de contrôle. Un collaborateur de l'aéroport de Bruxelles National s'était vu retirer son badge

---

situation au sein du service de renseignement militaire dans son ensemble. Il entendait initier une dynamique qui aurait donné lieu à un réel changement et, là où c'était nécessaire, à une réelle amélioration… COMITÉ PERMANENT R, *Rapport d'activités 2011*, 7-14 ('II.1. Un audit au sein du service de renseignement militaire'). Le Comité a formulé toute une série de recommandations (104-107, 'IX.2.1. Recommandations relatives à l'audit effectué au sein du SGRS').

d'accès suite à un avis négatif[33] de l'Autorité nationale de sécurité (ANS). Il avait introduit un recours devant l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité ainsi qu'un recours en suspension et en annulation devant le Conseil d'État. L'Organe de recours avait jugé la plainte irrecevable, car elle avait été introduite contre la décision du SPF Mobilité et Transports et non contre l'avis émis par l'ANS. Le plaignant s'était alors tourné vers le Comité permanent R, sans toutefois définir l'objet de sa plainte. Il déclarait ne pas comprendre les raisons de l'avis négatif, qui avait eu pour effet de le priver de son travail et, de surcroît, de voir sa licence de pilote suspendue.

Le Comité estimait légitime, en partant d'un cas individuel, d'ouvrir une enquête de contrôle plus large sur la manière dont les services de renseignement réalisent les vérifications de sécurité.[34] En raison d'autres priorités, les premiers devoirs d'enquête n'ont pu être effectués qu'en octobre 2017.

II.6.4. LES SERVICES D'APPUI DE L'OCAM

L'Organe de coordination pour l'analyse de la menace (OCAM) a été institué par la Loi du 10 juillet 2006 relative à l'analyse de la menace. Cet organe a été créé dans le but de donner aux autorités politiques, administratives et judiciaires la vision la plus précise possible de la menace terroriste ou extrémiste en et contre la Belgique, et de leur permettre de réagir de manière adéquate.[35] Le *core business* de l'OCAM consiste à réaliser des évaluations ponctuelles ou stratégiques. Cette tâche incombe à des analystes et à des experts détachés de ce que l'on appelle les 'services d'appui'. Ces services d'appui constituent la principale source d'informations pour l'organe de coordination. En 2017, il s'agissait de la VSSE, du SGRS, de la Police intégrée, de l'Administration des Douanes et Accises du SPF Finances, de l'Office des étrangers du SPF Intérieur, du SPF Mobilité et du SPF Affaires étrangères (art. 2, 2. L.OCAM). Ce sont des services très variés, de culture et de taille différentes.[36]

---

33 L'avis était motivé comme suit : *'overwegende dat betrokkene contacten met een radicale familiale omgeving heeft ; overwegende dat die contacten een mogelijk veiligheidsrisico met zich meebrengen'*. ('Attendu que l'intéressé est en contact avec un environnement familial radical ; attendu que ces contacts présenteraient un risque pour la sécurité' (traduction libre)).

34 'Enquête de contrôle sur la manière dont la VSSE et la SGRS procèdent aux vérifications de sécurité et à l'évaluation des données nécessaires à l'octroi des attestations de sécurité, en application des articles 22*bis* à 22*sexies* de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&HS)'. L'enquête a été ouverte le 13 février 2017.

35 W. VAN LAETHEM, 'Het coördinatieorgaan voor de dreigingsanalyse : een punctuele analyse', *Vigiles*, 2007, Afl. 4, 109-127. Voir également : Belgian Standing Committee I, *All Source threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, Antwerpen, Intersentia, 2010, 220 p.

36 Le législateur a autorisé l'ajout d'autres institutions à la liste des 'services d'appui'.

Précédemment, en 2010, le Comité permanent R avait effectué une enquête, conjointement avec le Comité permanent P, sur les flux d'informations entre l'OCAM et les services d'appui, en mettant l'accent sur les deux services de renseignement et sur les Polices fédérale et locale.[37]

Lors de la réunion plénière commune de décembre 2017, les Comités permanents R et P ont décidé d'ouvrir une enquête de contrôle sur les 'autres' services d'appui.[38] Les Comités souhaitent ainsi établir un *status quaestionis* du flux d'informations entre l'OCAM et les autres services d'appui, et ce, en menant toute une série d'auditions.

[37] Voir à ce propos COMITÉ PERMANENT R, *Rapport d'activités 2010*, 45-46 ('II.12.6. Communication de renseignements à l'OCAM par les services d'appui') et, plus en détail, *Rapport d'activités 2011*, 25-33 ('II.4. Les flux d'informations entre l'OCAM et ses services d'appui').

[38] Enquête de contrôle sur les services d'appui de l'OCAM autres que la police intégrée et les services de renseignement.

CHAPITRE III
LE CONTRÔLE DES MÉTHODES PARTICULIÈRES ET DE CERTAINES MÉTHODES ORDINAIRES DE RENSEIGNEMENT

Ce chapitre offre un aperçu de l'utilisation, en 2017, des méthodes particulières de renseignement par la VSSE et le SGRS et de la manière dont le Comité permanent R a rempli sa mission de contrôle juridictionnel. Il est basé sur le rapport qui a été établi par le Comité permanent R en exécution de l'article 35 § 2 L.Contrôle du 18 juillet 1991.

Ce rapport reprend les chiffres détaillés de l'utilisation des méthodes particulières et de certaines méthodes ordinaires par la Sûreté de l'État (VSSE) et par le Service Général du Renseignement et de la Sécurité (SGRS), ainsi que les chiffres relatifs à la manière dont le Comité permanent R a assuré sa mission juridictionnelle de contrôle sur les méthodes particulières.

Il convient toutefois de mentionner en premier lieu la modification de loi importante qui est entrée en vigueur en 2017 (plus précisément le 8 mai 2017) concernant les missions et les compétences des services de renseignement en général, et la mise en œuvre des méthodes spécifiques et exceptionnelles, en particulier. La Loi du 30 mars 2017 (*M.B.* 28 avril 2017) a modifié en profondeur la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité, y compris en ce qui concerne les méthodes particulières de renseignement. Globalement, on peut affirmer que la VSSE et le SGRS se sont vu octroyer davantage de compétences. Il est impossible de détailler chaque modification dans le cadre de ce rapport d'activités. Il n'empêche que certains aspects seront développés, dans la mesure où la modification de loi a impacté les méthodes particulières de renseignement (ou leur mise en œuvre).

Chapitre III

III.1. LES CHIFFRES RELATIFS AUX MÉTHODES PARTICULIÈRES ET À CERTAINES MÉTHODES ORDINAIRES

Entre le 1er janvier et le 31 décembre 2017, 1923 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 1822 pour la VSSE (1612 spécifiques et 210 exceptionnelles) et 101 pour le SGRS (79 spécifiques et 22 exceptionnelles).

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

	SGRS		VSSE		TOTAL
	Méthodes spécifiques	**Méthodes exceptionnelles**	**Méthodes spécifiques**	**Méthodes exceptionnelles**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923

Ces tableaux montrent que le nombre de méthodes mises en œuvre par le SGRS demeure faible et dessine une courbe rentrante, alors que l'augmentation se poursuit à la VSSE. Les mêmes tendances sont constatées pour les méthodes ordinaires de réquisitions auprès d'opérateurs en vue d'identifier certains moyens de communication. La VSSE a émis pas moins de 4327 réquisitions, contre 257 pour le SGRS.[39]

	Réquisitions par le SGRS	**Réquisitions par la VSSE**
2016	216	2203
2017	257	4327

Dans ce qui suit, quatre rubriques sont établies pour chaque service : des données chiffrées sur certaines méthodes ordinaires, des données chiffrées sur les méthodes spécifiques, des données chiffrées sur les méthodes exceptionnelles et des données chiffrées sur les menaces et les intérêts à protéger qui sont visés par les différentes méthodes (les chiffres relatifs aux menaces et aux intérêts à

[39] Aucune donnée bancaire n'a été requise dans le cadre de la problématique des cartes prépayées (voir également ci-après le point III.1.1.1).

protéger dans le cadre de l'utilisation des méthodes ordinaires ne sont pas encore disponibles).

III.1.1. LES MÉTHODES RELATIVES AU SGRS

III.1.1.1. Les méthodes ordinaires

Par la Loi du 5 février 2016 modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice (*M.B.* 19 février 2016), l'identification de l'utilisateur de télécommunications (p. ex. d'un numéro de GSM ou d'une adresse IP) ou d'un moyen de communication utilisé est considérée – sur recommandation du Comité permanent R[40] – comme une méthode ordinaire, dans la mesure où elle a lieu via une réquisition ou un accès direct aux fichiers des clients d'un opérateur. Auparavant, il s'agissait d'une méthode spécifique. La modification a été opérée en insérant un nouvel article 16/2 à la Loi du 30 novembre 1998.

Lorsque l'identification a lieu à l'aide d'un moyen technique (et donc pas via une réquisition à un opérateur), la collecte reste une méthode spécifique. L'article 18/7 § 1er L.R&S a été adapté en ce sens.

La réglementation prévoit une obligation pour la VSSE et le SGRS de tenir un registre de toutes les identifications requises et de toutes les identifications obtenues par accès direct. Le Comité permanent R reçoit chaque mois une liste des identifications requises et de chaque accès.[41] Conformément à l'article 35 § 2, alinéa 1er, de la Loi Contrôle du 18 juillet 1991, le Comité fait rapport à la Chambre dans son rapport annuel.

En outre, par la Loi du 1er septembre 2016 (*M.B.* 7 décembre 2016), une nouvelle méthode ordinaire a été introduite à l'article 16/2 L.R&S : '*§ 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée visée dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.*' Comme dans le cadre de l'identification de l'utilisateur de télécommunications ou d'un moyen de communication utilisé, la VSSE et le SGRS doivent tenir un registre de toutes

40 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 71.

41 Dans la pratique, le Comité reçoit un courrier mensuel reprenant le nombre de réquisitions. Le Comité n'y voit pas d'inconvénient, mais précise qu'il vérifiera, d'une part, la manière dont les services de renseignement auront contrôlé en interne l'utilisation de ces méthodes et, d'autre part, un échantillon annuel de plusieurs réquisitions. Les services doivent donc à tout moment pouvoir mettre à disposition les données qu'ils avaient requises et qu'ils ont reçues.

les identifications requises. Conformément à l'article 35 § 2, alinéa 1er de la Loi Contrôle du 18 juillet 1991, le Comité doit également faire rapport à la Chambre dans son rapport annuel.[42]

Le tableau repris ci-dessous offre un aperçu (1) du nombre de réquisitions adressées à des opérateurs (en 2017, il n'y a eu aucun accès direct (3) ni réquisition adressée à des institutions bancaires (4)) et (2) du nombre de numéros sur lesquels portaient ces réquisitions (des dizaines de numéros peuvent figurer dans une seule réquisition).

	Identification des télécommunications			**Identification des télécommunications par accès direct (3)**	**Identification des cartes prépayées (4)**
	Nombre de méthodes	**Nombre de réquisitions (1)**	**Nombre de numéros (2)**		
2013	66	non connu	non connu	pas d'application	pas d'application
2014	67	non connu	non connu	pas d'application	pas d'application
2015	55	non connu	non connu	pas d'application	pas d'application
2016	non connu	216	non connu	0	pas d'application
2017	non connu	257	1058	0	0

III.1.1.2. Les méthodes spécifiques

Le tableau ci-dessous reprend les chiffres relatifs à l'application des méthodes spécifiques par le SGRS. Les différentes rubriques sont tout d'abord expliquées.
On distingue sept méthodes spécifiques. La modification de loi intervenue entretemps a modifié (lisez : étendu) la portée de chaque méthode, et ce, à compter du 8 mai 2017. Toutefois, pour éviter toute complication inutile, les chiffres portant sur la période antérieure et postérieure à la modification de loi n'ont pas été dissociés.

A. Avant le 8 mai 2017 – Pénétrer et observer dans des lieux qui sont accessibles au public avec un moyen technique (art. 18/2 § 1er, 1° et 18/4 L.R&S) ;
   Après le 8 mai 2017 – Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans

42 La Loi 25 décembre 2016 (*M.B.* 25 janvier 2017) a donné la possibilité à la VSSE et au SGRS d'avoir accès à des informations provenant de l'Unité d'information des passagers (art. 16/3 L.R&S). Le Comité est informé de cette méthode et peut l'interdire le cas échéant. Contrairement aux méthodes reprises à l'article 16/2 L.R&S, il n'a pas été prévu qu'un rapport doive être transmis au Parlement ; l'article 35 § 2 L.Contrôle n'a en effet pas été adapté. Le Comité permanent R recommande de le faire, d'autant qu'il faut établir un rapport sur la demande de données de transport et de voyage sur base de l'article 18/6/1 L.R&S, puisqu'il s'agit d'une méthode spécifique. Le Comité estime d'ailleurs qu'un tel rapport est tout aussi indiqué pour la possibilité introduite par la Loi du 21 mars 2018 (*M.B.* 16 avril 2018) d'utiliser des images enregistrées par des caméras et reprises dans des fichiers (art. 16/4 L.R&S).

un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S) ;

B. Avant le 8 mai 2017 – Pénétrer et inspecter des lieux accessibles au public avec un moyen technique (art. 18/2 § 1er, 2° et 18/5 L.R&S) ;
   Après le 8 mai 2017 – Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S) ;
C. Avant le 8 mai 2017 – Prendre connaissance de données d'identification du trafic postal et requérir le concours d'un opérateur postal (art. 18/2 § 1er, 3° et 18/6 L.R&S) ;
   Après le 8 mai 2017 – Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S) ;
D. Avant le 8 mai 2017 – Rien n'était prévu ;
   Après le 8 mai – Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S) ;
E. Toute l'année 2017 – Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée, et requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 L.R&S) ;
F. Toute l'année 2017 – Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S) ;
G. Toute l'année 2017 – Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S).

Méthodes spécifiques (SGRS)	**Nombre d'autorisations**
Observation	7
Inspection	0
Identification du trafic postal	0
Données de transport et de voyage	0
Identification d'un abonné ou du moyen de communication ou de paiement	4
Identification de données d'appel	36
Prise de connaissance de données de localisation	32
TOTAL	**79**

En ce qui concerne la mise en œuvre de méthodes spécifiques par le SGRS, aucune tendance marquante n'est à signaler.

III.1.1.3. Les méthodes exceptionnelles

Les méthodes exceptionnelles ont elles aussi été modifiées à plusieurs égards par la Loi du 30 mars 2017. Ces modifications sont précisées ci-après.

A. Avant le 8 mai 2017 – Observer, à l'aide ou non de moyens techniques, dans des lieux privés qui ne sont pas accessibles au public, dans des domiciles ou une dépendance propre y enclose d'un domicile au sens des articles 479, 480 et 481 du Code pénal, ou dans un local utilisé à des fins professionnelles ou comme résidence par un avocat, un médecin ou un journaliste et pénétrer dans ces lieux, dans le cadre d'une observation, afin d'installer un moyen technique, de le réparer ou de le retirer (art. 18/2 § 2, 1° en 18/11 L.R&S) ;
   Après le 8 mai 2017 – Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S) ;
B. Avant le 8 mai 2017 – Inspecter ces lieux à l'aide ou non de moyens techniques (art. 18/2 § 2, 2° en 18/12 L.R&S) ;
   Après le 8 mai 2017 – Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S) ;
C. Avant le 8 mai 2017 – Créer ou recourir à une personne morale à l'appui d'activités opérationnelles et recourir à des agents du service, sous le couvert d'une identité ou d'une qualité fictive (art. 18/2 § 2, 3° en 18/13 L.R&S) ;
   Après le 8 mai 2017 – Recourir à une personne morale visée à l'article 13/3, § 1er L.R&S afin de collecter des données (art. 18/13 L.R&S) ;
D. Toute l'année 2017 – Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S) ;
E. Toute l'année 2017 – Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S) ;
F. Toute l'année 2017 – S'introduire dans un système informatique (article 18/16 L.R&S) ;
G. Toute l'année 2017 – Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S).

Méthodes exceptionnelles (SGRS)	Nombre d'autorisations
Observation	7
Inspection	10
Personne morale fictive	0
Ouverture de courrier	0
Recueil de données bancaires	2
Intrusion dans des systèmes informatiques	1
Écoute de communications	1
TOTAL	**22**

III.1.1.4. Les missions et les menaces justifiant le recours aux méthodes particulières[43]

Depuis l'entrée en vigueur de la Loi du 29 janvier 2016 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique, le SGRS est autorisé à utiliser des méthodes spécifiques et exceptionnelles dans le cadre de quatre missions. Cela signifie que ces méthodes ne peuvent être utilisées dans le cadre d'enquêtes de sécurité ou d'autres missions assignées au SGRS par des lois particulières (p. ex. effectuer des vérifications de sécurité pour des candidats-militaires). Néanmoins, la Loi du 30 mars 2017 a apporté des modifications à ces quatre missions. Ces missions peuvent désormais être résumées comme suit :

1. **La mission de renseignement (art. 11, 1° L.R&S)**
   Le recueil, l'analyse et le traitement du renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir.
   Le recueil, l'analyse et le traitement du renseignement relatif à toute activité qui menace ou pourrait menacer les intérêts suivants :
   - l'intégrité du territoire national ou la survie de tout ou partie de la population ;
   - les plans de défense militaires ;
   - le potentiel économique et scientifique en rapport avec la défense ;
   - l'accomplissement des missions des Forces armées ;
   - la sécurité des ressortissants belges à l'étranger.

[43] Plusieurs intérêts et menaces peuvent figurer dans une même autorisation.

2. **Le maintien de la sécurité militaire (art. 11, 2° L.R&S)**
   - la sécurité militaire du personnel relevant du ministre de la Défense nationale ;
   - les installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires ;
   - dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense nationale gère, neutraliser l'attaque et en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés.
3. **La protection de secrets (art. 11, 3° L.R&S)**
   La protection du secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que gère le ministre de la Défense nationale.
4. **La recherche, l'analyse et le traitement du renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge (art. 11, 5°, L.R&S).**

Depuis l'entrée en vigueur de la Loi du 30 mars 2017, la mise en œuvre des méthodes particulières de renseignement ne se limite plus au territoire belge (art. 18/1, 2° L.R&S).

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

NATURE DE LA MISSION	NOMBRE EN 2017
1. Mission de renseignement	48
2. Sécurité militaire	2
3. Protection de secrets	5
4. Suivi des activités des services étrangers en Belgique	46

NATURE DE LA MENACE	NOMBRE EN 2017
1. Espionnage	77
2. Terrorisme (et processus de radicalisation)	16
3. Extrémisme	4
4. Ingérence	4
5. Organisations criminelles	0
6. Autre	0

Cette année de référence est la première pour laquelle des chiffres sont disponibles en ce qui concerne le suivi des activités des services de renseignement

étrangers en Belgique. Le chiffre est d'emblée très élevé. On ne peut cependant pas en déduire qu'en 2017, le SGRS a suivi un nouveau genre de menace. En effet, le suivi de services étrangers était auparavant plus vite associé à la 'mission de renseignement' dans le cadre de la lutte contre 'l'espionnage'.

III.1.2. LES MÉTHODES RELATIVES À LA VSSE

III.1.2.1. Les méthodes ordinaires

Le tableau repris ci-dessous offre un aperçu (1) du nombre de réquisitions adressées à des opérateurs (en 2017, il n'y a eu aucun accès direct (3) ni réquisition adressée à des institutions bancaires (4)) et (2) du nombre de numéros sur lesquels portaient ces réquisitions (des dizaines de numéros peuvent figurer dans une seule réquisition).

	Identification des télécommunications			**Identification des télécommunications par accès direct (3)**	**Identification des cartes prépayées (4)**
	Nombre de méthodes	**Nombre de réquisitions (1)**	**Nombre de numéros (2)**		
2013	66	non connu	non connu	pas d'application	pas d'application
2014	67	non connu	non connu	pas d'application	pas d'application
2015	55	non connu	non connu	pas d'application	pas d'application
2016	non connu	2203	non connu	0	pas d'application
2017	non connu	4327	21566	0	0

Indépendamment du fait qu'il est pratiquement impossible de comparer les chiffres en matière d'identifications sur base annuelle, le Comité ne peut nier qu'un nombre beaucoup plus élevé d'identifications ont été effectuées depuis l'introduction de la procédure assouplie visée à l'article 16/2 L.R&S. S'appuyant sur sa compétence générale de contrôle, le Comité demandera à la VSSE d'examiner en interne dans quelle mesure ce nombre élevé de réquisitions tient (en partie) à l'assouplissement de la procédure. Il convient à cet égard d'être attentif à la nature des menaces qui justifient les réquisitions et à la question de savoir si et dans quelle mesure de telles réquisitions ont lieu à la demande d'autorités étrangères ou de services partenaires étrangers.

III.1.2.2. Les méthodes spécifiques

Méthodes spécifiques (VSSE)	**Nombre d'autorisations**
Observation	121
Inspection	0
Identification du trafic postal	0
Données de transport et de voyage	54
Identification d'un abonné ou du moyen de communication ou de paiement	49
Identification de données d'appel	708
Prise de connaissance de données de localisation	680
TOTAL	**1612**

S'il n'est pas évident de comparer les chiffres repris ci-dessus avec les années précédentes en raison de modification de loi intervenue entre-temps, on peut néanmoins affirmer que l'augmentation du nombre de méthodes spécifiques s'explique essentiellement par une forte augmentation du nombre de 'localisations' (680 contre 596 l'année précédente).

III.1.2.3. Les méthodes exceptionnelles

Méthodes exceptionnelles (SGRS)	**Nombre d'autorisations**
Observation	9
Inspection	22
Personne morale fictive	0
Ouverture de courrier	15
Recueil de données bancaires	10
Intrusion dans des systèmes informatiques	35
Écoute de communications	119
TOTAL	**210**

Les nombreux attentats qui ont été perpétrés en Belgique et à l'étranger avaient complètement inversé la tendance en 2016. Cette année-là, une forte hausse du nombre de méthodes exceptionnelles avait été constatée, contrairement à 2015, qui avait été marquée par une baisse. Cette tendance à la hausse s'est poursuivie en 2017. À noter toutefois une stagnation du nombre de mesures d'écoutes.

III.1.2.4. 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 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). Depuis le 8 mai 2017, les méthodes exceptionnelles peuvent également être mises en œuvre dans le cadre de l'extrémisme et de l'ingérence, ce qui n'était pas autorité auparavant. 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 infractions, 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.

Depuis l'entrée en vigueur de la Loi du 30 mars 2017, les méthodes particulières de renseignement peuvent également être mises en œuvre '*à partir du territoire du Royaume*', et donc plus uniquement '*sur*' le territoire (art. 18/1, 1° L.R&S).

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

NATURE DE LA MENACE	NOMBRE EN 2017
1. Espionnage	308
2.Terrorisme (et processus de radicalisation)	678
3. Extrémisme	63
4. Prolifération	4
5. Organisations sectaires nuisibles	0
6. Ingérence	9
7. Organisations criminelles	0
8. Suivi des activités des services étrangers en Belgique[44]	308

Les chiffres repris ci-dessus montrent que le 'terrorisme', pour ce qui est de la mise en œuvre de MRD, est la priorité absolue de la VSSE.

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 :

1. 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.
2. 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.
3. La sauvegarde des éléments essentiels du potentiel économique et scientifique.

44 Ce n'est que par la Loi du 29 janvier 2016 que cette mission a été insérée.

INTÉRÊTS PROTÉGÉS	NOMBRE EN 2017
La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel	1053
La sûreté extérieure de l'État et les relations internationales	1024
La sauvegarde des éléments essentiels du potentiel économique et scientifique	17

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. L'attention se focalise ici sur les décisions juridictionnelles prises en la matière, mais pas sur les données opérationnelles. 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. Par ailleurs, un membre du Service d'Enquêtes participe, depuis 2017, à une réunion de quinzaine, au cours de laquelle la VSSE informe la Commission BIM sur l'exécution des méthodes exceptionnelles. Un rapport en est fait à l'intention du Comité, ce qui lui permet d'avoir une meilleure vue sur ces méthodes.[45]

L'article 43/4 L.R&S stipule que le Comité permanent R peut être saisi de cinq manières :

1. D'initiative ;
2. À la demande de la Commission de la protection de la vie privée ;
3. Par le dépôt d'une plainte d'un citoyen ;
4. 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 ;
5. De plein droit, quand le ministre compétent a donné son autorisation sur base de l'article 18/10, § 3 L.R&S.

[45] Le Comité a également recommandé au SGRS d'organiser de telles réunions. Il s'agit en effet d'une obligation légale (art. 18/10 § 1er, alinéa 3 L.R&S et art. 9, AR 12 octobre 2010).

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 cas échéant, le Comité rend 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	2013	2014	2015	2016	2017
1. D'initiative	16	12	16	3	1
2. Commission Vie Privée	0	0	0	0	0
3. Plainte	0	0	0	1	0
4. Suspension par la Commission BIM	5	5	11	19	15
5. Autorisation du ministre	2	1	0	0	0
6. Auteur d'avis préjudiciel	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**

Le nombre de décisions prises par le Comité a diminué en 2017, nonobstant l'augmentation du nombre de méthodes et l'entrée en vigueur, à la mi-2017, d'une nouvelle modification de loi complexe. En outre, toutes les saisines, à une exception près, résultent d'une suspension décidée par la Commission BIM.

Une fois saisi, le Comité peut prendre plusieurs types de décisions et de décisions intermédiaires. Les décisions intermédiaires sont mentionnées aux points 3. à 10., tandis que les décisions finales sont reprises aux points 11 à 16. Dans trois cas, (voir 1, 2 et – parfois – 6), 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. 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 à 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 est fait référence à la fois aux multiples informations complémentaires recueillies de manière plutôt informelle par le

Service d'Enquêtes R avant la saisine proprement dite et aux informations recueillies par le Comité après la saisine ;
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 à une 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) ;
10. Pour le Président du Comité permanent R, statuer, après avoir entendu le dirigeant du service, si le membre du service de renseignement 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). Ceci implique que la méthode autorisée par le dirigeant du service soit (partiellement) considérée comme légale, proportionnelle et subsidiaire par le Comité ;
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' (art. 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	2014	2015	2016	2017
Décisions préalables à la saisine					
1. Plainte frappée de nullité	0	0	0	0	0
2. Plainte manifestement non fondée	0	0	0	0	0
Décisions intermédiaires					
3. Suspension de la méthode	0	3	2	1	0
4. Informations complémentaires de la Commission BIM	0	0	0	0	0

NATURE DE LA DÉCISION	2013	2014	2015	2016	2017
5. Information complémentaire du service de renseignement	0	1	1	4	0
6. Mission d'enquête confiée au Service d'Enquêtes R	50	54	48	60	35
7. Audition de membres de la Commission BIM	0	0	2	0	0
8.Audition de membres des services de renseignement	0	0	2	0	0
9. Décision relative au secret de l'instruction	0	0	0	0	0
10. Informations sensibles lors de l'audition	0	0	0	0	0
Décisions finales					
11. Cessation de la méthode	9	3	3	6	9
12. Cessation partielle de la méthode	5	10	13	4	6
13. Levée (partielle) de l'interdiction de la Commission BIM	2	0	4	11	0
14. Incompétence	0	0	0	0	0
15. Autorisation légale/Non- cessation de la méthode/Non-fondement	7	4	6	2	1
Avis préjudiciels					
16. Avis préjudiciel	0	0	0	0	0

III.2.2. LA JURISPRUDENCE

La substance des décisions finales prises par le Comité permanent R en 2017 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, puisque certaines décisions du Comité ont été classifiées.

Les décisions ont été regroupées en trois rubriques :

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

III.2.2.1. Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode : décision préalable du dirigeant du service et notification à la Commission BIM

Une méthode spécifique ne peut être effectivement mise en œuvre qu'après la notification, à la Commission BIM, de l'autorisation du dirigeant du service (art. 18/3 § 1er, alinéa 2, L.R&S). Dans le dossier 2017/5650, des doutes ont surgi à ce propos. La Commission BIM avait remarqué qu'une observation avec une caméra par le biais d'une méthode spécifique avait été prolongée par le dirigeant du service, mais que plusieurs jours s'étaient écoulés entre la fin de la première période et le début de la seconde. Par conséquent, la Commission BIM a suspendu la méthode pour ce qui concerne la courte période entre les deux autorisations valables. Le Comité a lui aussi estimé que le service concerné ne pouvait exclure que des données aient été recueillies pendant ces quelques jours. Le Comité en a dès lors conclu '*que la mise en œuvre éventuelle de la méthode spécifique ne résulte en effet pas d'une décision [du chef de service] avec information concomitante à la Commission BIM ; que dans cette mesure ces données éventuellement recueillies sont illégales et que la procédure légale prévue par la Loi R&S trouve à s'appliquer même si [le service] envisage la destruction des données éventuellement recueillies.*'

Dans un autre cas, la Commission BIM avait constaté qu'un service de renseignement avait observé un domicile pendant plusieurs jours à l'aide d'un moyen technique (art. 18/4 L.R&S) sans l'autorisation requise (dossier 2017/5807). Les périodes antérieure et postérieure étaient quant à elles couvertes par une autorisation valable. Selon toute vraisemblance, il s'agissait d'une simple omission. Le Comité a cependant estimé '*ontegensprekelijk vaststaat dat de vigerende wettelijke bepalingen voor het uitvoeren van een BIM niet werden nageleefd. Dat de verklaringen van de [dienst] – stellende dat de methode, bestaand uit het observeren van een woning, goede resultaten oplevert – hieraan geen afbreuk doen. Dat de zwaarwichtigheid van het dossier deze onwettige situatie evenmin kan rechtzetten.*'[46] Le Comité a donc ordonné la destruction des données recueillies illégalement.

Le Comité a dû prendre des décisions identiques dans les dossiers 2017/5832 et 2017/5843. Il y était question de la même problématique, c'est-à-dire une prolongation non couverte : le service avait omis d'octroyer une autorisation pour une période de respectivement trois et six jours entre deux autorisations valables. Le Comité a ici aussi estimé que '*de zwaarwichtigheid van het dossier de aangehaalde onwettige situatie niet kan rechtzetten.*'[47]

---

46 '*que le non-respect des dispositions légales en vigueur pour l'exécution d'une MRD ne prête pas à discussion. Que les déclarations du [service] – selon laquelle la méthode, consistant à observer un domicile, a donné de bons résultats – n'y change rien. Que de la gravité du dossier ne peut pas non plus justifier l'illégalité de cette situation*' (traduction libre).

47 *Que de la gravité du dossier ne peut justifier de caractère illégal de la situation mentionnée*' (traduction libre).

Lorsque la Commission BIM a appris du dirigeant d'un service de renseignement qu'une observation avait été menée un mois durant sans autorisation légale, elle a ordonné '*d'interdire l'exploitation des données ainsi récoltées*' (dossier 2017/5900). Le Comité n'a pu que confirmer cette décision.

Par ailleurs, dans le dossier 2017/5998, le service a lui-même fait remarquer qu'une méthode spécifique avait continué à être mise en œuvre après l'expiration du délai mentionné dans l'autorisation. Le service en a informé la Commission BIM, qui a interdit l'exploitation des données recueillies. Le Comité, qui était saisi d'office, a confirmé la décision de la Commission, vu que '*des données ont été récoltées au-delà de la période prévue par la décision du chef de service ; que ces données n'ont pas été récoltées conformément à la loi à défaut d'autorisation du chef de service.*'

III.2.2.2. La légalité de la méthode concernant les techniques utilisées, les données recueillies, la durée de la mesure et la nature de la menace

III.2.2.2.1. La demande de données de téléphonie

Dans trois cas identiques, un service de renseignement souhaitait procéder à une prise de connaissance de données d'appel et de localisation d'un GSM bien déterminé (dossiers 2017/5573, 2017/5574 et 2017/5575). Il est ressorti des données complémentaires qui avaient été demandées par la Commission BIM que le service avait obtenu ce numéro en recourant à une méthode ordinaire (art. 16/2 L.R&S), alors que la réquisition adressée à l'opérateur ne portait pas sur la simple identification d'un numéro, mais '*sur l'identification réalisée au moyen d'une opération technique, telle que la consultation des informations passées par un mat*'. La méthode utilisée nécessitait la mise en œuvre d'une méthode spécifique (art. 18/8 § 1er, 1° et 2° L.R&S) (voir également à ce propos le point III.2.3).

Le 3 avril 2017, un service de renseignement a décidé, dans deux dossiers liés (2017/5776 et 2017/5777) et sur base de l'art. 18/8 L.R&S, d'obtenir des informations sur des données d'appel d'un numéro de téléphone, et ce, pour les neuf mois écoulés. La loi le permet, vu la menace concernée, pour un maximum de '*negen maanden voorafgaand aan de beslissing.*'[48] Il est cependant apparu que le service souhaitait obtenir des informations à compter du 1er juillet 2016. Le Comité a toutefois estimé '*[d]at de uiterste datum om negen maanden terug te gaan in de tijd – rekening houdend met het moment van beslissing, zijnde 3 april 2017 – 2 juli 2016 is en niet 1 juli 2016*'.[49] La récolte de données téléphoniques n'était donc pas couverte par une méthode légale le 1er juillet 2016.

---

48 '*neuf mois précédant la décision*' (traduction libre).

49 '*que la date limite à laquelle on peut remonter – compte tenu du moment de la décision, c'est-à-dire le 3 avril 2017 – est le 2 juillet 2016 et non le 1er juillet 2016*' (traduction libre).

Le dossier 2017/5916 était identique à cet égard. Le service voulait procéder à une prise de connaissance de données d'appel et de localisation (art. 18/8 § 1er L.R&S), pour une période allant du 19 mai 2016 au 16 mai 2017. Toutefois, en exécution de l'art. 18/8 § 2 L.R&S, '*la récolte de telles données ne peut excéder une période de 12 mois précédant le jour de la décision*'. Étant donné que cette décision a été prise le 23 mai 2017, '*la période maximale de récolte rétroactive de données ne peut donc s'étendre que du 22 mai 2016 au 22 mai 2017*.' Par conséquent, la décision du dirigeant du service a été annulée pour ce qui concerne le recueil de données allant du 19 au 21 mai 2016 inclus.

Cette jurisprudence s'est encore représentée dans deux dossiers distincts.

L'article 18/8, § 2 L.R&S stipule que '*pour une menace potentielle qui se rapporte à une activité qui peut être liée au terrorisme ou à l'extrémisme, le dirigeant du service peut dans sa décision requérir les données [de téléphonie] pour une période de douze mois préalable à la décision*.' Dans le cas présent, la décision datait du 27 décembre 2017. Il en résulte que la méthode peut porter sur la période allant du 26 décembre 2016 au 26 décembre 2017. Le service avait toutefois demandé des données à partir du 20 décembre 2016 jusqu'au 20 décembre 2017. Aussi, le Comité a conclu que '*deze methode […] wettelijk gezien 6 dagen te vroeg start, nu pas vanaf 26 december 2016 de methode mocht worden geactiveerd*'[50] (dossier 2017/6611).

Dans le dossier 2017/6612, la menace était l''espionnage', si bien que les données de téléphonie ne pouvaient être requises que '*voor een periode van 9 maanden voorafgaand aan de beslissing*'[51] (art. 18/8 § 2, 2° L.R&S). La décision du dirigeant du service ne respectait pas cette limite et était donc partiellement frappée d'illégalité.

Lorsque la Commission BIM a demandé au service concerné quelle réquisition avait été envoyée aux opérateurs de télécommunications en exécution d'une autorisation parfaitement légale pour prendre connaissance de données d'appel, elle a constaté que des données de localisation avaient aussi été demandées (dossier 2017/5994). Vu que cette demande ne figure pas dans l'autorisation, le Comité a décidé que '*les données de localisation éventuellement obtenues de l'opérateur l'ont été illégalement*.'

III.2.2.2.2. La demande de données de voyage

Un service de renseignement souhaitait se renseigner sur les voyages en avion d'un target. Celui-ci était en contact avec une personne qui aurait constitué une cellule terroriste à l'étranger (dossier 2017/6208). La méthode portait sur une période de plus de deux ans et demi. Le Comité a constaté que '*la méthode est*

50 '*du point de vue légal, cette méthode a été mise en œuvre 6 jours trop tôt. La méthode ne pouvait en effet être activée qu'à partir du 26 décembre 2016*' (traduction libre).

51 '*pour une période de 9 mois préalable à la décision*' (traduction libre).

prévue par l'article 18/6/1 de la L.R&S qui ne fixe pas de limite de temps.' Le Comité a cependant remarqué que le législateur avait bien fixé des limites de temps dans le cadre de la méthode visée à l'article 18/8 L.R&S. Ainsi, la possibilité de demander des données de téléphonie a été limitée à six, neuf ou douze mois précédant la décision du dirigeant du service, et ce, en fonction de la nature de la menace. Le Comité a néanmoins ajouté '*que ce serait ajouter une condition non prévue par l'article 18/6/1 que de limiter dans le temps les demandes de données de voyage par référence à l'article 18/8.*' Mais cela ne signifie pas qu'une telle méthode peut être mise en œuvre pour une période illimitée : '*toutes les méthodes de recueil de données, qu'elles soient spécifiques ou exceptionnelles, doivent respecter les principes de subsidiarité et de proportionnalité ; que le Comité permanent R a déjà fait application de ce principe pour limiter dans le temps une observation spécifique visée à l'article 18/4 (cf rapport d'activité 2010 page 68) […] ; Attendu que, dans le cas d'espèce, la nature et la gravité de la menace décrites dans la décision […] sont telles qu'une réquisition de données de transport pour une période de 32 mois […] n'enfreint pas le principe de proportionnalité.*'

III.2.2.3. Les conséquences d'une méthode (mise en œuvre) illégale(ment)

Un service de renseignement souhaitait procéder à la prise de connaissance de données d'appel et de localisation d'un GSM déterminé (dossiers 2017/5573, 2017/5574 et 2017/5575). Il est ressorti des données reçues à la demande de la Commission BIM que le service avait obtenu ce numéro en recourant à une méthode ordinaire (art. 16/2 L.R&S), alors que la réquisition à l'opérateur montrait qu'il ne s'agissait pas d'une simple identification de numéro. La méthode utilisée nécessitait la mise en œuvre d'une méthode spécifique (art. 18/8 § 1er, 1° et 2° L.R&S). '*Attendu en conséquence que les numéros de GSM obtenus l'ont été d'une manière non conforme à la loi ; Attendu que cette illégalité à l'origine ne peut qu'entraîner l'illégalité des méthodes qui se fondent sur cette méthode jugée illégale ; Attendu en conséquence que la présente méthode ne peut qu'être illégale*'.

III.3. CONCLUSIONS ET RECOMMANDATIONS

Le Comité permanent R formule les conclusions et les recommandations générales suivantes :

– Le nombre de méthodes particulières mises en œuvre par la VSSE a poursuivi sa courbe ascendante. Pour l'année 2017, cette tendance s'explique par l'augmentation des activités de renseignement au vu de la persistance de la menace terroriste. Cette augmentation est en grande partie attribuée à la forte hausse du nombre de 'localisations'.

- Nonobstant la persistance de la menace terroriste, le nombre (déjà peu élevé) de méthodes particulières mises en œuvre par le SGRS a continué de décroître.
- En ce qui concerne le SGRS, le Comité insiste sur le respect de l'obligation légale d'informer la Commission BIM toutes les deux semaines de l'exécution des méthodes exceptionnelles (art. 18/10 § 1er, alinéa 3 L.R&S et art. 9 AR 12 octobre 2010).
- Dans le cadre de la mise en œuvre des MRD, le SGRS s'est davantage concentré, comme toujours, sur la menace 'espionnage', tandis que la VSSE a focalisé son attention sur le 'terrorisme'.
- Indépendamment du fait qu'il est pratiquement impossible de comparer les chiffres en matière d'identifications sur base annuelle, le Comité ne peut nier le fait qu'un nombre beaucoup plus élevé d'identifications ont été effectuées depuis l'introduction de la procédure assouplie visée à l'article 16/2 L.R&S. S'appuyant sur sa compétence générale de contrôle, le Comité demandera à la VSSE d'examiner en interne dans quelle mesure ce nombre élevé de réquisitions tient (en partie) à l'assouplissement de la procédure. Il convient à cet égard d'être attentif à la nature des menaces qui justifient les réquisitions et à la question de savoir si et dans quelle mesure de telles réquisitions ont lieu à la demande d'autorités étrangères ou de services partenaires étrangers.
- Contrairement à la mise en œuvre des méthodes particulières, le Comité ne dispose pas des chiffres relatifs à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires visées à l'article 16/2 L.R&S. Le Comité recommande aux services de consigner également ces données et de les tenir à la disposition du Comité permanent R.
- La Loi du 25 décembre 2016 (*M.B.* 25 janvier 2017) a donné la possibilité à la VSSE et au SGRS d'avoir accès à des informations provenant de l'Unité d'information des passagers (art. 16/3 L.R&S). Le Comité est informé de cette méthode et peut l'interdire le cas échéant. Contrairement aux méthodes reprises à l'article 16/2 L.R&S, il n'a pas été prévu qu'un rapport doive être transmis au Parlement ; l'article 35 § 2 L.Contrôle n'a en effet pas été adapté. Le Comité permanent R recommande de le faire, d'autant qu'il faut établir un rapport sur la demande de données de transport et de voyage sur base de l'article 18/6/1 L.R&S, puisqu'il s'agit d'une méthode spécifique. Le Comité estime d'ailleurs qu'un tel rapport est tout aussi indiqué pour la possibilité introduite par la Loi du 21 mars 2018 (*M.B.* 16 avril 2018) d'utiliser des images enregistrées par des caméras et reprises dans des fichiers (art. 16/4 L.R&S).
- Le Comité n'a dû constater une illégalité que dans 15 dossiers. Comme le montre l'analyse de la jurisprudence, il s'agit essentiellement de dossiers dans lesquels le service de renseignement concerné avait omis d'autoriser l'exécution d'une méthode pour la période (parfois brève) entre deux méthodes légales.

CHAPITRE IV
LE CONTRÔLE DES INTERCEPTIONS À L'ÉTRANGER, DES PRISES D'IMAGES ET DES INTRUSIONS DANS DES SYSTÈMES INFORMATIQUES

Par la Loi du 30 novembre 1998, le SGRS s'est vu attribuer une compétence d'interception limitée : 'l'interception, l'écoute, la prise de connaissance ou l'enregistrement, […] à des fins militaires, de radiocommunications militaires émises à l'étranger.'

En 2003, cette possibilité a été considérablement étendue, tant en ce qui concerne la nature de la communication qu'en ce qui concerne la menace. Depuis lors, le SGRS peut concentrer ses interceptions sur '*toute forme de communications émises à l'étranger tant à des fins militaires dans le cadre des missions explicitées à l'article 11, § 2, 1° et 2° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité que pour des motifs de sécurité et de protection de nos troupes et de celles de nos alliés lors de missions à l'étranger et de nos ressortissants établis à l'étranger, comme explicité au même article 11, § 2, 3° et 4°.*' L'extension de cette compétence explique qu'une mission de contrôle spécifique ait été confiée au Comité permanent R (voir plus loin).

En 2010, la Loi a encore été modifiée[52] : outre '*l'interception, l'écoute, la prise de connaissance ou l'enregistrement*', le SGRS peut désormais '*rechercher*' des communications. Avant de procéder à l'interception, à l'écoute, à la prise de connaissance ou à l'enregistrement, le SGRS doit, en effet, être en mesure de surveiller l'ensemble du spectre électromagnétique et le cyberespace, par exemple en vue de rechercher de nouvelles possibilités (d'exploitation) ou pour disposer de suffisamment d'informations afin de s'assurer de la légalité de certaines interceptions.

En 2017, les compétences du SGRS ont une nouvelle fois été étendues, tout comme la mission de contrôle du Comité permanent R. Dans la première partie

---

52 Cette possibilité a été insérée par la 'Loi MRD'. Cette loi a permis à la VSSE et au SGRS d'écouter et d'enregistrer des communications sur le territoire belge (art. 18/17, § 1er L.R&S et Chapitre III). Il convient toutefois d'établir une distinction claire entre les 'interceptions MRD' et les 'interceptions de sécurité' décrites dans ce chapitre, que ce soit en ce qui concerne le champ d'application qu'en ce qui concerne le contrôle.

de ce chapitre, la modification de la loi est brièvement expliquée, tandis que la seconde partie propose un résumé de la manière dont le Comité a assuré sa mission de contrôle en 2017.

IV.1. MODIFICATION DE LA LOI : DE NOUVELLES COMPÉTENCES POUR LE SGRS ET UN CONTRÔLE RENFORCÉ[53]

Le 30 mars 2017, la Loi organique sur les services de renseignement et de sécurité a été modifiée. Cette modification, qui est entrée en vigueur le 8 mai 2017, élargit les compétences du SGRS dans le cadre des interceptions de sécurité. Les interceptions peuvent désormais porter sur des communications '*émises ou reçues à l'étranger*'. Avant la modification de la loi, les interceptions étaient strictement limitées aux communications émises à l'étranger. De plus, depuis mai 2017, cette possibilité vaut pour presque toutes les missions du SGRS.[54] Il est d'ailleurs intéressant d'observer que les descriptions de missions ont elles aussi été élargies par la même modification de loi (voir également Chapitre III.2.1).[55]

En outre, la loi introduit deux autres méthodes, à savoir l'intrusion dans un système informatique à l'étranger[56] et la prise d'images animées.[57]

La manière dont le Comité peut contrôler ces méthodes, a également changé à certains égards.

Le contrôle *préalable* aux interceptions, prises d'images fixes ou animées s'effectue sur base d'une liste établie annuellement.[58] Cela signifie qu'en plus du plan d'interceptions annuel, le SGRS doit également élaborer un plan d'intrusions et d'images. Le SGRS y dresse une liste d'*'intrusions dans leurs systèmes informatiques ou de prises d'images fixes ou animées dans le courant de l'année à venir. Ces listes justifieront pour chaque organisation ou institution la raison pour laquelle elle fera l'objet d'une interception, intrusion ou prise d'images*

---

53 Cf. art. 44 à 44/5 inclus L.R&S.

54 *'dans le cadre des missions visées à l'article 11, § 1er, 1° à 3° et 5° L.R&S'.*

55 Si une opération sur un réseau de communications est nécessaire pour permettre l'interception de communications émises ou reçues à l'étranger, le SGRS peut requérir le concours d'un opérateur de réseau ou d'un fournisseur du service de communications électroniques (art. 44/5 L.R&S).

56 Dans ce cadre, le SGRS peut *'procéder à l'intrusion dans un système informatique situé à l'étranger, y lever toute protection, y installer des dispositifs techniques en vue du décryptage, du décodage, du stockage et de la manipulation des données stockées, traitées ou transmises par le système, et perturber et neutraliser le système informatique'* (art. 44/1 L.R&S).

57 Dans ce cadre, le SGRS peut *'utiliser des moyens de prises d'images fixes ou animées à l'étranger'* (art. 44/2 L.R&S).

58 Cela ne signifie pas que le Comité permanent R a la compétence d'approuver ou non la liste approuvée par le Ministre.

fixes ou animées en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°, et mentionneront la durée prévue' (art. 44/3 L.R&S). Le SGRS doit envoyer ces listes au ministre de la Défense au mois de décembre pour autorisation. Le ministre prend une décision endéans les dix jours ouvrables et doit la communiquer au SGRS[59], qui transmet à son tour les listes pourvues de l'autorisation ministérielle au Comité permanent R.[60, 61]

Le contrôle réalisé *pendant* l'interception, l'intrusion ou la prise d'images s'effectue '*à tout moment moyennant des visites aux installations dans lesquelles le Service Général du Renseignement et de la Sécurité effectue ces interceptions, intrusions et prises d'images fixes ou animées*'.

Le contrôle réalisé *après* l'exécution a été sensiblement renforcé. Il s'effectue '*sur base de listes mensuelles des pays ou des organisations ou institutions ayant effectivement fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images durant le mois écoulé*' et qui justifient '*la raison pour laquelle l'écoute, l'intrusion ou la prise d'images a été effectuée en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°*'. Ces listes doivent être notifiées au Comité permanent R. Le contrôle *ex post* s'effectue aussi sur base '*du contrôle de journaux de bord tenus d'une façon permanente sur le lieu d'interception, d'intrusion ou de prise d'images fixes ou animées par le Service Général du Renseignement et de la Sécurité*'. Le Comité permanent R doit toujours avoir accès à ces journaux de bord.

Que peut faire le Comité permanent R s'il constate une irrégularité ? L'article 44/4 L.R&S stipule que, '*le Comité permanent de contrôle des services de renseignement, sans préjudice des autres compétences attribuées à ce Comité par la loi du 18 juillet 1991, a le droit de faire cesser des interceptions, intrusions ou prises d'images en cours lorsqu'il apparaît que celles-ci ne respectent pas les dispositions légales ou l'autorisation [ministérielle]. Il ordonne l'interdiction d'exploiter les données recueillies illégalement et leur destruction, selon les modalités à fixer par le Roi.*'[62] Le Comité doit motiver sa décision de manière circonstanciée et la communiquer au ministre et au SGRS.

---

59 Si le ministre n'a pas pris de décision ou ne l'a pas transmise au SGRS avant le 1er janvier, le service peut procéder aux interceptions, intrusions et prises d'images fixes ou animées prévues, sans préjudice de toute décision ultérieure du ministre.

60 Pour les interceptions, les intrusions ou les prises d'images qui ne figurent pas dans les listes annuelles mais qui *'s'avèrent indispensables et urgentes*', le ministre est averti dans les plus brefs délais et au plus tard le premier jour ouvrable qui suit le début de l'interception. S'il n'est pas d'accord, il peut faire cesser l'interception. Cette décision est communiquée au Comité permanent R le plus rapidement possible par le SGRS.

61 Le premier plan d'images et d'intrusions n'a été transmis au Comité que courant 2018.

62 Un tel arrêté royal n'a pas encore pris.

IV.2. LES CONTRÔLES EFFECTUÉS EN 2017

IV.2.1. LE PLAN D'ÉCOUTE

Le Comité permanent R n'a reçu qu'en juillet 2017 le plan d'interceptions validé par le ministre.[63] Les principales remarques formulées par le Comité portaient sur les différences en termes de priorité entre, d'une part, le Plan Directeur du Renseignement[64], et d'autre part, les interceptions prévues et le caractère trop général de la description des organisations ou des institutions qui feraient l'objet d'interceptions.

IV.2.2. L'INSPECTION ANNUELLE

Fin 2017, le Comité permanent R a effectué une visite de travail dans les installations SIGINT du SGRS afin de vérifier, entre autres, la conformité du journal de bord *(logbook)* avec la loi et avec les directives en la matière. Le Comité a également participé à une réunion de coordination de la section SIGINT.

Le Comité permanent R a pu constater que, tenant compte de ses remarques de l'année précédente, le SGRS utilisait un nouveau journal de bord. Aucune irrégularité n'a été relevée dans la tenue de ce journal, qui est conforme aux dispositions en vigueur.

IV.2.3. *MEMORANDUM OF UNDERSTANDING* AVEC UN PARTENAIRE ÉTRANGER

Le Comité permanent R a été informé de la signature d'un *Memorandum of Understanding* (MoU) avec un partenaire étranger concernant une capacité d'interception commune.

Si le Comité permanent R n'a pas relevé d'éléments contraires à la loi dans la mise en œuvre de ce MoU, il a néanmoins constaté que faute de personnel suffisant, les données interceptées n'avaient pas encore pu être exploitées.

IV.2.4. RÉSULTATS ET ÉVOLUTIONS

Dans le cadre du contrôle annuel effectué dans les installations SIGINT du SGRS, le Comité permanent R a pu se rendre compte des réalisations accomplies

63 Les années précédentes aussi, la liste a été transmise au Comité avec du retard.

64 Il s'agit d'un plan établi par la Direction I, qui reprend les pays à suivre et leur degré de priorité.

par la section SIGINT. Il a également été informé des projets initiés par la section sur le plan technique[65], pour l'engagement de traducteurs[66], au niveau des procédures[67] et pour l'utilisation des moyens.[68]

Pour 2018, le Comité permanent R a émis l'intention de s'investir encore plus dans le suivi de ce moyen de collecte, qui ne cesse de gagner en importance dans les échanges d'informations au niveau international. Il accorderait une attention particulière aux nouvelles compétences du SGRS (prises d'images et intrusions dans des systèmes informatiques) et à l'extension des finalités d'interception, à la coopération structurelle avec les partenaires et au développement de la description des targets.

65 Suite à l'augmentation du nombre de dossiers terroristes et à la nécessité de pouvoir échanger plus rapidement des informations brutes avec la VSSE, le SGRS a notamment instauré une ligne sécurisée avec ce service.

66 Le SIGINT est toujours confronté à un problème de capacités de traduction. Le Comité avait déjà exprimé ses préoccupations dans son *Rapport d'activités 2016* quant au manque de traducteurs qualifiés. Il a dû constater une nouvelle baisse du nombre de traducteurs. La section SIGINT travaille activement au recrutement de nouveaux collaborateurs, mais se heurte au refus de la DG Human Resources de libérer les candidats identifiés. Le manque de traducteurs au sein de cette section a un impact négatif sur l'ensemble du processus SIGINT, puisque les interceptions ne peuvent être traduites, ce qui ne permet donc pas d'en exploiter le contenu. Bien que la présence d'un traducteur ne soit pas toujours nécessaire pour exploiter une interception, le risque de 'rater' une information est jugé élevé.

67 À titre d'exemple, la section SIGINT poursuit la mise en place des 'fiches projets' initiée il y a deux ans. Le Comité permanent R a pu constater que le commandement de la section les utilisait dans le cadre de son processus décisionnel. Ce processus avait déjà évolué vers une symbiose entre la collecte et l'analyse. Il est toutefois nécessaire d'aller encore plus loin dans le sens d'une *analyse driven collection*. Les organisations et les institutions sont beaucoup mieux décrites dans ces fiches que dans le plan d'interceptions, notamment au moyen de sélecteurs. Ainsi, les fiches répondent mieux à l'exigence légale à satisfaire dans la confection d'une liste motivée d'institutions et d'organisations. Selon le Comité, les listes actuelles doivent être plus détaillées. Le SGRS-SIGINT s'est engagé à évoluer en ce sens, tout en affirmant de pas être en mesure de fournir des listes exhaustives de targets.

68 Par exemple, pour permettre à des personnes qui, dans l'exercice de leurs fonctions, devraient pouvoir disposer de données SIGINT, une nouvelle technologie est en cours d'élaboration pour élargir l'accès à certaines banques de données.

CHAPITRE V
MISSIONS POUR DES COMMISSIONS D'ENQUÊTE PARLEMENTAIRES

Depuis 1996[69], une Commission d'enquête parlementaire peut faire appel au Comité permanent R dans le cadre de ses enquêtes. Cette évolution s'inscrivait dans le cadre d'une réforme globale (en l'occurrence une extension[70]) des possibilités d'enquêtes parlementaires. C'est en 2016 que la possibilité de recourir aux services du Comité a été utilisée pour la première fois : tant la Commission d'enquête parlementaire sur les attentats terroristes que celle sur la transaction pénale ont confié plusieurs missions au Comité. En 2017 également, il s'est vu assigner différentes missions d'enquêtes par ces deux Commissions.

V.1. LA COMMISSION D'ENQUÊTE PARLEMENTAIRE SUR LES ATTENTATS

Le 22 mars 2016, la Belgique a été la cible d'attentats terroristes de grande ampleur. À la mi-avril 2016, une Commission d'enquête parlementaire 'chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste' a été instaurée[71], et ce, *'afin d'analyser si la Belgique s'est dotée de moyens pour lutter efficacement contre le radicalisme et le terrorisme,*

---

69 Loi du 30 juin 1996 modifiant la Loi du 3 mai 1880 sur les enquêtes parlementaires et l'article 458 du Code pénal, *M.B.* 16 juillet 1996 (en l'espèce, article 4 § 3 qui stipule que *'la Commission peut également, conformément à la loi du 18 juillet 1991 organique du contrôle des services de de police et de renseignements, charger les Comités permanents P et R d'effectuer les enquêtes nécessaires'*). Voir W. VAN LAETHEM, 'De Wetsgeschiedenis van 1991 tot 2013', VAN LAETHEM, W. et VANDERBORGHT, J. (eds.), *Regards sur le contrôle. Vingt ans de contrôle sur les services de renseignement*, Antwerpen, Intersentia, 2013, 55.

70 La loi énonce aujourd'hui que la Commission peut *'prendre toutes les mesures d'instruction prévues par le Code d'instruction criminelle'*. Une Commission d'enquête parlementaire peut donc effectuer une enquête sur place, procéder à l'audition de témoins, organiser des confrontations, désigner des experts ou procéder ou faire procéder au repérage de communications téléphoniques. Elle peut également faire procéder à des perquisitions et des saisies, et peut donc confier des missions d'enquête aux Comités permanents R et P.

71 *Doc. parl.*, Chambre 2016-17, 54-1752/1.

d'examiner si elle dispose de services aptes à assurer la sécurité des citoyens et de faire des recommandations qui permettraient de les améliorer'. À la mi-juin 2017, la Commission a déposé son 'Troisième rapport intermédiaire sur le volet Architecture de la sécurité'.[72]

Pour l'élaboration de son rapport, la Commission a fait appel à diverses reprises au Comité permanent R en 2016.[73] En 2017, les missions d'enquête se sont concentrées sur trois thèmes : la position d'information des services de renseignement sur un des protagonistes des attentats, Oussama Atar[74] ; le financement de la Grande Mosquée de Bruxelles ; et, enfin, l'état d'avancement du 'Plan d'action contre la radicalisation dans les prisons'.

À la mi-décembre 2016, le Président de la Commission avait souhaité obtenir de la VSSE[75] des informations sur Oussama Atar. Le Comité avait alors demandé au service de renseignement de quelles informations il disposait après le premier voyage de l'intéressé en Syrie, quels contacts il avait entretenus, et si des informations avaient été échangées à ce propos avec le SPF Affaires étrangères. Étant donné que l'enquête judiciaire était en cours et que des aspects des informations reçues provenaient de sources humaines et/ou de services partenaires, le Comité a traité les informations dans un rapport classifié. La note pouvait être consultée par l'expert de la Commission d'enquête titulaire d'une habilitation de sécurité. Un rapport déclassifié a été rédigé pour les membres de la Commission.

Après les auditions de l'imam de la Grande Mosquée de Bruxelles et du directeur du Centre Islamique et Culturel de Belgique (CICB), le Président de la Commission d'enquête parlementaire a demandé quelques autres précisions au Comité permanent R, en mars 2017 : la Commission souhaitait savoir si des *foreign terrorist fighters* (FTF) suivaient des formations organisées par la Grande Mosquée et si la Sûreté de l'État disposait d'informations sur les flux financiers entre le CICB et l'Arabie Saoudite. Le Comité a interrogé, à cet effet, tant la VSSE que l'OCAM.[76] La VSSE a conclu que l'examen des comptes du CICB n'apportait aucune preuve de financement direct d'une organisation terroriste par le Centre. En revanche, le CICB a joué un rôle important dans le financement d'individus ou d'entités actifs dans la propagande de l'idéologie salafiste-wahhabite sur le

---

72 *Doc. parl.*, Chambre 2016-17, 54-1752/8, 567 p.

73 Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2016* ('Chapitre V. Missions pour les Commissions d'enquête parlementaires'), 113-125.

74 Une enquête a également été effectuée en marge concernant l'existence à la VSSE d'informations sur un ancien inspecteur de police malinois.

75 Le Comité a aussi interrogé le SGRS à ce propos. Dans un premier temps, il est apparu que le service de renseignement militaire ne disposait d'aucune information concernant Atar. Par la suite, le Comité a pu démontrer que le SGRS détenait bien des informations sur l'intéressé.

76 Pour une réponse à cette question, il a également été suggéré par le Président de la Commission d'enquête de faire appel à la Cellule de Traitement des Informations Financières (CTIF).

territoire belge. La réponse à la question de savoir si des FTF suivaient une formation à la Grande Mosquée de Bruxelles a fait l'objet d'un rapport classifié.

En juillet 2017, enfin, la Commission d'enquête a demandé au ministre de la Justice d'exposer l'état d'avancement de l'exécution du 'Plan d'action contre la radicalisation dans les prisons' (mars 2015).[77] En effet, on sait que les prisons représentent un terreau pour l'idéologie radicale en raison de l'environnement, de l'absence de perspectives, de la santé mentale des détenus, de l'ennui… Dans les prisons belges, on ne recense quasiment que des cas de radicalisation et d'extrémisme religieux (islam). Depuis la mi-2014, la VSSE accorde une attention spécifique à ce phénomène. Le service a adressé au Comité permanent R une réponse classifiée et détaillée sur l'exécution du Plan d'action. Le Comité a ensuite permis à l'expert de la Commission de consulter ces informations.

La Commission d'enquête parlementaire a finalisé son rapport en octobre 2017.[78] Ce rapport préconise l'instauration d'une 'Commission de suivi' chargée de contrôler la concrétisation des recommandations.

V.2. LA COMMISSION D'ENQUÊTE PARLEMENTAIRE SUR LA LOI 'TRANSACTION PÉNALE'

V.2.1. PRÉAMBULE

Début décembre 2016, le texte visant à instaurer une seconde Commission d'enquête parlementaire a été adopté en séance plénière de la Chambre.[79] L'élaboration de la transaction pénale élargie (Loi du 14 avril 2011) était un élément central. En effet, à la suite de la parution d'articles dans la presse, de sérieuses questions se sont posées sur la rapidité avec laquelle une proposition de loi a reçu l'aval du Parlement en 2011. Un lobbying intensif aurait été exercé pour en accélérer le traitement. L'hebdomadaire français *Le Canard Enchaîné* prétendait que les autorités kazakhes avaient conditionné la commande d'hélicoptères français à la capacité des autorités françaises à mettre un terme aux poursuites lancées, en Belgique, à l'encontre du 'trio kazakh'.[80] À cette

77 Le plan poursuit une double finalité : d'une part, éviter que des détenus se radicalisent au cours de leur séjour en prison et, d'autre part, élaborer un encadrement spécialisé des personnes radicalisées pendant leur détention.

78 *Doc. parl.*, Chambre, 2017-18, 54-1752/10.

79 Proposition visant à instituer une Commission d'enquête parlementaire chargée d'enquêter sur les circonstances ayant conduit à l'adoption et l'application de la loi du 14 avril 2011 portant des dispositions diverses, en ce qui concerne la transaction pénale (*Doc. parl.*, Chambre 2016-17, 54-2179/6). La Commission a finalisé son rapport le 16 avril 2018 (*Doc. parl.*, Chambre 2017-18, 54-2179/7).

80 Il s'agit de trois associés provenant d'Asie centrale qui se sont établis en Belgique au début des années 90 pour fonder des sociétés.

époque, les autorités françaises auraient fait appel à un sénateur belge et membre de l'Assemblée parlementaire du Conseil de l'Europe.

L'affaire a été mise au jour en 2012 et a conduit à l'ouverture d'une enquête par les autorités judiciaires françaises. En février 2015, d'autres révélations ont suivi : une enquête approfondie s'imposait sur les interventions politiques et financières, individuelles et diplomatiques, nationales et internationales, ainsi que sur les pressions et l'influence qui ont mené à l'élaboration de cette 'loi sur la transaction financière'.

La Commission d'enquête a subdivisé ses activités en trois volets : 'Volet I. Naturalisation et acquisition de la nationalité' ; 'Volet II. Élaboration de la Loi du 14 avril 2011 portant des dispositions diverses, en ce qui concerne la transaction pénale'[81] ; et enfin 'Volet III. Application de la Loi transaction pénale élargie jusqu'à l'entrée en vigueur de la Loi de réparation du 11 juillet 2011'.[82]

À la mi-décembre 2016, le Président du Comité permanent R a adressé un courrier au Président de la Commission, dans lequel il l'informait que le Comité disposait de documents relatifs à la naturalisation des personnes citées dans le dossier. Ces documents provenaient essentiellement de la Sûreté de l'État (VSSE) – qui a une compétence d'avis en matière de naturalisations – et étaient issus d'enquêtes de contrôle clôturées (Tractebel, *infra*).

En 2017, le Comité permanent R[83] a été impliqué de manière intensive et s'est vu confier diverses missions d'enquête par la Commission d'enquête parlementaire. Les activités du Comité permanent R pour cette Commission étaient de plusieurs ordres : transmettre des rapports d'enquête, rédiger divers rapports, faire office de 'passerelle' en ce qui concerne les informations classifiées, en les expurgeant des informations les plus sensibles, et être entendu comme témoin.

V.2.2. TRANSMISSION D'ANCIENS RAPPORTS D'ENQUÊTE

Le Comité permanent R avait déjà effectué des enquêtes de contrôle susceptibles de présenter un intérêt direct ou indirect pour la Commission d'enquête. Il s'agissait des enquêtes concernant 'Le fonctionnement des services de renseignement belges dans la gestion d'éventuelles informations dans un contexte préalable à la passation d'un marché international' (2000)[84], un rapport

---

81 Un Volet II(bis) y a été ajouté : 'Mise sur pied de l'équipe d'avocats […] pour le compte de l'Élysée'.

82 Article 1er § 1er, alinéa 3 de l'arrêté de constitution (*Doc. parl.*, Chambre 2016-17, 54-2179/6).

83 Le Comité permanent P s'est lui aussi vu confier une mission d'enquête dans le cadre du Volet I (rapport 30875/2017).

84 L'enquête de contrôle a fait l'objet de deux rapports concis (COMITÉ PERMANENT R, *Rapport d'activités 2001*, 5-7 et *Rapport d'activités 2003*, 118). Cette enquête n'a jamais été menée à son terme en raison d'autres priorités.

sur la manière dont la VSSE s'acquitte de sa nouvelle mission de protection du potentiel économique et scientifique[85], ainsi que l'enquête portant sur 'Le rôle de la VSSE dans le cadre des procédures d'acquisition de la nationalité belge.'[86]

V.2.3. 'FILTRE' POUR LA CONSULTATION DE DOCUMENTS CLASSIFIÉS

Eu égard à sa mission et à l'étendue de ses compétences, la Commission d'enquête parlementaire a estimé utile d'avoir accès à des documents contenant des renseignements classifiés, qu'il s'agisse de dossiers d'instructions judicaires, ou encore d'informations détenues par des organismes dont le travail est par essence secret (tels que la Sûreté de l'État, le SGRS).

Quant à la consultation d'informations classifiées de la Sûreté de l'État[87], il convenait de trouver un *modus vivendi*, vu que les membres de la Commission n'étaient pas titulaires de l'habilitation de sécurité requise.[88] Il a été décidé que les informations classifiées seraient examinées par le Comité permanent R et qu'en accord avec les services de renseignement, celui-ci déciderait quelles informations peuvent être transmises. En effet, contrairement à la Commission d'enquête sur les attentats terroristes, la Commission ne pouvait pas s'appuyer sur ses experts, ceux-ci n'étant pas titulaires d'une habilitation de sécurité.

Dix rapports ont finalement été rédigés et diffusés sur une période allant de janvier à septembre 2017.[89] Plusieurs thèmes y étaient abordés. Par exemple, le rôle de la VSSE a pu être expliqué dans le cadre de l'octroi de la naturalisation et de la nationalité au trio kazakh, ainsi que l'attention portée (dans le passé) par le service de renseignement à l'octroi de permis de travail. En outre, les activités de la VSSE avant, pendant et après la confection de la Loi sur la transaction pénale élargie, ont été décrites, notamment l'attention du service pour la présence croissante d'hommes d'affaires et de responsables politiques du Kazakhstan. La visite à Paris d'un ancien Vice-président du Sénat a été abordée. Il était question d'une rencontre avec les adjoints du coordinateur national des services de renseignement français, rencontre au cours de laquelle un document classifié

85 COMITÉ PERMANENT R, *Rapport d'activités 2000*, 109-148.

86 Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2012*, 5-14.

87 À cet effet, la VSSE a mis à la disposition du Comité plusieurs classeurs bien fournis de documentation (classifiée) et a répondu à des questions d'enquête ponctuelles formulées par le Comité.

88 La Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité stipule, en effet, que *'nul n'est admis à avoir accès aux informations, documents […] s'il n'est pas titulaire d'une habilitation de sécurité correspondante et s'il n'a pas besoin d'en connaître et d'y avoir accès pour l'exercice de sa fonction […]'* (art. 8 L.C&HM).

89 Les rapports – en version 'Diffusion restreinte' – ont été systématiquement soumis à la VSSE, en lui demandant de déclassifier un maximum de pièces.

(ladite 'fiche V', *infra*) aurait été remis.[90] Une autre affaire relative au Sénateur précité a été examinée : il s'est permis d'approcher l'ancien Administrateur général en lui demandant d'ordonner l'utilisation d'une méthode particulière de renseignement afin de retrouver son GSM. Un autre rapport portait sur la description d'Eric V. – un homme d'affaires qui a un passé judiciaire, qui est entré en contact avec le trio kazakh et qui apparaissait à maintes reprises dans la documentation de la VSSE. Si nécessaire, le Comité permanent R a informé la Commission sur ce qui était paru dans la presse à propos des différents témoins.[91]

Le SGRS était lui aussi, certes dans une moindre mesure, impliqué dans l'enquête. Le Comité a vérifié si, avant la conclusion d'un *Memorandum of Understanding* (MoU), le 25 octobre 2010, entre le Centre d'Étude de l'Énergie Nucléaire belge, le Centre National Nucléaire du Kazakhstan et Kazatomprom, le SGRS était au courant des développements en la matière, et si les noms du trio kazakh y étaient mentionnés.

V.2.4. TÉMOIN(S) DEVANT LA COMMISSION D'ENQUÊTE

Le Président du Comité permanent R a été entendu à cinq reprises.[92] Les rapports d'enquête ont été discutés en audience publique, sauf si le Président – en raison du caractère très sensible non seulement des faits et des événements relatés, mais aussi des personnes citées – sollicitait le huis clos.[93]

Le Président a fait rapport sur la naturalisation des protagonistes et sur des dossiers apparentés, en mentionnant l'intervention de la VSSE dans ces dossiers de naturalisation. Dans un deuxième temps, un rapport sur l'acquisition de la nationalité de ces protagonistes a été discuté, ainsi que le fonctionnement interne du Comité permanent R. Le dossier Tractebel a par ailleurs été abordé. La discussion portant sur les informations dont disposait la VSSE sur les activités et les contacts, au cours de la période 2010-2011, de personnes qui faisaient l'objet

---

90 Dans ce cadre, une réflexion a été menée sur l'application par la VSSE de l'article 29 CIC ou de l'article 19 L.R&S et sur ce qu'il convenait de faire avec les informations disponibles concernant un parlementaire.

91 Par exemple, sur une donation de l'Ordre de Malte au fonds de bienfaisance (Fonds d'Entraide Prince et Princesse Alexandre de Belgique) et 'la Compagnie des Mousquetaires d'Armagnac', ou l'intervention d'une avocate dans les dossiers de naturalisation et concernant les contacts avec le trio kazakh avec la direction de Tractebel.

92 Les 25 janvier 2017, 15 février 2017 (en partie à huis clos), 29 mars 2017 (en partie à huis clos), 24 avril 2017 (à huis clos) et 7 juin 2017 (à huis clos). L'ancien Président du Comité permanent R, Jean-Claude Delepière, et l'ancien Conseiller Walter De Smedt ont eux aussi été entendus par la Commission.

93 Le Président a dû expliquer à plusieurs reprises la législation en vigueur en matière de classification. La Commission d'enquête a, à son tour, envisagé d'introduire une plainte auprès du Parquet de Bruxelles après des fuites répétées dans les médias.

de l'enquête de la Commission et sur l'influence éventuelle de la France dans l'élaboration de la Loi sur la transaction pénale élargie (Volet II) a eu lieu à huis clos. Lors de la quatrième audition, quelques renseignements déclassifiés de la VSSE sur les protagonistes ont été développés pour la période février-mars 2011. Enfin, une explication a été donnée sur une enquête qui avait été menée à la demande de la Commission sur l'ancien Administrateur général de la VSSE. Dans la foulée, ce dernier a été auditionné en réunion publique sur les conclusions du Comité permanent R concernant ses contacts avec le Sénateur précité et avec un service de renseignement français.

V.2.5. L'EXÉCUTION DE MISSIONS D'ENQUÊTE COMPLÉMENTAIRES

À la demande du Président de la Commission d'enquête parlementaire, le Comité permanent R s'est penché sur une plainte anonyme adressée à la Chambre des Représentants.[94] Il était question de deux thématiques dans le courrier non daté : la naturalisation et l'intimidation de certains collaborateurs du service de renseignement ainsi que l'ingérence, au sein de la VSSE, de figures éminentes d'un parti politique. À l'exception de l'existence d'un conflit interpersonnel entre deux membres de la Sûreté de l'État, le Comité n'a trouvé aucun élément susceptible d'étayer les faits décrits dans le courrier.

Enfin, le flux d'informations entre les Comités permanents R et P, la relation entre les enquêtes de contrôle et les enquêtes judiciaires en cours, ainsi que la manière de clôturer des enquêtes de contrôle ont été abordés.

94 La plainte anonyme était intitulée comme suit : '*Kazakhgate : ce que la Sûreté ne veut pas dire à la Commission parlementaire*'.

CHAPITRE VI
LE CONTRÔLE DE BANQUES DE DONNÉES COMMUNES

Adoptée dans la foulée des attentats de Bruxelles, la Loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme[95] a modifié la Loi du 5 août 1992 sur la fonction de police (LFP) afin d'instaurer une base légale pour la création de banques de données communes.

L'article 44/6 LFP assigne le contrôle du traitement des informations et des données à caractère personnel contenues dans les banques de données communes à l'Organe de contrôle de l'information policière (C.O.C.) et au Comité permanent R. Les deux instances sont également chargées de rendre conjointement un avis préalable à la création d'une banque de données commune, sur base d'une 'déclaration préalable' à introduire par les responsables du traitement (les ministres de l'Intérieur et de la Justice). En vue d'exercer ces deux compétences de manière coordonnée, les deux institutions ont conclu un protocole d'accord en décembre 2017.

VI.1. LA BANQUE DE DONNÉES *FOREIGN TERRORIST FIGHTERS* : UN BREF RAPPEL[96]

S'appuyant sur cette nouvelle possibilité offerte par le législateur, les ministres de l'Intérieur et de la Justice ont créé la banque de données commune *foreign terrorist fighters*.[97]

Cette banque de données est composée de fiches de renseignements concernant les personnes impliquées dans le phénomène des combattants qui se rendent dans des zones de combat djihadistes. Ces fiches doivent permettre d'évaluer la menace potentielle que représentent ces personnes, mais

95 *M.B.* 9 mai 2016.

96 Pour un commentaire approfondi, voir COMITÉ PERMANENT R, *Rapport d'activités 2016*, 129-140 (www.comiteri.be).

97 A.R. du 21 juillet 2016 relatif à la banque de données commune 'Foreign Terrorist Fighters' et portant exécution de certaines dispositions de la section 1ère *bis* 'de la gestion des informations' du chapitre IV de la Loi sur la fonction de police, *M.B.* 22 septembre 2016.

essentiellement d'en assurer le suivi afin d'anticiper et d'empêcher de possibles actes terroristes de leur part.[98]

Les fiches sont tenues actualisées par les 'services de base' (l'OCAM, la police intégrée et les services de renseignement) et 'les services partenaires'.[99] Les différents services qui accèdent directement à la banque de données ont l'obligation de l'alimenter en permanence, raison pour laquelle elle est qualifiée de banque de données 'dynamique'.

Les fiches de renseignements contiennent toutes les données à caractère personnel et les informations[100] non classifiées concernant les intéressés.

Ces fiches sont exclusivement établies à propos des personnes résidant ou ayant résidé en Belgique, ayant ou non la nationalité belge et qui, dans le but de se rallier à des groupements terroristes ou de leur fournir un soutien actif, se trouvent dans une des situations (catégories) suivantes (art. 6, § 1er, 1° AR FTF) :

- Elles se sont rendues dans une zone de conflit djihadiste (Catégorie 1) ;
- Elles ont quitté la Belgique pour se rendre dans une zone de conflit djihadiste (Catégorie 2) ;
- Elles sont en route vers la Belgique ou sont revenues en Belgique après s'être rendues dans une zone de conflit djihadiste (Catégorie 3) ;
- Elles ont (volontairement ou non) été empêchées de se rendre dans une zone de conflit djihadiste (Catégorie 4) ;
- Elles ont l'intention de se rendre dans une zone de conflit djihadiste (à condition qu'il existe des indications sérieuses démontrant ces intentions) (Catégorie 5) ;
- OU
- Il existe de sérieux indices qu'elles puissent remplir un des critères précédents (art. 6, § 1er, 2° AR FTF).

Des 'cartes d'information' sont élaborées à l'intention des instances qui n'ont pas d'accès aux fiches de renseignements. La carte est un extrait de la fiche de renseignements et contient les données et les informations strictement limitées aux besoins du destinataire. Seuls les services de base sont autorisés à transmettre la carte d'information.

---

98 Extrait du Rapport au Roi (*M.B.* 22 septembre 2016, 63970).

99 Certains des services partenaires (la Direction générale Établissements pénitentiaires et les établissements pénitentiaires, le Ministère public, la Cellule de Traitement des Informations Financières et l'Office des étrangers) disposent d'un accès direct à la banque de données, comme c'est le cas des services de base. D'autres services partenaires (la Direction générale du centre de crise, la Direction générale Sécurité et Prévention du SPF Intérieur, la Direction générale des Affaires consulaires du SPF Affaires étrangères et les services d'enquête et de recherche des Douanes et Accises) peuvent l'interroger directement sur base du principe du *hit/no hit*.

100 Données d'identification, judiciaires, administratives, de police judiciaire, de police administrative et les renseignements non classifiés adéquat(e)s, pertinent(e)s et non excessives (excessifs).

VI.2. LA MISSION DE CONTRÔLE

VI.2.1. L'OBJET DU CONTRÔLE

Dans le cadre de leur mission de contrôle conjoint, le C.O.C. et le Comité permanent R ont décidé, en 2017, d'examiner les éléments suivants :
- le contenu de la fiche de renseignements et de la carte d'information ainsi que son adéquation avec les prescrits légaux et réglementaires ;
- le contrôle des actions de l'OCAM en ce qui concerne la validation initiale comme FTF ainsi que les traitements ultérieurs ;
- le contrôle des consultations des fiches de renseignements et de cartes d'information par les services de base et les services partenaires ;
- le contrôle sur la manière dont les bourgmestres sont informés de la carte d'information (ceci peut concerner plusieurs bourgmestres par entité) ;
- l'identification des utilisateurs de la banque de données commune FTF, le nombre d'accès directs/interrogations directes, l'exécution (ou non) d'un contrôle de la légitimité des accès directs/interrogations directes, l'existence (ou non) d'un système de validation et la survenance d'éventuels incidents de sécurité ;
- l'existence d'une mise à jour du manuel d'utilisation de la banque de données ;
- l'examen des données de journalisation relatives à deux journées présélectionnées ;
- la désignation d'un conseiller en sécurité et en protection de la vie privée.

VI.2.2. CONTRÔLES EFFECTUÉS ET CONSTATATIONS

VI.2.2.1. Au niveau de l'Organe pour la coordination et l'analyse de la menace

Compte tenu du rôle central qu'il occupe en sa qualité de responsable opérationnel de la banque de données FTF[101], un contrôle prioritaire s'imposait au niveau de l'OCAM.[102]

---

101 L'art. 44/11/3*bis* LFP lui assigne les missions de contrôler la qualité et la pertinence des données traitées, d'organiser la collaboration adéquate et le respect des finalités prévues. Des missions spécifiques lui sont également attribuées par l'art. 4 de l'AR FTF : l'évaluation des données de la fiche de renseignements, la validation d'une personne comme FTF, le rôle de point de contact avec les ministres de l'Intérieur et de la Justice et l'information du service concerné lorsqu'une de ses informations n'est plus adéquate, pertinente ou est devenue excessive.

102 Plusieurs réunions ont été organisées avec l'OCAM. Le C.O.C. et le Comité permanent R se sont vu remettre par l'OCAM les documents (fiches et cartes) demandées. Des questionnaires écrits lui ont également été adressés.

VI.2.2.1.1. Une gestion opérationnelle parfois difficile

Au moment du contrôle, l'OCAM procédait à un double enregistrement.

Le premier enregistrement avait lieu dans la banque de données (classifiée) propre à l'OCAM. Toutes les informations (classifiées ou non) relatives à une entité y étaient reprises et servaient à l'évaluation de celle-ci. Pour ce faire, les éléments 'à charge' et 'à décharge' étaient pris en considération dans une fiche de travail préparatoire.

Un second encodage, portant sur les informations non classifiées et non soumises à embargo (c'est-à-dire la partie la plus importante des informations reçues), était ensuite effectué dans la banque de données FTF. C'est au niveau de ce second encodage que l'OCAM déplorait une perte de temps.

Une solution technique a pu être dégagée. Sa mise en œuvre est prévue dans le courant de l'année 2018.

VI.2.2.1.2. Le contrôle de qualité effectué par l'OCAM

Le C.O.C. et le Comité permanent R ont pu constater que l'OCAM veillait à la qualité des données figurant dans les fiches des dossiers analysés et à la pertinence de ces données au regard des finalités légales. À titre d'exemple, l'OCAM a signalé à plusieurs reprises à un service concerné que les informations fournies n'étaient pas pertinentes en vue d'un enregistrement dans la banque de données commune FTF.

L'OCAM a rédigé une note concernant le contrôle de qualité en ce qui concerne le traitement des données dans la banque de données commune. Une 'équipe qualité' ('*team Q*') a été mise sur pied au sein de l'OCAM au début de l'année 2017. Cette équipe est chargée du contrôle de qualité et de l'élaboration de directives pour le traitement des données. L'analyse porte sur la qualité de l'enregistrement de données de base, la vérification de l'encodage des niveaux de menace, le contrôle de la présence de l'évaluation des données et la motivation de cette évaluation. L'exactitude de l'encodage de certaines dates fait également l'objet d'un contrôle. En outre, la rédaction de la fiche (et la motivation) est analysée en ce qui concerne le respect des différents degrés de classification.

Les résultats des mois de mai, juin et octobre (2017) ont été communiqués au C.O.C. et au Comité permanent R. Il est ressorti des documents qui ont été remis qu'en fonction des constatations, un suivi approprié (briefing supplémentaire, interpellation du titulaire de la fiche, communications par e-mail aux titulaires…) a été donné après les omissions constatées.[103]

Le C.O.C. et le Comité permanent R ont estimé que l'exécution (et la documentation) des contrôles de qualité démontrait que l'OCAM assumait avec

[103] Les omissions constatées dans quelques fiches se situent principalement au niveau de l'évaluation des données ou de la motivation de cette évaluation. Par ailleurs, il est apparu que certaines dates de dernières mises à jour n'étaient pas indiquées.

rigueur son rôle de responsable opérationnel de la banque de données FTF. Le C.O.C. et le Comité permanent R ont exhorté l'OCAM à poursuivre ces contrôles, à les documenter et, évidemment, à en tirer les conclusions requises au niveau approprié.

VI.2.2.1.3. Un contrôle aléatoire par le C.O.C. et le Comité permanent R

Une sélection aléatoire a été effectuée dans la banque de données commune FTF parmi les 619 entités FTF qui y figuraient alors. Le C.O.C. et le Comité permanent R ont pu constater que le contenu des fiches de renseignements et des cartes d'information des dossiers concernés répondait aux dispositions légales et réglementaires.

Les informations figurant dans ces fiches de renseignements étaient alimentées et enrichies par différents services (pas seulement la police et la VSSE, mais aussi, par exemple, par la Direction générale des Établissements pénitentiaires), ce qui apportait une plus-value et répondait ainsi à la finalité de la banque de données commune.

Le C.O.C. et le Comité permanent R ont constaté, sur base des fiches de renseignements et des cartes d'information FTF présentées et analysées, que l'OCAM avait une approche professionnelle et sérieuse dans l'évaluation des informations qui lui étaient adressées.

Par ailleurs, l'enquête n'a révélé aucune trace d'informations qui, conformément à un embargo judiciaire ou à une classification légale, n'auraient pas pu être reprises.

Des informations policières provenant de rapports d'informations (RIR) portant le code 00 ou 01 figuraient dans la banque de données.[104] L'OCAM avait pourtant indiqué ne jamais les reprendre dans la banque de données FTF, compte tenu de la sensibilité des informations qu'ils contiennent.

Il ressort de l'analyse du C.O.C. et du Comité permanent R que cette pratique de l'OCAM d'exclure systématiquement les RIR 00 et 01 n'était pas prévue dans la réglementation. En effet, *de lege lata*, les seules exceptions à l'obligation d'alimenter la banque de données commune d'une information résultent :

– soit de la classification[105] : l'information classifiée ne peut être contenue dans les fiches de renseignements ni dans les cartes d'information[106] ;

---

104 Ces codes sont attribués par le service (policier) rédacteur. Un 'RIR 01' concerne des informations policières qui ne peuvent être utilisées qu'avec l'accord du rédacteur. Un 'RIR 00' concerne des informations policières qui ne peuvent en aucun cas être utilisées. Il s'agit d'informations très sensibles qui, par exemple, peuvent conduire à l'identification d'une source. Ces codes résultent de la Circulaire MFO3 du 14 juin 2002 des ministres de l'Intérieur et de la Justice relative à la gestion de l'information de police judiciaire et de police administrative.

105 Sur base de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

106 Article 1er, 11° et 12° ; Article 6 § 1er, 3° AR FTF.

– soit d'un embargo décidé par le magistrat compétent avec l'accord du procureur fédéral[107] : dans ce cas, l'obligation d'alimentation est différée (et non exclue) aussi longtemps que cette alimentation peut compromettre l'exercice de l'action publique ou la sécurité d'une personne ;
– soit d'un embargo décidé par le dirigeant d'un service de renseignement et de sécurité lorsque et aussi longtemps qu'il estime que cette alimentation peut compromettre la sécurité d'une personne ou lorsque l'information émane d'un service étranger qui a explicitement demandé de ne pas la transmettre à d'autres services.[108]

Ceci signifie qu'à défaut de classification ou d'embargo, tout rapport d'information doit être repris dans la banque de données communes FTF.

VI.2.2.1.4. Les personnes en 'pré-enquête'

Les personnes pour lesquelles il n'existe que des 'indices sérieux' (et donc aucune certitude) d'appartenance à l'une des cinq catégories ne peuvent figurer dans la banque de données que pour une durée maximale de six mois (art. 6 § 1er, 2° et 13 AR FTF). Si, dans ce délai, aucune information ne vient justifier l'appartenance à l'une des cinq catégories, il convient d'effacer les noms de ces personnes en 'pré-enquête'.

L'examen des listes de ces personnes de mars 2017 (près de trois cents personnes) et de décembre 2017 (une vingtaine de personnes) a mis en évidence que cinq entités qui figuraient sur la première liste apparaissaient encore sur la seconde. Vu le délai maximal de conservation de six mois, cela n'aurait pas dû être le cas. Il n'y avait apparemment aucun effacement ni signal automatique si l'OCAM omettait d'intervenir. Ce point était dès lors susceptible d'amélioration.

VI.2.2.1.5. La conservation des données

Pour les personnes reprises dans la banque de données, la LFP prévoit qu'il faut examiner, au minimum tous les trois ans après le dernier traitement, si les données présentent toujours un lien direct avec la finalité. Dans l'affirmative, elles sont conservées.

Selon les constatations du C.O.C et du Comité permanent R, l'OCAM ne disposait pas d'un outil informatique permettant d'assurer le respect de cette obligation spécifique. À ce propos, l'OCAM a affirmé que cette solution technique n'était pas (encore) une priorité (en 2017), étant donné que l'évaluation ne doit avoir lieu qu'au plus tard après trois ans, et que la banque de données commune est effective depuis le 1er janvier 2016.

107 Article 44/11/3*ter*, § 5 LFP.
108 Article 44/11/3*ter*, § 5 LFP.

Le C.O.C. et le Comité permanent R préconisent le développement d'un outil informatique en 2018, de manière à ce que l'OCAM puisse suivre les délais de conservation dès janvier 2019.

VI.2.2.2. Le contrôle des loggings auprès du gestionnaire de la banque de données

Le C.O.C. et le Comité permanent R ont demandé à la Police fédérale de leur transmettre le détail des loggings des différents services concernant deux journées choisies de manière aléatoire. Les informations transmises, corroborées par l'analyse d'un échantillon des fiches de renseignements (*supra*), montrent que la banque de données commune FTF était effectivement consultée, alimentée et utilisée par les différents services.

Un accès aussi large comporte évidemment des risques en termes de sécurité. Les conseillers en sécurité et en protection de la vie privée des services concernés et le conseiller pour la banque de données FTF ont ici un rôle important à jouer, puisqu'ils veillent à la légalité des divers accès par les différents services. Les loggings constituent, à cet effet, le moyen de contrôle par excellence. Au moment de l'inspection, le C.O.C. et le Comité permanent R ont cependant dû constater qu'il n'y avait eu que peu de contrôles des loggins, voire aucun (*infra*).

Par conséquent, le C.O.C. et le Comité permanent R ont estimé que les conseillers en sécurité et en protection de la vie privée concernés devaient effectuer des contrôles systématiques, ou à tout le moins des échantillonnages réguliers, sur les loggings de leurs services.

VI.2.2.3. L'information des bourgmestres

L'AR FTF prévoit que le chef de corps de la zone de police concernée transmet (systématiquement) au bourgmestre la carte d'informations relative aux *foreign fighters* résidant dans sa commune. Le bourgmestre peut ensuite l'utiliser dans le cadre de ses compétences et sous sa responsabilité. L'OCAM n'avait aucune vue sur la manière dont cette obligation était respectée.[109]

VI.2.2.4. Communication d'extraits de la carte d'information à des tiers

L'OCAM transmet chaque mois à différents destinataires une liste dans laquelle figuraient les noms de tous les FTF.[110] De l'avis de l'OCAM, il s'agit de services qui ont besoin de ces informations dans l'exercice de leurs compétences.

---

109 Dès lors, l'enquête portant sur le respect de cette obligation doit être effectuée d'une autre manière. Le C.O.C. et le Comité permanent R reviendront sur cet aspect dans une enquête ultérieure. Ils n'en ont pas moins attiré l'attention sur l'utilité d'un outil de suivi au niveau de l'OCAM pour veiller à ce que cette obligation soit effectivement respectée.

110 À noter que cette communication s'effectuait par e-mail. Même si ces données ne sont pas classifiées et que l'article 11 AR FTF prévoit que cette transmission peut avoir lieu '*par*

Certains de ces services ont un accès direct à la banque de données. Aucun problème ne se pose pour eux. En ce qui concerne les autres services, le C.O.C. et le Comité permanent R rappellent que la lecture conjointe des articles 44/11/3*quater* LFP et 11 § 2 AR FTF impose que ces communications à des tiers fassent préalablement l'objet d'une évaluation par l'OCAM ou les services de police et de renseignement.

Le C.O.C. et le Comité permanent R estiment qu'une telle évaluation doit nécessairement inclure l'analyse de tous les aspects en matière de sécurité des informations concernant les FTF et, sur base de cette analyse, imposer des mesures de sécurité adéquates aux différents destinataires.

VI.2.2.5. Contrôle d'autres services dotés d'un accès à la banque de données FTF

VI.2.2.5.1. Vérifications menées auprès de différents services

Le contrôle effectué en 2017 ne s'est pas limité à l'OCAM. Suite à des vérifications effectuées auprès de différents services, le C.O.C. et le Comité permanent R ont pu établir que :

- tous les services disposaient d'une liste mentionnant l'identité des personnes ayant accès à la banque de données. Il a été déclaré que toutes ces personnes détenaient une habilitation de sécurité du niveau 'secret' ;
- les services n'avaient pas directement accès aux loggings (ceux-ci sont disponibles auprès de la Police fédérale), si bien que la plupart des services n'ont pas été en mesure d'effectuer un contrôle de la légalité des accès ou interrogations de la banque de données (*supra*).
- à l'exception du Ministère public[111], la plupart des services disposent d'un système de validation. Certains d'entre eux l'ont affiné suite à la question du C.O.C. et du Comité permanent R. Des réserves doivent être formulées quant au système présenté par l'un des services qui n'effectue un contrôle dans la banque de données FTF que si la personne est déjà connue dans la Banque de données nationale générale des services de police (BNG). Une personne peut

quelque moyen que ce soit', le C.O.C. et le Comité permanent R estiment que, compte tenu de la sensibilité des informations, il convient d'être attentif à la sécurisation de cette transmission.

111 Il y a lieu de se référer à l'Exposé des motifs de la Loi 27 avril 2016 (*Doc. parl.*, Chambre 2015-2016, 54-1727/1, 30) et au Rapport au Roi de l'AR FTF : '*Le législateur a pris en compte le statut indépendant particulier du Ministère public et a estimé que les données judiciaires proviennent essentiellement des services de police. De ce fait, l'obligation pour les services de police d'alimenter la banque de données communes est suffisante pour que soient enregistrées les données pertinentes. Pour s'assurer que l'alimentation de la banque de données FTF soit bien exécutée dans ce cadre, les autorités judiciaires donnent les instructions appropriées par voie, notamment, des circulaires*'. La COL 22/2016 énonce les directives en ce sens à l'attention des services de police.

en effet être insérée dans la banque de données FTF (par exemple à l'initiative d'un service de renseignement), sans nécessairement être reprise en BNG.

– aucun service n'a eu connaissance d'un incident de sécurité.[112] Réinterrogée ultérieurement à ce propos, la Police fédérale a informé le C.O.C. et le Comité permanent R de la survenance d'un incident de sécurité durant le mois d'octobre 2017. Le C.O.C. et le Comité permanent R estiment, en leur qualité d'organes de contrôle de la banque de données commune FTF, qu'ils doivent être informés systématiquement et spontanément de chaque incident de sécurité.

VI.2.2.5.2. Vérifications menées auprès du gestionnaire de la banque de données

Suite à différentes vérifications effectuées auprès de la Police fédérale, en sa qualité de gestionnaire de la banque de données FTF[113], le C.O.C. et le Comité permanent ont pu constater avec satisfaction que le guide d'utilisation de la banque de données FTF avait été mis à jour. Le C.O.C. et le Comité permanent R insistent sur le fait qu'à côté de cet indispensable outil, des formations et des mises à niveau des utilisateurs doivent être organisées à l'initiative des conseillers en sécurité et en protection de la vie privée désignés.

Le C.O.C. et le Comité permanent R ont par ailleurs eu communication de la liste de l'ensemble des personnes accédant à la banque de données FTF (1506 personnes au 14 avril 2017), ainsi que des loggings (historique des accès) aux dates choisies (*supra*).

Enfin, la Police fédérale a fourni une explication sur l'incident de sécurité résultant d'une information insérée par erreur dans la banque de données.

VI.2.2.6. La non-désignation d'un conseiller en sécurité et en protection de la vie privée de la banque de données FTF

Chaque service utilisateur a désigné un conseiller en sécurité et en protection de la vie privée (dont la compétence est limitée au service en question).

Cependant, fin 2017, les responsables de traitement (les ministres de la Justice et de l'Intérieur) n'avaient toujours pas désigné le conseiller en sécurité pour la banque de données FTF. Ses attributions sont pourtant cruciales.[114]

Le C.O.C. et le Comité permanent R avaient toutefois adressé en 2017 deux courriers à cet égard aux responsables de traitement (les ministres de la Justice et

---

112 L'Office des étrangers a signalé avoir pris des initiatives en matière de sécurité de l'information, c'est-à-dire le développement d'une formation spécifique et d'une application gérant les accès grâce à une authentification via e-ID. Le C.O.C. et le Comité permanent R appuient et encouragent ces initiatives.

113 Art. 3 A.R. FTF.

114 Voir les articles 44/3 § 1er/1 LFP & 5 AR FTF.

de l'Intérieur). Ces courriers complétaient les interpellations formulées précédemment dans les avis communs.[115]

VI.2.2.7. Deux nouveaux traitements : home-grown terrorist fighters et prédicateurs de haine

En marge de leur enquête portant sur la banque de données commune FTF, le C.O.C. et le Comité permanent R ont constaté le traitement d'entités qui étaient reprises dans la liste dénommée *Joint Information Box* (JIB)[116], c'est-à-dire la liste (gérée par l'OCAM) des personnes et des organisations qui jouent un rôle clé dans le processus de radicalisation.[117]

En outre, un autre nouveau traitement, dénommé *home-grown terrorist fighters* (HTF), a été créé.[118] Celui-ci vise à recenser les personnes qui ont des velléités terroristes en Belgique et qui, à la différence des *foreign terrorist fighters*, n'avaient eu aucune volonté de se rendre dans une zone de combat djihadiste ou n'ont pas l'intention de s'y rendre dans le futur.

Ces nouveaux traitements font suite à une demande expresse des ministres de la Justice et de l'Intérieur. Sans mettre en doute l'opportunité ni l'utilité opérationnelle de tels traitements supplémentaires[119], le C.O.C. et le Comité permanent R ont attiré l'attention sur le fait qu'ils avaient débuté en l'absence d'Arrêté royal et de déclaration préalable.

Le C.O.C. et le Comité permanent R ont signalé cette situation aux ministres de la Justice et de l'Intérieur.

VI.3. LA FONCTION D'AVIS

VI.3.1. UNE 'DÉCLARATION PRÉALABLE COMPLÉMENTAIRE'

Par courrier du 22 juin 2017, les ministres de l'Intérieur et de la Justice ont adressé une 'déclaration préalable complémentaire' de la banque de données FTF aux Présidents du C.O.C. et du Comité permanent R.

Cette déclaration visait à compléter la déclaration initiale à propos des modalités d'accès direct à la banque de données FTF pour les Maisons de justice (plus précisément : l'Administration générale des Maisons de Justice de la

115 Voir l'avis commun 1/2016 du 20 juin 2016 (point 10) et l'avis commun 2/2016 du 1er décembre 2016 (point 10), COMITÉ PERMANENT R, *Rapport d'activités 2016*, 216-227.

116 Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2015*, 7-11.

117 Il s'agissait de 72 entités au 13 novembre 2017.

118 Il s'agissait de 30 entités au 13 novembre 2017.

119 Voir à ce propos les points 7 et 8 de l'avis commun n°01/2016 du 20 juin 2016, dans : COMITÉ PERMANENT R, *Rapport d'activités 2016*, 216 et suiv.

Fédération Wallonie-Bruxelles, le Département Maison de Justice du Ministère de la Communauté Germanophone et l'*'Afdeling Justitiehuizen van de administratieve diensten van de Vlaamse overheid, beleidsdomein Welzijn, Volksgezondheid en Gezin*[120]').

Pour ces services, la réglementation limite leur accès direct aux données à caractère personnel des *foreign terrorist fighters* pour lesquels le service doit assurer sa mission d'accompagnement judiciaire et de surveillance (article 7 § 1er, al. 6 AR FTF). Corollairement à leur accès direct (limité), ces services ont l'obligation d'alimenter la banque de données FTF (articles 44/11/3*ter* §§ 4 et 5 LFP et 7 § 1er, al. 5 AR FTF).

La déclaration complémentaire ajoutait essentiellement, pour chacun des services en question, des explications et des précisions quant à l'identité des conseillers en sécurité, l'identification des personnes bénéficiant de l'accès direct et la description du système de validation des données.

VI.3.2. UN AVIS COMMUN

Conformément à l'article 44/11/3*bis* § 3 LFP, le C.O.C. et le Comité permanent R ont rendu un avis commun le 20 juillet 2017.[121]

En résumé, le C.O.C. et le Comité permanent R :

- relevaient que la déclaration préalable complémentaire ne faisait (toujours) pas mention du conseiller en protection de la vie privée qui doit être désigné par les ministres de l'Intérieur et de la Justice, nonobstant les précédentes observations formulées à ce propos. Dans leur courrier du 22 juin 2017, les ministres annonçaient une 'désignation urgente' de cette personne ;
- insistaient, concernant les types d'accès, sur le fait que le *need to share* – souligné à juste titre par la Commission d'enquête 'Attentats'[122] – ne porte aucunement préjudice au principe du *need to know*. En d'autres termes, les accès doivent être régulés, de sorte que le nécessaire *need to share* n'évolue pas *de facto* vers le *nice to know* ;
- rappelaient qu'il était indispensable, dans le cadre de leur mission de contrôle, de pouvoir disposer d'un historique des fiches de renseignement de manière à pouvoir en déterminer le contenu à un moment choisi. Dans le courrier d'accompagnement, les Ministres précisaient qu'une solution technique était recherchée par la Police fédérale (chargée de la gestion technique et fonctionnelle de la banque de données FTF) à ce propos ;

120 Division des Maisons de Justice des services administratifs de l'Autorité flamande, domaine de la politique du Bien-être, de la Santé Publique et de la Famille (traduction libre).

121 L'avis peut être consulté sur www.comiteri.be.

122 *Doc. parl.*, Chambre 2016-17, 54-1752/8, 166.

– exhortaient les services concernés, dans l'élaboration de leur système interne de validation, à pouvoir démontrer (au moyen de la production d'un document) que les données à caractère personnel et les informations qu'ils introduisent sont adéquates, pertinentes et non excessives à la lumière des objectifs et des finalités de la banque de données FTF.

CHAPITRE VII
AVIS

L'article 33, alinéa 7, L. Contrôle stipule que le Comité '*ne peut rendre un avis sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant les orientations politiques des ministres compétents, qu'à la demande de la Chambre des représentants ou du Ministre compétent.*' Le Comité doit également rendre des avis dans le cadre de la réglementation légale relative aux banques de données communes, et ce, conjointement avec l'Organe de contrôle de l'information policière (C.O.C.). Cette compétence d'avis est traitée au Chapitre VI.

En 2017, le Comité a été sollicité à trois reprises par le Parlement et à deux reprises par le ministre de la Justice. L'avis demandé par la Commission de l'Intérieur dans le cadre du Projet de loi portant modification de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité a été développé dans le Chapitre X.2.3, puisqu'il est associé au fonctionnement de l'Organe de recours.

VII.1. AVIS RELATIF AU PROJET DE LOI MODIFIANT LA LOI DU 30 NOVEMBRE 1998

En février 2016, le ministre de la Justice a demandé au Comité permanent R de rendre un avis concernant l'avant-projet de loi modifiant la Loi organique des services de renseignement et de sécurité du 30 novembre 1998.[123, 124] Dans le cadre de la discussion sur le projet à la Chambre des Représentants, un avis similaire[125] a été transmis, début 2017, à la Commission Justice de la Chambre.

Dans son avis, le Comité permanent R a recommandé, de manière générale, de spécifier les propositions de modification au regard de la finalité, et dans certains cas, de régler ces propositions plus en détail dans le projet. En outre, une réflexion plus approfondie devait être menée sur certaines options fondamentales.

---

123 Cet avis a déjà été repris intégralement dans le *Rapport d'activités 2016*, 207-215.

124 Entre-temps, la Loi du 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal (*M.B.* 8 mai 2017) est entrée en vigueur.

125 L'avis peut être consulté sur www.comiteri.be.

Et le Comité de préconiser que le contrôle soit porté au niveau adéquat afin de conserver un équilibre entre les possibilités des services et celles des organes de contrôle. Ces considérations devaient impérativement s'inscrire dans le cadre des exigences fondamentales, comme celles qui découlent des normes légales nationales et internationales. Le Comité insistait sur le fait que le projet élargi contenait de nombreux éléments positifs, que ce soit du point de vue légistique ou du point de vue des besoins opérationnels des deux services de renseignement.

VII.2. AVIS SUR LE PROJET DE LOI PORTANT MODIFICATION DE LA LOI RELATIVE À LA CLASSIFICATION ET AUX HABILITATIONS, ATTESTATIONS ET AVIS DE SÉCURITÉ

Le 1er décembre 2017, le Président de la Commission de l'Intérieur des Affaires générales et de la Fonction publique a demandé au Comité permanent R de rendre un avis sur le projet de loi portant modification de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.[126]

Le Comité a souligné au préalable qu'il n'était nulle part fait référence aux répercussions éventuelles/inévitables sur la charge de travail de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité.

Le Comité a formulé toute une série de remarques et de préoccupations. Une réponse appropriée du législateur s'imposait afin d'éviter toute insécurité juridique dans une matière de cette importance, qui se situe à l'intersection de la sécurité et des droits des citoyens.

Le Comité a insisté sur le fait que le projet n'apportait pas de réponse à de nombreux problèmes découlant de l'application de la réglementation actuelle (complexité, délais de recours beaucoup trop courts…), tant pour les administrations et les citoyens concernés que pour l'Organe de recours. Des propositions avaient déjà été formulées pour remédier à certains de ces problèmes. Non seulement le projet de loi ne les traitait pas, mais il créait inévitablement des problèmes supplémentaires pour tous les acteurs. Par conséquent, le Comité a estimé qu'il serait indiqué de réformer de manière cohérente la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité *et* la Loi du 11 décembre 1998 portant création de l'Organe de recours.

---

126 Vu, d'une part, les délais de réponse extrêmement serrés (l'avis était attendu pour le 15 décembre 2017), et d'autre part, vu l'étendue et la complexité des modifications proposées, le Comité n'a pas été en mesure d'examiner en détail tous les aspects de ce projet. Il n'a pas pu non plus effectuer un contrôle légistique ni élaborer des propositions de texte alternatives. L'avis peut être consulté sur www.comiteri.be.

VII.3. AVIS SUR L'AVANT-PROJET DE LOI RELATIF À L'UTILISATION DE CAMÉRAS

En 2017, le Comité permanent R a également rendu un avis au ministre de la Justice concernant l' 'Avant-projet de loi modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance et la loi du 30 novembre 1998 organique des services de renseignement et de sécurité'.[127]

Le Comité s'est tout d'abord interrogé sur la nécessité de ce projet (ou du moins de certains de ses aspects) et a attiré l'attention sur la complexité de la réglementation proposée. De plus, le Comité a examiné en détail la proposition d'article 16/4 § 1er L.R&S (la possibilité d'accéder directement à des informations et à des données à caractère personnel qui sont collectées au moyen de caméras utilisées par les services de police), la proposition d'article 16/4 § 2 L.R&S (la possibilité d'accéder *a posteriori* à des données collectées, dont le contrôle prévu n'est pas, selon le Comité, proportionnel au caractère potentiellement intrusif de la méthode proposée), la proposition d'article 16/4 § 4 L.R&S (qui introduit une nouvelle possibilité de grande portée pour les services de renseignement sous la forme de datamining (exploration de données), qui permettrait que les/tous les targets (connus ou potentiels) des services de renseignement puissent être automatiquement comparés aux données disponibles dans les banques de données techniques) et, enfin, la proposition d'article 16/4 § 6 L.R&S (où le Comité se demandait si le secret de l'enquête ne pourrait plus être invoqué à l'égard des services de renseignement qui souhaitent consulter des images provenant de caméras).

VII.4. AVIS SUR UNE RÉGLEMENTATION RELATIVE À UNE MÉTHODE DE RENSEIGNEMENT PERMETTANT AUX SOURCES HUMAINES DE COMMETTRE DES INFRACTIONS

À la mi-décembre 2017, le Comité permanent R a rendu un avis[128] demandé par le ministre de la Justice concernant '*een wettelijke regeling voor een inlichtingenmethode voor het machtigen van menselijke bronnen tot het plegen van misdrijven in de Wet van 30 november 1998 houdende de inlichtingen- en veiligheidsdiensten*'.[129]

127 L'avis peut être consulté sur www.comiteri.be.

128 L'avis peut être consulté sur www.comiteri.be.

129 Une réglementation légale à inscrire dans la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité concernant une méthode de renseignement visant à autoriser des sources humaines à commettre des infractions (traduction libre).

Dans cet avis, le Comité faisait remarquer qu'avant de prévoir la possibilité pour des informateurs de commettre des infractions, l'obligation légale d'émettre une directive sur le fonctionnement des sources humaines, devait être une priorité.[130]

En ce qui concerne la possibilité de commettre des infractions, le Comité estimait qu'aucun rôle ne devait être attribué au Parquet fédéral, mais bien à la Commission BIM et, au vu de l'importance de la matière, au Comité permanent R.

Quant à l'élaboration de la réglementation, il convient tout d'abord de déterminer la ou les finalité(s) de la commission d'infractions. Si la raison principale est que cela doit permettre aux services de 'conserver leur position d'information', la possibilité prévue à l'article 13/1 L.R&S peut être envisagée. Dans ce cas, l'autorisation est, en effet, plutôt une 'mesure de protection ou d'appui'. Mais dans ce cas de figure, il faut prévoir une intervention du Comité permanent R. Toutefois, si l'idée sous-jacente est (aussi) que les informateurs puissent commettre des infractions pour obtenir certains renseignements (par exemple subtiliser des documents), le Comité est d'avis qu'il s'agit d'une méthode spécifique, ce qui implique que tant la Commission BIM que le Comité permanent R peuvent intervenir.

Par ailleurs, le Comité estimait qu'il fallait envisager de définir explicitement dans la loi que les méthodes particulières de renseignement peuvent être utilisées pour vérifier la fiabilité d'informateurs qui procèdent à des infiltrations à la demande des services de renseignement, et qui, le cas échéant, sont autorisés à commettre des infractions.

130 Cette obligation est inscrite depuis 2010 à l'article 18 L.R&S.

CHAPITRE VIII
LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Parallèlement aux enquêtes de contrôle, le Service d'Enquêtes R du Comité 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.[131] 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 infractions 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. La raison en est évidente : l'organe de contrôle est avant tout à la disposition du Parlement. Cette mission pourrait être mise en péril si trop de temps devait être investi dans les dossiers judiciaires. Le Président peut, le cas échéant, se concerter avec les autorités judiciaires quant à la participation des membres du Service d'Enquêtes R à des enquêtes pénales (art. 61*bis* L.Contrôle).

Quand le Service d'Enquêtes R effectue des enquêtes pénales, le Directeur doit remettre un rapport au Comité permanent R au terme de celles-ci. 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).

---

131 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, Antwerpen, 2013, 295-305.

En 2017 également, le Service d'Enquêtes R a effectué des devoirs d'enquête dans le cadre d'informations judiciaires. Le premier dossier concernait une enquête menée pour le compte des autorités judiciaires de Bruxelles sur l'utilisation potentiellement frauduleuse d'une carte de service par un membre d'un service de renseignement. La seconde information a été effectuée sur réquisition du Parquet fédéral et portait sur l'éventuelle implication d'un membre d'un service de renseignement dans un délit ou un crime contre la sûreté intérieure et extérieure de l'État.

Par ailleurs, l'article 50 L. Contrôle dispose que *'[t]out membre d'un service de police qui constate un crime ou un délit commis par un membre d'un service de renseignements rédige un rapport d'information et le communique dans les quinze jours au chef du Service d'enquêtes R*'. En 2017, le Service d'Enquêtes a reçu deux signalements de ce genre.

CHAPITRE IX
EXPERTISE ET CONTACTS EXTERNES

IX.1. EXPERT DANS DIVERS FORUMS

En 2017, 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. Dans le courant de l'année 2017, le BISC a organisé deux journées d'étude sur les thèmes suivants : 'Managing uncertainties. The protection of critical infrastructures and intelligence services' et 'Counter insurgency – Terrorisme and the role of intelligence services'. Le Président du Comité en a assuré l'ouverture ;
- Fin janvier 2017, le Greffier a participé, sur invitation de la *European Union Agency for Fundamental Rights* (FRA), au panel de discussion 'Enforcing the right to remedy in cases of surveillance : a human right challenge' lors de la '10th International Conference on Computers, Privacy and Data Protection' à Bruxelles ;
- En février 2017, le Comité permanent R a participé à la troisième réunion d'experts 'National intelligence authorities and surveillance in the EU : Fundamental rights safeguards and remedies', organisée à l'initiative du Directeur du *Sector of Information Society, Privacy and Data Protection Freedoms and Justice Department* de la *European Union Agency for Fundamental Rights* (FRA).[132] Les résultats de cette enquête menée par des experts ont été discutés, et un projet de rapport[133] a été présenté ;

---

[132] 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). Missionnée par le Parlement européenne dans la foulée de l'adoption de la Résolution du 12 mars 2014, FRA est chargée de réaliser une étude comparative sur le contrôle démocratique des services de renseignement dans les États membres de l'Union.

[133] Ce projet a donné lieu à la publication, en octobre 2017, de FRA, *Surveillance by intelligence services : fundamental rights safeguards and remedies in the EU. Volume II : field perspectives and legal update*, Luxembourg, 2017, 164 p.

- Le Greffier du Comité permanent R a été invité 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) ;
- En mars, le Comité permanent R a été l'interlocuteur de la *Stiftung Neue Verantwortung* lors d'un échange de vues autour des 'New challenges and changes to democratic control of intelligence in Belgium and Germany' ;
- Dans le cadre de la conférence RightsCon organisée à Bruxelles en mars 2017, le Greffier a pris part au panel de discussion 'Surveying Surveillance in the EU' ;
- À l'invitation du *Geneva Centre for the Democratic Control of Armed Forces* (DCAF), le Président et le Greffier du Comité ont participé, fin avril 2017, en Tunisie, à une table ronde sur *'Les lois qui régissent le renseignement – Droit comparés'*. Le Président du Comité est intervenu dans le même contexte, en novembre 2017 à Tunis, lors de la session intitulée 'Redevabilité et protection des données personnelles' dans le cadre de la table-ronde 'Cybersécurité – Expériences internationales et Droits comparés' ;
- Le Comité a été sollicité pour son expertise lors d'un séminaire pratique destiné à la police, à la magistrature et au barreau autour du thème 'classification et habilitations de sécurité' ;
- En octobre 2017, le Comité permanent R a été impliqué dans une formation dispensée par le DCAF sur le 'Monitoring Law Enforcement and Intelligence Services in Georgia – Status, Needs and International Best Practices' (Tbilissi, Géorgie) ;
- En octobre 2017, le Comité permanent R a collaboré à l'enquête menée par *Privacy International* (UK) et La Ligue des Droits de l'Homme (B) concernant l''Oversight of intelligence sharing between your government and foreign governements' ;
- Le Greffier du Comité permanent R a participé, en novembre 2017, à l''Expert Roundtable on Intelligence Oversight in the framework of the DCAF Assistance Program for the Parliament of the Republic of Macedonia' sur 'The Accountability of Electronic Interception of Communication'. L'accent y a été mis, entre autres, sur un 'Parliamentary Handbook on Inspection Visits' ;
- En 2017, le Président a fait un exposé sur *'Le renseignement, ses défis et son contrôle'* en *'Le contrôle parlementaire'*, à la demande du Département de Sciences Politiques de la Faculté de Droit de l'Université de Liège.

IX.2. PROTOCOLE DE COOPÉRATION 'DROITS DE L'HOMME'

La Belgique œuvre depuis des années à la création d'un Institut national des droits de l'homme. Il s'agit d'un engagement qui a été pris lors de la signature du Protocole dans le cadre de la convention des Nations Unies contre la torture.

L'instauration effective d'un tel institut n'a pu être approuvée qu'après la ratification du protocole par le Parlement fédéral, mais aussi par toutes les entités fédérées. Entre-temps, les actes d'assentiment des Communautés flamande, Wallonie-Bruxelles et germanophone, ainsi que de la Région wallonne, sont parus au Moniteur, et l'acte de l'Assemblée réunie de la Commission communautaire commune a été publié. Seule la loi d'assentiment fédérale manque encore à l'appel.

En attendant l'instauration de l'institut, les réunions de différentes institutions dotées d'un mandat en matière de droits de l'homme[134] ont donné lieu, en janvier 2015, à la conclusion d'un protocole de coopération.[135] Les instances participantes s'y sont accordées pour échanger des pratiques et des méthodes, pour examiner des questions communes et pour promouvoir la coopération mutuelle.

En 2017, les activités de cette plateforme se sont traduites par l'organisation de réunions de concertation mensuelles, lors desquelles ont été abordés tant les problématiques générales (p. ex. la Belgique et la promotion et la protection des droits de l'homme, les efforts visant à contribuer au renforcement de l'infrastructure des droits de l'homme, le secret professionnel et la nouvelle loi relative aux étrangers qui représentent un danger pour la société…) que l'échange de procédés et de méthodologies sur des dossiers individuels concrets. Unia a repris la présidence annuelle en 2017, succédant ainsi à la Commission Vie privée.

IX.3. UNE INITIATIVE MULTINATIONALE EN MATIÈRE D'ÉCHANGE D'INFORMATIONS

Depuis 2015, des organes de contrôle indépendants issus de cinq pays européens effectuent simultanément, mais chacun dans le cadre de son mandat et de ses compétences, une enquête sur l'échange international de données à caractère personnel dans le cadre de la lutte contre les FTF. Il s'agit de la Belgique, du Danemark, des Pays-Bas, de la Norvège et de la Suisse.[136] L'objectif est d'aboutir à un rapport commun.

En 2017, divers projets de textes ont été échangés. De plus, deux réunions d'experts ont eu lieu à l'invitation de l'EOS norvégien. Elles ont donné lieu à un premier projet de document commun qui a servi de base aux discussions.

---

134 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 R et P.

135 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.

136 Voir COMITÉ PERMANENT R, *Rapport d'activités 2015*, 80-81.

IX.4. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

Le Comité permanent R entretient des contacts étroits avec plusieurs organismes français : la Délégation parlementaire au renseignement (DPR), la Commission nationale de contrôle des interceptions de sécurité (CNCIS) et la Commission nationale de contrôle des techniques de renseignement (CNCTR), qui a été instaurée récemment. Un colloque organisé à l'Assemblée nationale française en mars 2017, auquel le Comité était représenté, a été l'occasion de renforcer ces relations.

Les 27 et 28 novembre 2017, le Comité a reçu le nouvel organe de contrôle suisse *Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten* (Autorité de surveillance indépendante des activités de renseignement), qu'il avait invité à effectuer une visite à Bruxelles.

Le nouvel ambassadeur du Canada a été reçu par le Président du Comité permanent R pour une visite de courtoisie. En outre, des informations ont été échangées avec l'organe de contrôle canadien sur les changements imminents dans le paysage du contrôle des services de renseignement canadiens, en particulier la création de *l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*.

En novembre 2017, l'*International Intelligence Oversight Forum* a été organisé à Bruxelles par le *Special Rapporteur for Privacy* (SRP) des Nations Unies. Y ont participé des représentants des organes de contrôle, mais aussi des services de renseignement, des universités et des ONG. En 2017, le thème était 'The Road Ahead – Dilemmas and Best Practices in Democratic Intelligence Oversight'. Une délégation du Comité permanent R a noué des contacts informels avec des organes de contrôle des Pays-Bas, de la France, du Royaume-Uni, d'Allemagne, de Norvège… Ce forum visait à améliorer, en toute confidentialité, la compréhension des défis auxquels, entre autres, les organes de contrôle démocratiques sont confrontés dans un monde numérique.

Enfin, des contacts ont été établis en vue de préparer la visite à Bruxelles, courant 2018, de l'*Office of the Personal Data Protection Inspector* géorgien et de représentants du parlement géorgien.

IX.5. 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 contrôle la légalité, la légitimité et l'efficacité de toutes les dépenses, y compris, en principe, de toutes les dépenses des services de renseignement. Cependant, vu le 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. C'est un représentant du Cabinet du ministre de la Défense qui effectue 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. En 2017 également, le contrôle a été effectué en sa présence.

IX.6. 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	Organe de presse
12 janvier 2017	'Comité I bundelt aanwijzingen tegen Oussama Atar voor commissie aanslagen 22 maart'	De Morgen
25 janvier 2017	'Kazachgate : Chodiev est devenu belge alors que la Sûreté connaissait ses liens avec la mafia, dit le Comité R'	La Libre Belgique
25 janvier 2017	'La Sûreté ne s'est pas opposée à la naturalisation de Chodiev qu'elle savait mafieux'	Le Vif
29 mars 2017	'Kazachgate zorgt voor spanningen bij Staatsveiligheid'	Knack
29 mars 2017	'Kazachgate : Comité I ziet geen elementen die aantijgingen in anonieme brief ondersteunen'	nl.metrotime.be
12 juillet 2017	'Geldgebrek belemmert waakhond Staatsveiligheid'	De Standaard
17 octobre 2017	'Attentats à Bruxelles : le service de renseignement militaire pointé du doigt dans le rapport du Comité R'	rtbf.be
18 octobre 2017	'Jaarverslag Comité I 'Inlichtingendiensten lieten steken vallen vóór 2017''	De Standaard

CHAPITRE X
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 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 administratives 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.[137]

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. Il met à disposition non seulement son Président et son Greffier, mais aussi le personnel administratif requis, qui veille à la préparation, au traitement et au suivi des recours. Ces processus prennent beaucoup de temps.

X.1. UNE PROCÉDURE PARFOIS LOURDE ET COMPLEXE

Tant le greffe que l'Organe de recours sont confrontés à une charge de travail croissante. En effet, les dossiers ne cessent de se complexifier du point de vue de la gestion administrative, des audiences et des décisions.

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

Ainsi, de nombreux envois ne respectent pas les articles 2 et 3 de l'AR Org. recours, qui stipulent respectivement que '*l'envoi à l'organe de recours de toutes pièces de procédure se fait sous pli recommandé à la poste*' et que '*le recours est signé et daté par le requérant ou par son avocat*'. Le Greffier se voit dès lors contraint d'interpeller le requérant afin de régulariser la situation dans le délai légal.[138] Il en va de même pour les dossiers administratifs transmis par les différentes autorités de sécurité, qui ne sont pas toujours complets. Dans ce cas, le greffe doit également effectuer des démarches supplémentaires pour y remédier. Dans le même sens, l'application de l'article 5 § 3 L. Org.recours se révèle problématique : la demande de soustraire certaines pièces au regard du requérant lorsqu'il consulte son dossier est rarement motivée correctement ou émane d'une autorité qui n'est pas légalement compétente en la matière, ce qui oblige parfois le greffe, ici aussi, à recueillir des informations complémentaires.[139]

Ces difficultés ont amené l'Organe de recours à adresser un courrier aux différentes autorités de sécurité concernant la motivation des décisions (et les notifications de celles-ci aux personnes intéressées), la composition des dossiers ainsi que la (motivation de la) demande de soustraction de certaines pièces à la consultation des requérants. L'objectif de l'Organe de recours était de rappeler les principes légaux concernant les différentes possibilités (de demandes) d'embargo portant sur des informations sensibles, de manière à ce que les droits de la défense puissent s'exercer au mieux dans cette matière complexe dans laquelle des intérêts de sécurité nationale sont parfois en jeu. Cette démarche n'a toutefois pas eu l'effet escompté auprès de toutes les autorités de sécurité. L'invocation de motifs non prévus par loi pour imposer un embargo sur la consultation demeure problématique. En outre, plusieurs autorités de sécurité considèrent toujours que pour la seule raison de leur classification, des documents ne peuvent être vus par le requérant ou par son avocat, ce qui est contraire à l'esprit et à la lettre de la loi. Par ailleurs, il y a lieu de constater que, dans leurs décisions, les diverses autorités de sécurité ne respectent pas toujours les principes minimaux de droit administratif. Ainsi, il y a notamment des décisions ne comportant pas la moindre motivation et des décisions dépourvues de dates ou de l'identité du fonctionnaire qui les a adoptées.

---

138 Compte tenu de la brièveté des délais, le recours est souvent tardif et donc irrecevable dans ces cas.

139 L'article 5 § 3 L.Org.recours permet à l'Organe de recours, à la demande d'un service de renseignement ou d'un service de police, de décider de soustraire certaines pièces à la consultation du requérant (ou de son avocat) lorsque leur divulgation porterait préjudice à la protection des sources, à la vie privée de tiers ou à l'accomplissement des missions légales des services de renseignement. Par le biais de la loi du 21 avril 2016 (*M.B.* 29 avril 2016), le législateur a élargi cette possibilité en autorisant l'Organe de recours, toujours à la demande du service concerné, à décider de soustraire du dossier les pièces qui relèvent du secret de l'information ou de l'instruction judiciaire. L'Organe de recours a mandaté le Président du Comité permanent R pour statuer sur ces demandes. Dans des cas exceptionnels, le Président a soustrait d'office des éléments relatifs à la vie privée de tiers. Il s'agissait de cas où le service concerné avait manifestement omis d'invoquer l'article 5 § 3 L. Organe de recours.

Par ailleurs, 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 (voire deux) avocat(s) qui expose(nt) la position de son (leur) client à l'audience. La complexité de certains dossiers nécessite beaucoup de temps. Enfin, de nombreux dossiers 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 des informations complémentaires.

Le processus de décision requiert lui aussi davantage de temps qu'il y a plusieurs années, et ce, pour deux raisons majeures. D'une part, le nombre toujours plus élevé 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. En outre, il arrive que des mesures de sécurité spécifiques doivent être prises.

La complexité croissante des dossiers et leur augmentation ont conduit le Comité permanent R à renforcer son administration. Un juriste et une assistante administrative ont en effet été recrutés début 2017, ce qui a eu inévitablement un impact important sur les moyens du Comité.

X.2. UN PROJET DE LOI ET UN AVIS

X.2.1. LE PROJET DE LOI

Divers éléments laissent supposer que la charge de travail de l'Organe de recours va encore (sensiblement) s'accroître dans le futur. Après les attentats de Paris et de Bruxelles, le gouvernement avait annoncé son intention d'augmenter les contrôles de moralité (screenings), en particulier dans l'optique de renforcer la sécurité des infrastructures critiques.

Cette intention s'est concrétisée fin 2017 par le dépôt d'un projet de loi[140] visant à modifier la L.C&HS. Le Président de la Commission de l'Intérieur, des Affaires générales et de la Fonction publique a demandé au Président du Comité permanent R de rendre un avis à propos ce projet de loi.[141] Les trois axes principaux du projet de loi sont résumés ci-après.

140 *Doc. parl.*, Chambre 2017-2018, n°54-2767/1.
141 L'avis peut être consulté sur www.comiteri.be.

X.2.2. LES PRINCIPAUX AXES DU PROJET DE LOI[142]

X.2.2.1. La compétence et le rôle de l'officier de sécurité

Le projet vise tout d'abord à l'élargissement de la fonction d'officier de sécurité dans le cadre des vérifications de sécurité (attestations et avis de sécurité) et à l'instauration de cette fonction au sein du Ministère public.

L'officier de sécurité se voit attribuer la compétence nouvelle de '*veiller à l'observation des règles de sécurité dans le cadre d'un avis de sécurité ou d'une attestation de sécurité*' au niveau de la personne morale de droit public ou de droit privé concernée.

X.2.2.2. La réforme de la procédure d'avis de sécurité

Le projet tend notamment à réformer la procédure d'avis de sécurité, que ce soit au niveau de la décision réglementaire de l'autorité administrative ou du mécanisme de décision individuelle.

Au niveau de la décision réglementaire, le nouveau système prévoit qu'il appartient au Roi de déterminer les secteurs d'activités soumis à l'application de l'avis de sécurité ainsi que les autorités administratives (sectorielles) compétentes.[143] Les personnes morales de droit privé ou public relevant du secteur concerné réalisent ensuite, d'initiative ou à la demande de l'autorité administrative compétente, une 'analyse de risques' qui est transmise à cette dernière. L'autorité administrative demande alors une 'analyse' spécifique 'de la menace' 'aux services compétents'. Dès réception de cette analyse, l'autorité administrative compétente réalise alors une 'analyse d'impact' visant identifier les dommages potentiels aux intérêts majeurs de l'État. Sur base des analyses précitées, l'autorité administrative transmet un dossier de demande de vérification de sécurité à l'ANS. Celle-ci décide en dernier ressort si des vérifications peuvent être ou non effectuées.

S'agissant du mécanisme de décision individuelle, le projet prévoit que les personnes morales doivent informer la personne concernée de l'obligation de se soumettre à une vérification de sécurité. L'officier de sécurité des personnes morales doit au préalable recueillir le consentement de la personne concernée. L'officier de sécurité de l'autorité administrative compétente doit veiller à la conformité des demandes de vérification. Il les transmet à son tour à l'ANS, qui

---

142 Ce projet a été adopté début 2018 : Loi du 23 février 2018 portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (*M.B.* 1er juin 2018). Le présent rapport se référant à l'année 2017, il maintient l'utilisation du terme 'projet'.

143 Il s'agit là d'une différence notable par rapport au système initial des avis de sécurité dans lequel 'une' (n'importe quelle) autorité administrative pouvait initier la procédure.

statue dans le délai prescrit (maximum un mois). À défaut, elle peut être mise en demeure de statuer dans un délai minimum équivalent au délai prescrit initialement. Si ce n'est pas le cas, l'avis est réputé positif. Le projet prévoit que l'avis est délivré pour une durée maximum de cinq ans[144], sous réserve d'une réévaluation spontanée par l'ANS (sur base de nouveaux éléments). L'autorité administrative informe l'officier de sécurité de l'employeur de l'avis de sécurité. S'il est négatif, l'autorité administrative le notifie par pli recommandé à la personne concernée, à l'exception des motifs dont la divulgation serait susceptible de nuire à l'un des intérêts fondamentaux énoncés par la loi, à la protection des sources, au secret d'une information ou d'une instruction judiciaire ou à la protection de la vie privée de tiers.[145]

X.2.2.3. Le contenu de la vérification de sécurité

Le dernier axe principal du projet de loi consiste à modifier la disposition régissant le contenu de la vérification de sécurité (art. 22*sexies* L.C.&HS), et ce, avec un triple objectif.

Tout d'abord, il vise à permettre la réalisation de la vérification de sécurité concernant des personnes mineures ainsi que, dans le cadre de vérifications de sécurité concernant des personnes majeures, la prise en compte de faits commis durant leur minorité.

Le projet permet en outre aux services de police et de renseignement[146] de solliciter des informations auprès de leurs homologues étrangers, lorsque la personne pour laquelle la vérification de sécurité est requise réside ou a résidé, a transité ou a séjourné à l'étranger.

Enfin, le projet étend les banques de données analysées. L'article 22*sexies* L.C.&HS prévoyait déjà la consultation et l'évaluation des données judiciaires[147], des informations des services de renseignement, du casier judiciaire central, du casier judiciaire et des registres de la population et des étrangers tenus par les communes, du registre national, du registre d'attente des étrangers ainsi que des données policières accessibles aux fonctionnaires de police lors de l'exécution d'un contrôle d'identité. Le projet y ajoute les données et les informations des banques de données policières internationales résultant de traités liant la Belgique, les données de police administrative, les données contenues dans les banques de données communes et d''*autres données et informations*'. Le projet

144 Il s'agit ici aussi d'une différence avec la réglementation en vigueur actuellement puisque celle-ci ne prévoit pas de 'durée de validité maximale'. En outre, jusqu'à présent, la réalisation de l'avis de sécurité devait avoir lieu 'préalablement' à l'exercice d'une profession, d'une fonction, d'une mission ou d'un mandat. Le projet introduit la possibilité de soumettre à une vérification de sécurité des personnes qui sont déjà en fonction.

145 Voir art. 22, al. 5 L.C&HS (inchangé).

146 L'ANS dispose déjà de cette compétence.

147 Communiquées avec l'accord des autorités judiciaires compétentes.

prévoit que le caractère adéquat, pertinent et non excessif de ces nouvelles données et informations, ainsi que la liste de celles-ci, doivent être déterminés par Arrêté royal.[148]

X.2.3. L'AVIS DU COMITÉ PERMANENT R[149]

Dans son avis, le Comité souligne le fait que le projet n'apporte pas de réponse à de nombreux problèmes générés par l'application de la réglementation actuelle (complexité, délais de recours beaucoup trop courts…), et ce, tant pour les administrations et les citoyens concernés que pour l'Organe de recours.

Le Comité avait précédemment formulé des propositions pour remédier à certains de ces problèmes. Le Comité permanent R relevait que non seulement le projet de loi ne les abordait pas, mais qu'il créait des problèmes supplémentaires pour tous les acteurs. Le Comité estimait qu'il était indiqué de réformer de manière cohérente les deux lois du 11 décembre 1998 (L.C.&HS et L.Org. recours).

X.3. LE DÉTAIL DES CHIFFRES

Cette section reprend 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 cinq dernières années sont également repris.

En 2017, la tendance haussière constatée l'année précédente se confirme. Le nombre de recours passe de 169 à 192, soit le niveau le plus élevé jamais atteint. L'augmentation constatée est particulièrement marquée en ce qui concerne le nombre de recours introduits contre des avis de sécurité négatifs (de 101 à 122), ce qui confirme la tendance constatée en 2016. Cette tendance à la hausse est également visible dans le nombre de recours introduits contre des décisions de refus ou de retrait d'attestations de sécurité (de 18 à 30), tandis que le nombre de recours en matière d' habilitations de sécurité a suivi le mouvement inverse (passant de 50 à 40 recours).

---

148 Cet Arrêté royal est paru dans le courant de l'année 2018 : A.R. du 8 mai 2018 déterminant la liste des données et informations qui peuvent être consultées dans le cadre de l'exécution d'une vérification de sécurité (*M.B.* 1er juin 2018).

149 L'avis peut être consulté sur www.comiteri.be.

Tableau 1. Autorités de sécurité concernées

	2013	2014	2015	2016	2017
Autorité nationale de sécurité	98	99	68	92	129
Sûreté de l'État	1	0	1	0	0
Service Général du Renseignement et de la Sécurité	78	60	47	68	53
Agence fédérale de Contrôle nucléaire	9	8	10	8	7
Police fédérale	1	3	3	1	3
Police locale	2	1	1	0	0
Commission aéroportuaire locale	–	–	–	–	–
TOTAL	**189**	**171**	**130**	**169**	**192**

Tableau 2. Nature des décisions contestées

	2013	2014	2015	2016	2017
Habilitations de sécurité (art. 12 et s. L.C&HS)					
Confidentiel	5	5	9	5	1
Secret	56	43	35	38	33
Très secret	5	4	4	7	6
Refus	41	25	36	28	30
Retrait	5	9	7	9	7
Refus et retrait	4	0	0	0	0
Habilitation pour une durée limitée	1	2	3	4	1
Habilitation pour un niveau inférieur	0	1	0	1	0
Pas de décision dans les délais	15	15	2	7	2
Pas de décision dans les nouveaux délais	0	0	0	1	0
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	**66**	**52**	**48**	**50**	**40**
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)					
Refus	0	4	6	1	3
Retrait	0	0	0	0	0
Pas de décision dans les délais	0	0	0	0	0

Attestations de sécurité lieu ou événement (art. 22*bis*, al.2 L.C&HS)					
Refus	15	16	12	9	20
Retrait	0	0	1	0	0
Pas de décision dans le délai	0	0	0	0	0
Attestations de sécurité lieu secteur nucléaire (art. 8bis L.C&HS)					
Refus	–	–	–	7	7
Retrait	–	–	–	1	0
Pas de décision dans le délai	–	–	–	0	0
Avis de sécurité (art. 22quinquies L.C&HS)					
Avis négatif	106	99	63	101	122
Pas d'avis	2	0	0	0	0
Révocation d'avis positif	0	0	0	0	0
Actes normatifs d'une autorité administrative (art. 12 L. Org.recours)					
Décision d'une autorité publique d'exiger des attestations de sécurité	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des attestations de sécurité	0	0	0	0	0
Décision d'une autorité administrative d'exiger des avis de sécurité	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des avis de sécurité	0	0	0	0	0
SOUS-TOTAL ATTESTATIONS ET AVIS	**123**	**119**	**82**	**119**	**152**
TOTAL DÉCISIONS CONTESTÉES	**189**	**171**	**130**	**169**	**192**

Tableau 3. Nature du requérant

	2013	2014	2015	2016	2017
Fonctionnaire	4	0	4	2	4
Militaire	26	17	29	23	20
Particulier	159	145	93	139	164
Personne morale	0	6	4	5	4

Tableau 4. Langue du requérant

	2013	2014	2015	2016	2017
Français	92	92	75	99	115
Néerlandais	97	76	54	70	77
Allemand	0	0	0	0	0
Autre langue	0	0	1	0	0

Tableau 5. Nature des décisions interlocutoires prises par l'Organe de recours[150]

	2013	2014	2015	2016	2017
Demande du dossier complet (1)	187	168	130	167	191
Demande d'informations complémentaires (2)	12	16	7	23	36
Audition d'un membre d'une autorité (3)	3	11	7	10	0
Décision du président (4)	0	0	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (5)	68	78	50	54	80[156]
Soustraction d'informations du dossier par le service de renseignement (6)	0	0	0	0	0

(1) L'Organe de recours peut demander l'intégralité du dossier 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.

150 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 2017, alors que la décision n'a été rendue qu'en 2018.

151 Voir *supra* à propos de l'art. 5 § 3 L Org. Recours. À noter que dans la plupart des cas, il n'a été fait que partiellement droit à la demande de soustraction d'informations (parfois en raison d'une motivation inadéquate au vu des exceptions légales).

(5) Si le service de renseignement ou de police concerné le demande, l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant.[152]
(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	2016	2017
Consultation du dossier par le requérant et/ou l'avocat	103	84	84	87	105
Audition du requérant (assisté ou non d'un avocat)[158]	138	115	107	127	158

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

	2013	2014	2015	2016	2017
Habilitations de sécurité (art. 12 et s. L.C&HS)					
Recours irrecevable	2	0	4	0	3
Recours sans objet	3	3	3	7	0
Recours non fondé	20	12	19	18	13
Recours fondé (avec octroi partiel ou complet)	35	14	24	24	24
Devoir d'enquête complémentaire par l'autorité	0	0	0	2	0
Délai supplémentaire pour l'autorité	14	12	1	2	1
Sans suite	0	0	1	0	0
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)					
Recours irrecevable	0	0	0	0	1
Recours sans objet	0	0	0	0	1
Recours non fondé	0	2	4	1	0
Recours fondé (avec octroi)	0	0	2	1	1

152 Voir *supra* à propos de l'art. 5 § 3 LOrg. Recours.
153 La L.Org.recours prévoit l'assistance d'un avocat à l'audience mais pas la représentation par ce dernier. À noter que, dans le cadre de certains dossiers, le requérant (assisté ou non de son avocat) est auditionné à plusieurs reprises.

Attestations de sécurité pour lieux ou événements (art. 22*bis*, al.2 L.C&HS)					
Recours irrecevable	1	0	0	0	1
Recours sans objet	0	0	0	0	1
Recours non fondé	6	6	8	2	12
Recours fondé (avec octroi)	11	8	10	4	7
Donne acte de retrait de recours	0	0	2	0	1
Attestations de sécurité pour le secteur nucléaire (art. 8*bis* § 2 L.C&HS)					
Recours irrecevable	–	–	–	1	1
Recours sans objet	–	–	–	1	0
Recours non fondé	–	–	–	0	1
Recours fondé (avec octroi)	–	–	–	7	5
Avis de sécurité (art. 22*quinquies* L.C&HS)					
Organe de recours non compétent	0	4	0	0	20[159]
Recours irrecevable	4	4	6	15	10
Recours sans objet	1	4	0	0	1
Confirmation de l'avis négatif	25	53	28	42	49
Transformation en avis positif	65	41	23	46	41
Donne acte de retrait de recours	0	0	2	0	1
Recours contre des actes normatifs d'une autorité administrative (art. 12 L. Org.recours)	0	0	0	0	0
TOTAL	**187**	**163**	**137**	**173**	**195**

154 Il s'agissait en l'espèce de recours introduits contre des avis de sécurité (négatifs) rendus par l'Autorité nationale de sécurité concernant le personnel de sous-traitants actifs pour les institutions européennes. L'Organe de recours avait décidé que les avis formulés par l'Autorité nationale de sécurité n'avaient pas de base juridique. En conséquence, l'Organe de recours s'était déclaré sans juridiction pour statuer sur le bien-fondé ou non de des avis de sécurité rendus par l'Autorité nationale de sécurité.

CHAPITRE XI
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

XI.1. COMPOSITION DU COMITÉ PERMANENT R

La composition du Comité permanent R n'a subi aucune modification en 2017 : la présidence a été assurée par Guy Rapaille (F), avocat général près la cour d'appel de Liège, et les fonctions de conseiller, par Gérald Vande Walle (F)[155] et Pieter-Alexander De Brock (N).

Deux commissaires auditeurs ont démissionné du Service d'Enquêtes et ont été remplacés respectivement en septembre et octobre 2017. Le service est toujours composé de cinq commissaires auditeurs, dont le Directeur Frank Franceus (N).

Le cadre administratif, placé sous la direction du Greffier Wouter De Ridder (N), a été renforcé par le recrutement d'une secrétaire et d'un juriste, et compte désormais 18 collaborateurs.

XI.2. RÉUNIONS AVEC LA COMMISSION DE SUIVI

Dans le courant de l'année 2017, deux réunions ont eu lieu avec la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de Contrôle des services de renseignement et de sécurité. Les treize membres avec voix délibérative[156] de la Commission étaient les suivants : Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Peter De Roover (N-VA), Laurette Onkelinx (PS), André Frédéric (PS),

---

155 Le Conseiller Gérald Vande Walle a atteint l'âge légal de la retraite le 31 décembre 2017 et a été remplacé, début 2018, par Laurent Van Doren, Commissaire divisionnaire de la police.

156 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').*

Denis Ducarme (MR), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld), Hans Bonte (sp.a), Gilles Vanden Burre (Ecolo-Groen) et Georges Dallemagne (cdH). Le Président de la Chambre Siegfried Bracke (N-VA) a assuré la présidence des réunions de la Commission. En outre, neuf de ces députés ont été désignés, en avril 2016, comme membres permanents de la Commission d'enquête parlementaire 'Attentats'. Les activités parlementaires se sont concentrées sur la Commission d'enquête (cf. Chapitre V.1).

Lors des deux réunions de la Commission, plusieurs enquêtes de contrôle communes du Comité permanent R et du Comité permanent P ont été discutées à huis clos. Les enquêtes clôturées par le Comité permanent R ont elles aussi fait l'objet de discussions, de même que le *Rapport d'activités 2016* du Comité permanent R, en novembre 2017. La Commission a pris *'acte du rapport d'activités 2016 du Comité R et souscrit à ses recommandation*'.[157] Enfin, du temps a été consacré à un échange autour du rapport annuel sur l'application des méthodes spécifiques et exceptionnelles par les services de renseignement et le contrôle exercé sur celles-ci par le Comité permanent R (art. 35 L.Contrôle).

XI.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 (art. 54 L.Contrôle). Ces réunions poursuivent un double objectif : d'une part, échanger des informations, et d'autre part, initier des enquêtes de contrôle communes et discuter des enquêtes en cours.

En 2017, il a été question de deux enquêtes de contrôle communes : l'enquête effectuée sur les attentats de Paris concernant '*la position d'information de l'OCAM sur les individus ou groupes ayant perpétré les attentats de Paris ou liés à ces attentats, avant le 13 novembre au soir*' (cf. II.5) et une nouvelle enquête portant sur les services d'appui de l'OCAM (cf. II.6.4).

Par ailleurs, toute une série de points ont été mis à l'ordre du jour : l'éventuelle adaptation du statut administratif, la gestion des problèmes budgétaires structurels, auxquels sont confrontées toutes les institutions à

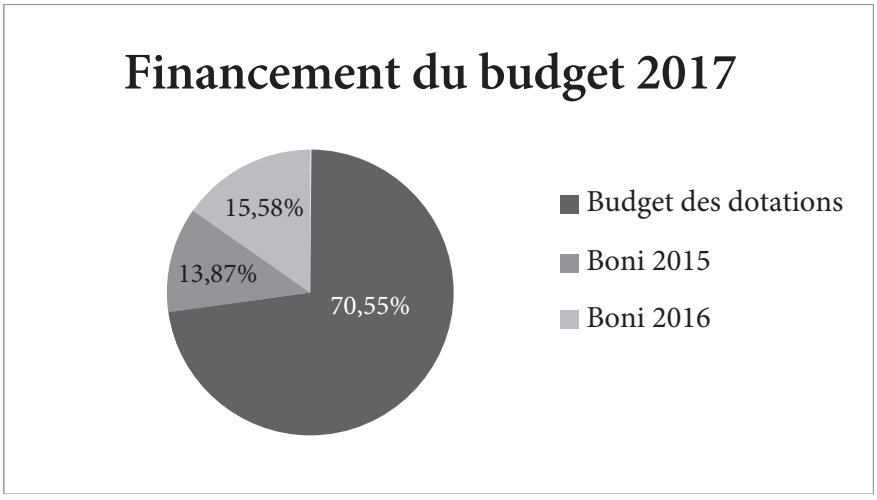
157 *Doc. parl.*, Chambre 2017-18, 54-2734/1 (Rapport d'activités 2016 du Comité permanent de Contrôle des services de renseignement et de sécurité, Rapport fait au nom de la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de contrôle des services de renseignement et de sécurité).

dotation, et les synergies possibles, le rôle des deux Comités en lien avec la 'Commission de suivi' établie dans le cadre de la Commission d'enquête parlementaire 'Attentats', le suivi de l'évolution de la nouvelle législation relative à la vie privée… Autre point à l'agenda : la préparation des célébrations du 25ème anniversaire des deux Comités. Enfin, les deux Comités se sont accordés sur la nécessité de développer une méthodologie commune, en premier lieu pour les enquêtes de contrôle communes.

Quatre réunions communes ont été organisées en 2017, sans compter les fréquents contacts informels sur le terrain.

XI.4. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Le budget 2017 du Comité permanent R a été fixé à 3,635,890 millions d'euros, soit une diminution de 3,6 % par rapport à 2016. Les sources de financement attribuées par la Chambre des Représentants[158] sont les suivantes :

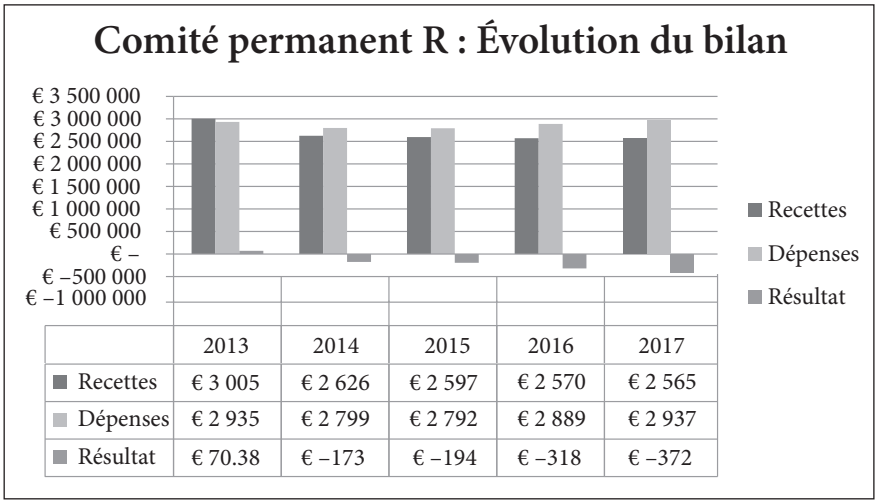


Dans la continuité de son budget précédent, le Comité permanent R est encore parvenu à réduire ses budgets de fonctionnement dans un contexte professionnel pourtant difficile et malgré le nombre de missions légales en constante progression. Dans ces circonstances, le Comité a quand même été en mesure, en 2017, de renforcer son service administratif de deux unités, tout en restant dans les limites de son enveloppe budgétaire.

158 *Doc. parl.*, Chambre 2016-17, 54-2225/1, 20-22.

L'exécution du budget 2017 a produit un boni comptable de 0,698 million d'euros, ce qui représente la différence entre le budget approuvé et les dépenses constatées.

Comme en 2016, la réalité financière aboutit à une tout autre constatation, moins édulcorée. L'article 57 alinéa 1er L.Contrôle stipule que les crédits de fonctionnement doivent être inscrits au budget des dotations. Or, comme le montre le tableau ci-dessus, le budget 2017 est composé de différentes sources de financement, et le seul apport nouveau de trésorerie nette est constitué par la dotation inscrite au budget général de l'État.[159] En termes de flux financiers, le Comité accuse ainsi une perte de 0,372 million d'euros, en augmentation de 16,87 % par rapport à l'exercice budgétaire 2016 (– 0,318 million d'euros). Cette tendance, déjà observée depuis quelques années, hypothèque la solvabilité du Comité sur le moyen terme, à politique inchangée.



	2013	2014	2015	2016	2017
Recettes	€ 3 005	€ 2 626	€ 2 597	€ 2 570	€ 2 565
Dépenses	€ 2 935	€ 2 799	€ 2 792	€ 2 889	€ 2 937
Résultat	€ 70.38	€ –173	€ –194	€ –318	€ –372

Le Conseil des ministres avait décidé, le 15 octobre 2014, c'est-à-dire en début de législature, de diminuer de 2 % de manière linéaire le budget des dotations. Cette décision restant d'application, le principal vecteur d'augmentation des dépenses réelles du Comité viendra très probablement du nombre de nouvelles missions légales qui lui sont confiées, plus que des phénomènes d'indexation. Sans relèvement significatif du montant de la dotation inscrite au budget de l'État, le risque d'épuisement des réserves accumulées mettra le Comité en difficulté de fonctionnement tant sur le plan opérationnel que financier.[160]

159 Loi du 25 décembre 2016 contenant le budget général des dépenses pour l'année budgétaire 2017, *M.B.* 29 décembre 2016.

160 D'autres institutions à dotation (le Comité permanent de Contrôle des services de police, la Commission de la protection de la vie privée, l'Organe de contrôle de l'information policière, le Médiateur fédéral, le Conseil supérieur de la Justice, la Commission BIM et les Commissions de nomination réunies pour le Notariat) sont également confrontées au même problème et en ont une vision commune. En 2017, ces institutions ont adressé au Président de

Cependant, des synergies entre les différentes institutions émargeant au budget des dotations ont été étudiées à l'initiative du Président de la Chambre des Représentants et produisent des effets dans certains domaines, par une mutualisation des tâches : cette approche permet d'éviter des coûts de gestion supplémentaires pour certains organismes mais reste marginale en termes financiers. Néanmoins, quelle que soit l'importance de cet avantage, il a le mérite d'être mis en application dans tous les cas possibles, dès que sa pertinence est validée par les études préparatoires.

XI.5. UN AUDIT EXTERNE DE TOUTES LES INSTITUTIONS À DOTATION

À la demande de la Commission de la Comptabilité de la Chambre des Représentants, la Cour des Comptes a initié une enquête, conjointement avec Ernst & Young, sur les institutions à dotation. Le Comité permanent R était donc concerné.

La Cour des Comptes devait surtout se concentrer sur les aspects budgétaires (une analyse des recettes et des dépenses) et sur la délimitation des missions des différentes institutions. De son côté, Ernst & Young était principalement chargé de procéder à une analyse approfondie des processus, des systèmes et de l'organisation de chacune de ces institutions.

Afin de pouvoir mener à bien ces missions, les institutions ont dû mettre à disposition de nombreux documents et quantité d'informations. Elles ont dû également répondre à toute une série de questions ponctuelles. Cet audit, qui a débuté fin 2017 et qui a livré ses résultats au premier trimestre 2018, a mobilisé les énergies au sein du Comité permanent R, et ce, en plus de la charge de travail croissante.

XI.6. FORMATION

Vu l'intérêt pour l'organisation, le Comité permanent R encourage ses membres et ses collaborateurs à suivre des formations générales (informatique, management…) ou propres au secteur, ou encore à participer à des conférences.[161] Concernant cette dernière catégorie, un ou plusieurs membre(s) du Comité permanent R ou membre(s) de son personnel a/ont assisté aux journées d'étude mentionnées ci-dessous.

---

la Chambre des Représentants un courrier conjoint exprimant leurs préoccupations quant aux lourdes conséquences des restrictions budgétaires (cf. Préface).

161 Des formations ont également été dispensées en interne, notamment plusieurs briefings de sécurité auxquels les collaborateurs étaient priés d'assister, ainsi que des formations liées au renseignement.

DATE	TITRE	ORGANISATION	LIEU
25-27 janvier 2017	The Age of Intelligence Machines	Computers, Privacy & Data Protection (CPDP)	Bruxelles
23 février 2017	Third Expert Meeting – National Intelligence Authorities and Surveillance in the EU : Fundamental Rights and Surveillance	European Union Agency for Fundamental Rights (FRA)	Vienne
27 février 2017	L'informateur de police : une production du renseignement entre fantasmes et réalités (La source)	Groupe de recherche METIS Renseignement	Paris
22 mars 2017	Le contrôle et l'évaluation de la politique publique du renseignement	Délégation parlementaire au renseignement (DPR) et Commission nationale de contrôle des techniques de renseignement (CNCTR)	Paris
31 mars 2017	Surveying Surveillance in the EU	RightsCon	Bruxelles
26-27 avril 2017	Table ronde sur le cadre légal régissant les services de renseignement	République tunisienne et Centre pour le contrôle démocratique des forces armées (DCAF)	Tunis
12 mai 2017	Managing uncertainties. The protection of critical infrastructures and intelligence services	Belgian Intelligence Studies Centre (BISC)	Gand
12 mai 2017	Les méthodes d'enquête pénale dans le domaine des nouvelles technologies	Centre de recherche information, droit et société (CRIDS)	Bruxelles
29 juin 2017	The Electromagnetic Attack	European Corporate Security Association (ECSA)	Bruxelles
12-13 septembre 2017	Information on Methods of Analysis Course	Belgian Intelligence Academy (BIA)	Heverlee
25 septembre 2017	Table ronde 'Que faire pour rendre le renseignement plus efficace encore dans la lutte contre le terrorisme ?'	Centre Com	Paris
2 octobre 2017	Champs d'application des textes, principes de base et rôle de la CPVP	Commission de la protection de la vie privée (CPVP)	Bruxelles
9 octobre 2017	Les obligations des responsables de traitements et des sous-traitants	Commission de la protection de la vie privée (CPVP)	Bruxelles

DATE	TITRE	ORGANISATION	LIEU
16 octobre 2017	Les obligations des responsables de traitements et des sous-traitants (suite) ; les flux transfrontaliers et les droits des personnes concernées	Commission de la protection de la vie privée (CPVP)	Bruxelles
24 octobre 2017	Cybersécurité et cyberdéfense : menaces, enjeux et réponses stratégiques	Royal Higher Institute for Defence and the Study Centre for Military Law and Law of War	Bruxelles
26-27 octobre 2017	Training on Monitoring Law Enforcement and Intelligence Services in Georgia – Status, Needs and International Best Practices	Democratic Centre for Armed Forces (DCAF) and the Public Defender of Georgia	Tbilissi
16-17 novembre 2017	Cybersécurité – Expériences internationales et Droits comparés	République tunisienne et Centre pour le contrôle démocratique des forces armées (DCAF)	Tunis
30 novembre 2017	Cybersecurity framework in BEL Defence – Cyber Coalition 2017 – scenario overview and deployed CSOC visit	SGRS	Bruxelles
1er décembre 2017	Terrorisme Counter insurgency et le rôle des services de renseignement	Belgian Intelligence Studies Centre (BISC)	Bruxelles
11 décembre 2017	Secret et publications : comment écrire sur les services de renseignement ?	Groupe de recherche METIS Renseignement	Paris

CHAPITRE XII
RECOMMANDATIONS

À la lumière des enquêtes de contrôle clôturées en 2017, 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 (XII.1), sur la coordination et l'efficacité des services de renseignement, de l'OCAM et des services d'appui (XII.2) et, enfin, sur la coordination et l'efficacité des services de renseignement, de l'OCAM et des services d'appui (XII.3).

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

XII.1.1. EXAMEN DE LA FORTE AUGMENTATION DU NOMBRE D'IDENTIFICATIONS ORDINAIRES[162]

Depuis l'introduction de la procédure assouplie visée à l'article 16/2 L.R&S, par laquelle certaines identifications de communications ne sont plus considérées comme une méthode spécifique, le nombre de réquisitions d'identifications adressées à des opérateurs a explosé. Dans le cadre de sa compétence générale de contrôle, le Comité recommande d'examiner, en interne, dans quelle mesure l'assouplissement de la procédure explique (en partie) ce nombre élevé de réquisitions. À cet égard, il convient notamment d'être attentif à la nature des menaces qui justifient les réquisitions et à la question de savoir si et dans quelle mesure de telles réquisitions se font à la demande d'autorités/services partenaires étrangers.

[162] Voir 'Chapitre III. Le contrôle des méthodes particulières de renseignement et de certaines méthodes d'identification ordinaires'.

XII.1.2. RÈGLES DE CONDUITE DANS LES CONTACTS AVEC DES CITOYENS[163]

Le Comité a insisté sur le fait que les agents de renseignement ne pouvaient pas donner à tort l'impression de posséder certaines compétences ou de disposer de certaines possibilités. En outre, lors d'un entretien, ils se doivent de prendre en considération le ressenti éventuel des personnes qui n'ont aucune idée du fonctionnement d'un service de renseignement. Le Comité recommande que la VSSE et le SGRS en tiennent compte dans le cadre de la formation dispensée à leurs agents, qu'ils y accordent une attention spécifique dans leurs directives, et que les inspecteurs, dans leurs contacts avec l'extérieur, expliquent très clairement quelles sont leurs compétences et quels sont les droits et les devoirs de leurs interlocuteurs. La VSSE et le SGRS peuvent élaborer certains instruments (p. ex. une brochure sur la VSSE et ses compétences, un synopsis de la L.R&S) qui, si le contexte s'y prête, peuvent être présentés ou remis pour information à l'intéressé(e).

XII.1.3. LE SECRET PROFESSIONNEL ET LES SERVICES DE RENSEIGNEMENT[164]

Depuis 2017, l'article 16 L.R&S stipule que *'[s]ans préjudice de l'article 2, § 2, les personnes et organisations relevant du secteur privé peuvent communiquer d'initiative aux services de renseignement et de sécurité, les informations et les données à caractère personnel utiles à l'exercice de leurs missions*.' Certaines catégories professionnelles ne sont donc plus tenues au secret professionnel dans leurs contacts avec les services de renseignement. Le Comité recommande toutefois que le législateur mentionne explicitement dans quelle mesure des obligations spécifiques de secret s'appliquent ou non aux relations avec la VSSE et le SGRS.

XII.1.4. UN PLAN D'ÉCOUTE PLUS DETAILLÉ[165]

Depuis quelque temps, la section SIGINT du SGRS travaille avec des 'fiches projets', qui donnent une description nettement plus détaillée que dans le plan d'interception (p. ex. en utilisant des sélecteurs) des organisations et des

163 Voir 'Chapitre II.2. La demande potentiellement injustifiée de transactions bancaires et le secret professionnel'.

164 Voir 'Chapitre II.2. La demande potentiellement injustifiée de transactions bancaires et le secret professionnel'.

165 Voir 'Chapitre IV. Le contrôle des interceptions à l'étranger, des prises d'images et des instrusions dans des systèmes informatiques'.

institutions devant faire l'objet d'interceptions. Ces fiches répondent mieux à l'exigence légale à satisfaire dans la confection d'une liste motivée d'institutions. Le Comité estime que les listes actuelles doivent être plus détaillées. Le SGRS s'est engagé à évoluer en ce sens, tout en affirmant ne pas être en mesure de fournir des listes exhaustives de targets.

XII.1.5. UNE BASE LÉGALE POUR LES NOUVELLES BANQUES DE DONNÉES COMMUNES[166]

En 2017, le Comité permanent R et le C.O.C. ont recommandé que les textes réglementaires requis soient adoptés en ce qui concerne les traitements de données et d'informations relatives aux prédicateurs de haine et aux *homegrown terrorist fighters*. Les Arrêtés royaux du 23 avril 2018[167] ont permis de se conformer à cette obligation : la banque de données FTF existante a été étendue aux *homegrown terrorist fighters*, et une seconde banque de données a été créée pour les prédicateurs de haine. Cependant, conformément à l'article 44/11/3*bis* de la Loi sur la fonction de police, la création d'une banque de données est conditionnée à la transmission d'une déclaration préalable (comprenant les modalités de fonctionnement) par les ministres compétents au C.O.C. et au Comité permanent R. Ces institutions ont ensuite trente jours pour formuler un avis. Au moment de la clôture du présent rapport d'activités (mi-2018), une telle déclaration manquait toujours à l'appel, alors que les deux banques de données sont opérationnelles.

XII.1.6. LA DÉSIGNATION D'UN CONSEILLER EN SÉCURITÉ ET EN PROTECTION DE LA VIE PRIVÉE[168]

Le contrôle conjoint de la banque de données FTF par le C.O.C et le Comité permanent R a mis en exergue certaines faiblesses, comme par exemple l'absence de contrôle de la légitimé des accès et de mécanisme de signalement des incidents de sécurité. Ces problèmes pouvaient s'expliquer par le fait qu'en 2017, la désignation du conseiller en sécurité et en prévention de la vie privée se faisait

166 Voir 'Chapitre VI. 'Le contrôle de banques de données communes'.

167 A.R. du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police ; A.R. du 23 avril 2018 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters.

168 Voir 'Chapitre VI. Le contrôle de banques de données communes'.

toujours attendre. Les deux institutions avaient pourtant régulièrement insisté sur ce point. Aussi le C.O.C. et le Comité recommandent-ils aux ministres compétents de procéder à la désignation de ce consultant dans les meilleurs délais.

XII.1.7. LE RÔLE DES CONSEILLERS EN SÉCURITÉ ET EN PROTECTION DE LA VIE PRIVÉE[169]

Le C.O.C. et le Comité permanent R recommandent que les conseillers en sécurité des différents services qui sont impliqués dans le fonctionnement de la banque de données FTF demandent régulièrement à la Police fédérale des échantillons de loggins pour effectuer un contrôle périodique de la légitimité des consultations. Ils recommandent également la réévaluation périodique des systèmes de validation, la prise d'initiatives en matière de sécurité d'information (concernant les contrôles d'accès, la formation, la sensibilisation…) et l'échange de bonnes pratiques par l'intermédiaire des conseillers en sécurité de l'information.

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

XII.2.1. ANALYSE DE RISQUES PRÉALABLE À TOUTE MISSION À L'ÉTRANGER[170]

Dans le cadre de l'enquête sur la manière dont le SGRS avait préparé une mission dans une zone de conflit, où des contacts avaient été établis avec une organisation donnée, le Comité permanent R a remarqué l'absence de toute analyse de risques formalisée à caractère stratégico-politique ou opérationnelle. Dans les différents documents de mission, des éléments du risque sont bien évoqués, mais pas de manière structurée et synthétique. Au début d'une opération, et évidemment aussi pendant son déroulement, le SGRS devrait établir une analyse de risques structurée et formelle. Cette démarche permet au service et au ministre, chacun dans le cadre de ses compétences, de lister tous les risques qui y sont liés (ainsi que les risques au niveau de la politique belge militaire et internationale), de les accepter ou non et, le cas échéant, de prendre des mesures pour les limiter (y compris la préparation d'éléments de langage dans l'hypothèse où un risque prévu se serait confirmé durant une opération).

169 Voir 'Chapitre VI. 'Le contrôle de banques de données communes'.
170 Voir 'Chapitre II.1. Une plainte concernant trois opérations du SGRS'.

XII.2.2. COUVERTURE POLITIQUE DES ACCORDS DE COOPÉRATION[171]

Dans le cadre des liens de coopération établis par le SGRS (mais aussi par la VSSE) au niveau international, des engagements ou des choix nécessitant une évaluation et une couverture politiques peuvent être posés. Le Comité recommandait déjà, en guise de principe général, que les ministres compétents soient suffisamment informés pour être en mesure d'assumer leur responsabilité politique à l'égard du Parlement.[172] Le Comité réitère cette recommandation et la rend plus concrète, en avançant des éléments susceptibles de constituer des critères permettant d'apprécier l'opportunité et le moment adéquat pour le service d'informer le ministre. Entre autres éléments : le bureau qui mènera l'opération, le lieu de l'opération (dans une zone de conflit ? Dans un domaine d'opération militaire belge ?) ; l'ampleur des risques stratégico-politiques (listés de manière structurée et formelle), le contexte international, la question de savoir s'il existe ou non un lien avec une enquête judiciaire, le danger de compromission de l'opération… Cette énumération n'est pas exhaustive.

Il appartient au service et au ministre de compléter la liste et d'en développer les éléments si nécessaire.

XII.2.3. HARMONISATION DE LA POLITIQUE DE RENSEIGNEMENT ENTRE LE SGRS ET LA VSSE[173]

Le Comité permanent R recommande que, lorsque deux services de renseignement nouent des contacts avec des services étrangers ou avec des acteurs non étatiques, ils se concertent de manière à harmoniser leur politique de renseignement afin d'aboutir à un résultat cohérent. Le Plan National du Renseignement, qui est établi sous la responsabilité du Conseil national de sécurité, peut constituer un cadre utile.

XII.2.4. LA GESTION, LA CONSERVATION ET LA COMMUNICATION D'INFORMATIONS REPRISES DANS LA BANQUE DE DONNÉES FTF[174]

Il convient de réfléchir à la question suivante : est-il ou non souhaitable de reprendre des informations policières sensibles (rapports d'information portant les codes 00 et 01) dans la banque de données FTF ? Dans la négative, le cadre légal nécessitera une adaptation.

---

171 Voir 'Chapitre II.1. Une plainte concernant trois opérations du SGRS'.
172 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 117-118.
173 Voir 'Chapitre II.1. Une plainte concernant trois opérations du SGRS'.
174 Voir 'Chapitre VI. Le contrôle de banques de données communes'.

Le C.O.C. et le Comité préconisent par ailleurs de développer des outils informatiques afin de faciliter le suivi des délais applicables en matière de conservation des données et le suivi de la transmission de la carte d'information aux bourgmestres.

Enfin, il est recommandé de sécuriser la communication des cartes d'information (ou des extraits) à des tiers, et de la soumettre à une évaluation préalable incluant certainement la mise en place de mesures de sécurité par ces tiers.

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

XII.3.1. MISE À DISPOSITION D'INFORMATIONS POUR LE COMITÉ PERMANENT R[175]

Contrairement à la mise en œuvre des méthodes particulières, le Comité ne possède pas les chiffres relatifs à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question à l'article 16/2 L.R&S. Le Comité recommande aux services de consigner également ces données et de les tenir à la disposition du Comité permanent R.

XII.3.2. ÉLARGISSEMENT DU REPORTING AU PARLEMENT[176]

La Loi du 25 décembre 2016 (*M.B.* 25 janvier 2017) a donné la possibilité à la VSSE et au SGRS d'avoir accès à des informations provenant de l'Unité d'information des passagers (art. 16/3 L.R&S). Le Comité est informé de cette méthode et peut l'interdire le cas échéant. Contrairement aux méthodes visées à l'article 16/2 L.R&S, il n'a pas été prévu qu'un rapport doive être transmis au Parlement ; l'article 35 § 2 L.Contrôle n'a en effet pas été adapté.

Le Comité permanent R recommande de le faire, d'autant qu'un rapport doit être établi sur les demandes de données de transport et de voyage sur base de l'article 18/6/1 L.R&S, puisqu'il s'agit d'une méthode spécifique. Le Comité estime d'ailleurs qu'un tel rapport est tout aussi indiqué pour la possibilité introduite par la Loi du 21 mars 2018 (*M.B.* 16 avril 2018) d'utiliser des images enregistrées par des caméras et reprises dans des fichiers (art. 16/4 L.R&S).

175 Voir 'Chapitre III. Le contrôle des méthodes particulières de renseignement et de certaines méthodes d'identification ordinaires'.

176 Voir 'Chapitre III. Le contrôle des méthodes particulières de renseignement et de certaines méthodes d'identification ordinaires'.

XII.3.3. OBLIGATION D'INFORMATION DANS LE CADRE DES MÉTHODES EXCEPTIONNELLES[177]

En ce qui concerne le SGRS, le Comité insiste sur le respect de l'obligation légale d'informer toutes les deux semaines la Commission BIM de l'exécution des méthodes exceptionnelles (art. 18/10 § 1er, alinéa 3 L.R&S et art. 9 A.R. du 12 octobre 2010).

XII.3.4. UN OUTIL PERMETTANT DE CONTRÔLER L'ÉVOLUTION DES FICHES DE RENSEIGNEMENTS DANS LA BANQUE DE DONNÉES FTF[178]

Afin de pouvoir contrôler de manière adéquate les fiches de renseignement dans la banque de données FTF, le C.O.C. et le Comité permanent R insistent sur la nécessité d'élaborer un outil permettant de prendre connaissance de toutes les opérations effectuées dans une fiche de renseignements. Ils demandent à la Police fédérale, qui gère la banque de données, de prendre toute mesure utile à cet égard.

177 Voir 'Chapitre III. Le contrôle des méthodes particulières de renseignement et de certaines méthodes d'identification ordinaires'.

178 Voir 'Chapitre VI. Le contrôle de banques de données communes'.

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 2017 AU 31 DÉCEMBRE 2017)

Loi 25 décembre 2016 relative au traitement des données des passagers, *M.B.* 25 janvier 2017

Loi 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal, *M.B.* 28 avril 2017

Loi 19 avril 2017 modifiant le Code d'instruction criminelle, le Code judiciaire et la loi du 10 avril 2014 modifiant diverses dispositions en vue d'établir un registre national des experts judiciaires et établissant un registre national des traducteurs, interprètes et traducteurs-interprètes jurés, *M.B.* 31 mai 2017

Loi 19 avril 2017 modifiant le Code d'instruction criminelle, le Code judiciaire et la loi du 10 avril 2014 modifiant diverses dispositions en vue d'établir un registre national des experts judiciaires et établissant un registre national des traducteurs, interprètes et traducteurs-interprètes jurés – Erratum, *M.B.* 12 juin 2017

Loi 31 juillet 2017 portant des dispositions diverses en matière de communications électroniques, *M.B.* 12 septembre 2017

Loi 2 octobre 2017 réglementant la sécurité privée et particulière, *M.B.* 31 octobre 2017

Loi 21 novembre 2017 contenant le deuxième ajustement du budget général des dépenses pour l'année budgétaire 2017, *M.B.* 27 novembre 2017

Loi 9 décembre 2015 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, *M.B.* 30 novembre 2017

Loi 22 décembre 2017 contenant le budget général des dépenses pour l'année budgétaire 2018, *M.B.* 28 décembre 2017

A.R. 12 décembre 2016 portant répartition partielle, pour ce qui concerne la lutte contre le terrorisme et le radicalisme, du crédit provisionnel inscrit au programme 03-41-1 du budget général des dépenses pour l'année budgétaire 2016 et destiné à couvrir les dépenses concernant le renforcement des mesures prises ainsi que les initiatives nouvelles en matière de lutte contre le terrorisme et le radicalisme, *M.B.* 9 janvier 2017

A.R. 14 décembre 2016 portant répartition partielle, pour ce qui concerne la lutte contre le terrorisme et le radicalisme, du crédit provisionnel inscrit au programme 03-41-1 du budget général des dépenses pour l'année budgétaire 2016 et destiné à couvrir les

dépenses concernant le renforcement des mesures prises ainsi que les initiatives nouvelles en matière de lutte contre le terrorisme et le radicalisme, *M.B.* 9 janvier 2017

A.R. 20 décembre 2016 portant répartition partielle, pour ce qui concerne la lutte contre le terrorisme et le radicalisme, du crédit provisionnel inscrit au programme 03-41-1 du budget général des dépenses pour l'année budgétaire 2016 et destiné à couvrir les dépenses concernant le renforcement des mesures prises ainsi que les initiatives nouvelles en matière de lutte contre le terrorisme et le radicalisme, *M.B.* 12 janvier 2017

A.R. 16 février 2017 portant la procédure selon laquelle le Roi peut procéder à la reconnaissance d'un acte de terrorisme au sens de l'article 42*bis* de la loi du 1er août 1985, *M.B.* 3 mars 2017

A.R. 6 mars 2017 modifiant l'arrêté royal du 23 mai 2016 organisant le transfert des assistants de protection de la Sûreté de l'État vers la police fédérale, *M.B.* 9 mars 2017

A.R. 19 mars 2017 fixant la date d'entrée en vigueur des articles 5 et 17 à 23 de la loi du 21 avril 2016 portant des dispositions diverses Intérieur – Police intégrée, *M.B.* 23 mars 2017

A.R. 12 mars 2017 fixant les cadres linguistiques des services centraux de la Sûreté de l'État, *M.B.* 5 avril 2017

A.R. 9 avril 2017 modifiant l'arrêté royal du 3 juin 2007 relatif à l'armement de la police intégrée, structurée à deux niveaux ainsi qu'à l'armement des membres des services d'enquêtes des comités permanents P et R et du personnel de l'Inspection générale de la police fédérale et de la police locale, *M.B.* 5 mai 2017

A.R. 21 décembre 2017 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant diverses dispositions concernant l'Unité d'information des passagers et le délégué à la protection des données, *M.B.* 29 décembre 2017

A.M. 22 février 2017 relatif aux épreuves de capacité de certains agents civils du département d'état-major renseignement et sécurité des forces armées, *M.B.* 16 mars 2017

A.M. 28 février 2017 relatif aux exigences de formation continuée de certains agents civils du département d'état-major renseignement et sécurité des forces armées, *M.B.* 17 mars 2017

A.M. 16 mai 2017 modifiant, en ce qui concerne la Sûreté de l'État, l'arrêté ministériel du 25 octobre 2013 portant organisation interne, délégations de pouvoir et autorisations de signature au sein du Service public fédéral Justice en matière de passation et d'exécution de marchés publics de travaux, de fournitures et de services, en matière de subventions et en matière de dépenses diverses, *M.B.* 14 juillet 2017

Sélection comparative de Cyber Security Expert (m/f/x) (niveau A2), francophones, pour le Ministère de la Défense, *M.B.* 15 mars 2017

Sélection comparative de Cyber Risk Prevention Expert (m/f/x) (niveau A2), francophones, pour le Ministère de la Défense, *M.B.* 15 mars 2017

Résultat de la sélection comparative néerlandophone d'accession au niveau A (3e série) pour le Ministère de la Défense : attaché analyste, *M.B.* 21 mars 2017

Sélection comparative de Cyber Security Expert (m/f/x) (niveau A2), francophones, pour le Ministre de la Défense – erratum, *M.B.* 22 mars 2017

Sélection comparative de Cyber Risk Prevention Expert (m/f/x) (niveau A2), francophones, pour le Ministère de la Défense – erratum, *M.B.* 22 mars 2017

Sélection comparative d'inspecteurs (m/f/x) (niveau B), francophones, pour le Ministère de la Défense, *M.B.* 24 mars 2017

Résultat de la sélection comparative de consultants ICT (m/f/x) (niveau B), néerlandophones pour l'OCAM-SPF Intérieur, *M.B.* 9 juin 2017

Appel aux candidats pour le mandat de membre francophone du Comité permanent de contrôle des services de renseignement, *M.B.* 4 juillet 2017

Nouvel appel aux candidats pour le mandat de membre masculin néerlandophone de la police locale pour l'Organe de contrôle de l'information policière, *M.B.* 26 septembre 2017

Sélection comparative de responsables de service budget et comptabilité (m/f/x) (niveau A3), francophones, pour la Sûreté de l'Etat, *M.B.* 22 novembre 2017

Sélection comparative de collaborateurs polyvalents secrétariat de direction (m/f/x) (niveau B), francophones, pour l'Organe de Coordination pour l'Analyse de la Menace (OCAM), *M.B.* 8 décembre 2017

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 2017 AU 31 DÉCEMBRE 2017)

Sénat

Proposition de résolution visant à charger les instances compétentes d'enquêter sur les organisations wahhabites actives sur notre territoire afin de déterminer si elles sont des organisations sectaires nuisibles, *Doc. parl.*, Sénat, 2017-2018, nº 6-383/1

Chambre des Représentants

Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste, troisième rapport intermédiaire, sur le volet 'architecture de la sécurité', *Doc. parl.*, Chambre, 2016-2017, nos 54-1752/7 à 54-1752/10

Projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers afin de renforcer la protection de l'ordre public et de la sécurité nationale (2215/1-4), *C.R.I.*, Chambre, 2016-2017, 9 février 2017, PLEN 156, p. 49

Amendements et articles réservés du projet de loi modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers afin de renforcer la protection de l'ordre public et de la sécurité nationale (2215/1-5), *C.R.I.*, Chambre, 2016-2017, 9 février 2017, PLEN 157, p. 42

Projet de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal, *Doc. parl.*, Chambre, 2016-2017, nos 54-2043/5 à 54-2043/11 et *C.R.I.*, Chambre, 2016-2017, 16 mars 2017, PLEN 161, p. 44

Proposition de résolution relative au soutien de la Belgique à la Tunisie (1427/1-6), *C.R.I.*, Chambre, 2016-2017, 30 mars 2017, PLEN 163, p. 50

Proposition de loi concernant le traitement de données à caractère personnel par le Service public fédéral Justice dans le cadre de l'exécution des peines et des mesures privatives de liberté et de la gestion des établissements dans lesquels cette exécution s'effectue, *Doc. parl.*, Chambre, 2016-2017, no 54-2194/2

Projet de loi portant simplification, harmonisation, informatisation et modernisation de dispositions de droit civil et de procédure civile ainsi que du notariat, et portant diverses mesures en matière de justice, *Doc. parl.*, Chambre, 2016-2017, no 54-2259/2

Proposition de loi relative à la dénonciation d'une atteinte suspectée à l'intégrité par les membres de la police intégrée, *Doc. parl.*, Chambre, 2016-2017, no 54-2355/1

Proposition de résolution relative à l'ingérence nuisible de certains États du Golfe dans le libre exercice du culte islamique en Belgique, *Doc. parl.*, Chambre, 2016-2017, no 54-2365/1

Projet de loi réglementant la sécurité privée, *Doc. parl.*, Chambre, 2016-2017, nos 54-2388/003, 54-2388/004, 54-2388/005 et 54-2388/007

Audition du Général Marc Compernol, Chef de la Défense concernant la Vision stratégique pour la Défense — Horizon 2030, *Doc. parl.*, Chambre, 2016-2017, no 54-2392/1

Projet de loi modifiant l'article 36*bis* de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *Doc. parl.*, Chambre, 2016-2017, no 54-2405/1

Projet de loi contenant le premier ajustement du budget général des dépenses pour l'année budgétaire 2017, *Doc. parl.*, Chambre, 2016-2017, no 54-2411/1

Proposition de loi modifiant le Code d'instruction criminelle en vue de promouvoir la lutte contre le terrorisme (2050/1-14) – proposition de loi modifiant la loi du 8 juillet 1976 organique des centres publics d'action sociale en vue de promouvoir la lutte contre les infractions terroristes (1687/1-4), *C.R.I.*, Chambre, 2016-2017, 7 mai 2017, PLEN 166, p. 66 et *C.R.I.*, Chambre, 2016-2017, 4 mai 2017, PLEN 167, p. 24

Proposition de loi modifiant l'article 134*quinquies* de la Nouvelle Loi Communale en vue de permettre au bourgmestre de fermer les établissements suspectés d'abriter des activités terroristes (1473/1-12) *C.R.I.*, Chambre, 2016-2017, 4 mai 2017, PLEN 167, p. 1

Projet de loi réglementant la sécurité privée et particulière (2388/1-6) – proposition de loi modifiant la loi du 10 avril 1990 réglementant la sécurité privée et particulière en ce qui concerne la prise en charge de missions de police (675/1-3) – proposition de loi modifiant la loi du 10 avril 1990 réglementant la sécurité privée et particulière en ce qui concerne les conditions d'exercice de fonctions au sein de la sécurité privée et particulière (1829/1) – proposition de loi modifiant la loi du 10 avril 1990

réglementant la sécurité privée et particulière en ce qui concerne la serrurerie (2035/1), *C.R.I.*, Chambre, 2016-2017, 8 juin 2017, PLEN 172, p. 95

La lutte contre le trafic d'armes, auditions, *Doc. parl.*, Chambre, 2016-2017, nº 54-2499/1

Comité permanent de contrôle des services de renseignements et de sécurité – remplacement d'un membre, *C.R.I.*, Chambre, 2016-2017, 29 juin 2017, PLEN 177, p. 44

Modifications du statut du directeur général et des membres du service d'enquêtes du Comité permanent de contrôle des services de Police, *Doc. parl.*, Chambre, 2016-2017, nº 54-2561/1 et *C.R.I.*, Chambre, 2016-2017, 6 juillet 2017, PLEN 178, p. 94

Proposition de loi visant à interdire le financement étranger d'activités entravant le libre exercice des cultes en Belgique, *Doc. parl.*, Chambre, 2016-2017, nº 54-2675/1

Comité permanent de contrôle des services de renseignements et de sécurité – remplacement d'un membre – candidatures introduites, *C.R.I.*, Chambre, 2016-2017, 21 septembre 2017, PLEN 184, p. 64

Commentaire et observations sur les projets de budget de l'État pour l'année budgétaire 2018, *Doc. parl.*, Chambre, 2017-2018, nº 54-2689/3 à 54-2689/5

Projet du budget général des dépenses pour l'année budgétaire 2018, *Doc. parl.*, Chambre, 2016-2017, nos 54-2690/1, 54-2690/5, 54-2690/11 et 54-2690/13

Justification du budget général des dépenses pour l'année budgétaire 2018, *Doc. parl.*, Chambre, 2016-2017, nº 54-2691/7

Note de politique générale, *Doc. parl.*, Chambre, 2016-2017, nos 54-2708/5, 54-2708/8, 54-2708/9, 54-2708/17, 54-2708/24 et 54-2708/29

Comité permanent de contrôle des services de renseignements et de sécurité remplacement d'un membre – audition des candidats, *C.R.I.*, Chambre, 2017-2018, 12 octobre 2017, PLEN 190, p. 11

Projet de loi modifiant la loi du 8 juin 2006 réglant des activités économiques et individuelles avec des armes, *Doc. parl.*, Chambre, 2016-2017, nº 54-2709/1

Commission de suivi, *C.R.I.*, Chambre, 2017-2018, 9 novembre 2017, PLEN 195, p. 49

Rapport d'activités 2016 du Comité permanent de contrôle des services de renseignement et de sécurité, *Doc. parl.*, Chambre, 2017-2018, nº 54-2734/1

Projet de loi portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *Doc. parl.*, Chambre, 2017-2018, nos 54-2767/1 et 54-2767/2

Nomination d'un membre effectif francophone du Comité permanent de contrôle des services de renseignements et de sécurité, *Doc. parl.*, Chambre, 2017-2018, nº 54-2770/1

Comité permanent de contrôle des services de renseignements et de sécurité – Nomination d'un membre effectif francophone, *C.R.I.*, Chambre, 2017-2018, 16 novembre 2017, PLEN 197, p. 114

Cour des comptes, Cour constitutionnelle, Conseil supérieur de la Justice, Comité permanent de contrôle des services de police, Comité permanent de contrôle des services de renseignements et de sécurité, Médiateurs fédéraux, Commission de la protection de la vie privée, Commissions de nomination pour le notariat, Organe de contrôle de l'information policière, Commission MRD, Commission fédérale de déontologie (comptes de l'année budgétaire 2016, ajustements budgétaires de l'année 2017 et propositions budgétaires pour l'année 2018), *Doc. parl.*, Chambre, 2017-2018, nos 54-2843/1 à 54-2843/3

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 2017 AU 31 DÉCEMBRE 2017)

Sénat

Question écrite de J.-J. De Gucht au ministre de la Justice sur les 'enfants de combattants pour la Syrie belges – endoctrinement par l'EIIS – traumatismes – risques pour notre société' (Sénat, 8 mai 2017, Q. nº 6-1449)

Question écrite de J.-J. De Gucht au ministre de la Justice sur les 'djihadistes mineurs – enfants soldats – risques pour notre société – confirmation d'une présence détectée au sein des demandeurs d'asile dans notre pays' (Sénat, 2016-2017, 12 septembre 2017, Q. nº 6-1541)

Question écrite de M. Taelman au ministre de la Coopération au développement sur la 'cybercriminalité – e-mail spoofing (usurpation d'adresse électronique) – autorité – services de sécurité – prévention' (Sénat, 2017-2018, 9 novembre 2017, Q. nº 6-1639)

Question écrite de J.-J. De Gucht au ministre de la Défense sur 'Sûreté de l'État (VSSE) – Service Général du Renseignement et de la Sécurité (SGRS) – Social Media Intelligence (SOCMINT)' (Sénat, 2017-2018, 29 novembre 2017, Q. nº 6-1669)

Chambre des Représentants

Question de G. Gilkinet au ministre de la Justice sur 'la sécurité des agents des SPF' (*Q.R.*, Chambre, 2016-2017, 10 janvier 2017, nº 101, p. 199, Q. nº 980)

Question de B. Pas au ministre de la Justice sur 'le financement du terrorisme' (*Q.R.*, Chambre, 2016-2017, 10 janvier 2017, nº 101, p. 204, Q. nº 1037)

Question de B. Pas au ministre de la Justice sur 'les mesures prises pour lutter contre le terrorisme – l'incarcération de djihadistes' (*Q.R.*, Chambre, 2016-2017, 10 janvier 2017, nº 101, p. 210, Q. nº 1176)

Question de F. Dewinter au ministre de la Justice sur 'le personnel des services de sécurité – Arabe' (*Q.R.*, Chambre, 2016-2017, 10 janvier 2017, nº 101, p. 217, Q. nº 1211)

Question de D. Van der Maelen au ministre de la Justice sur les 'compétence des services de renseignements britanniques sur le territoire belge' (*Q.R.*, Chambre, 2016-2017, 10 janvier 2017, nº 101, p. 224, Q. nº 1341)

Question de G. Dallemagne au ministre de la Justice sur les 'répartitions de la provision terrorisme déjà liquidée' (*Q.R.*, Chambre, 2016-2017, 10 janvier 2017, nº 101, p. 258, Q. nº 1521)

Question de B. Pas au ministre de la Mobilité sur les 'aéroports – personnel de sécurité – personnel d'entretien et de manutention des bagages' (*Q.R.*, Chambre, 2016-2017, 10 janvier 2017, nº 101, p. 322, Q. nº 1280)

Question de F. Dewinter au ministre de la Justice sur 'le phénomène de radicalisation dans les prisons' (*C.R.I.*, Chambre, 2016-2017, 12 janvier 2017, PLEN152, 20, Q. nº 1745)

Questions jointes de Ph. Blanchart et S Lahaye-Battheu au ministre l'Intérieur sur 'le projet eCall' (*C.R.I.*, Chambre, 2016-2017, 18 janvier 2017, COM 569, p. 7, Q. nos 15733 et 15948)

Question de R. Terwingen au ministre de la Justice sur 'la demande de consultation des avis de la Sûreté de l'État sur l'agrément des mosquées de la ministre flamande Homans' (*C.R.I.*, Chambre, 2016-2017, 19 janvier 2017, PLEN153, 21, Q. nº 1761)

Question de H. Bonte au ministre de l'Intérieur sur 'les services de sécurité – la composition des cadres ' (*Q.R.*, Chambre, 2016-2017, 20 janvier 2017, nº 102, p. 274, Q. nº 1537)

Question de F. Schepmans au ministre de l'Intérieur sur le '« Open Source and Social Media Collect and Analyse Tool » – Police fédérale' (*Q.R.*, Chambre, 2016-2017, 20 janvier 2017, nº 102, p. 287, Q. nº 1645)

Question de D. Ducarme au ministre des Affaires étrangères sur le 'retrait des habilitations ANS – Service Général du Renseignement et de la Sécurité' (*Q.R.*, Chambre, 2016-2017, 20 janvier 2017, nº 102, p. 374, Q. nº 750)

Question de K. Metsu au ministre de la Justice sur 'le droit de visite dans les prisons' (*C.R.I.*, Chambre, 2016-2017, 25 janvier 2017, COM 575, p. 1, Q. nº 15957)

Question de J.-M. Nollet au ministre de la Défense sur les 'services secrets britanniques – rapports d'écoutes téléphoniques' (*Q.R.*, Chambre, 2016-2017, 27 janvier 2017, nº 103, p. 350, Q. nº 997)

Questions jointes de G. Grovonius et J.-J. Flahaux au Premier ministre et au ministre des Affaires étrangères sur 'la Tunisie' (*C.R.I.*, Chambre, 2016-2017, 8 février 2017, COM 589, p. 15, Q. nos 15837 et 16173)

Questions jointes de F. Dewinter, H. Bonte, G. Dallemagne, K. Metsu, Ph. Pivin, G. Vanden Burre, H. Vuye, A. Turtelboom et V. Yüksel au Premier ministre sur 'les mesures antiterroristes du gouvernement et le rapport de l'OCAM sur l'expansion du wahabisme' (*C.R.I.*, Chambre, 2016-2017, PLEN 156, 16, Q. nos 1828, 1822, 1823, 1829, 1830, 1831, 1824,1825 et 1826)

Question de B. Pas au ministre de la Justice sur 'le screening des prédicateurs de haine' (*Q.R.*, Chambre, 2016-2017, 17 février 2017, nº 106, p. 177, Q. nº 1572)

Question de R. Hufkens au ministre de la Défense sur 'le projet-pilote relatif à la surveillance de la caserne de Heverlee' (*Q.R.*, Chambre, 2016-2017, 17 février 2017, nº 106, p. 363, Q. nº 1045)

Question d'E. Kir au secrétaire d'État à l'Asile et la Migration sur 'les contrôles de police à la gare du Nord dans le cadre de la lutte contre le terrorisme' (*C.R.I.*, Chambre, 2016-2017, 22 février 2017, COM 604, p. 17, Q. nº 16450)

Question de F. Dewinter au ministre de la Justice sur 'Abdelhamid Abaoud – plans de Brussels Airport' (*Q.R.*, Chambre, 2016-2017, 23 février 2017, nº 107, p. 195, Q. nº 1206)

Question de S. Lahaye-Battheu au ministre de la Justice sur 'la Sûreté de l'État – surveillance des sectes' (*Q.R.*, Chambre, 2016-2017, 23 février 2017, nº 107, p. 196, Q. nº 1350)

Question de B. Pas au ministre de la Justice sur la 'base de données « foreign terrorist fighters » – base de données prédicateurs de haine, recruteurs et « loups solitaires » – accès des services publics flamands' (*Q.R.*, Chambre, 2016-2017, 23 février 2017, nº 107, p. 203, Q. nº 1389)

Question de B. Pas au ministre de la Justice sur 'l'assignation à résidence des prédicateurs de haine' (*Q.R.*, Chambre, 2016-2017, 23 février 2017, nº 107, p. 209, Q. nº 1481)

Question de B. Hellings au ministre de la Justice sur 'l'enquête des Nations Unies – mise à disposition des archives de la Sûreté de l'État' (*Q.R.*, Chambre, 2016-2017, 23 février 2017, nº 107, p. 216, Q. nº 1548)

Question de N. Lijnen au ministre de la Défense sur 'les cyberattaques contre l'OTAN' (*Q.R.*, Chambre, 2016-2017, 23 février 2017, nº 107, p. 258, Q. nº 1031)

Question de S. Pirlot au ministre de la Défense sur 'la présence d'extrémistes salafistes au sein de l'armée' (*Q.R.*, Chambre, 2016-2017, 23 février 2017, nº 107, p. 276, Q. nº 1056)

Question de D. Ducarme au ministre de l'Intérieur sur 'les visas aux ministres du culte' (*Q.R.*, Chambre, 2016-2017, 3 mars 2017, nº 108, p. 283, Q. nº 683)

Question de K. Metsu au ministre de l'Intérieur sur les 'demandeurs d'asile – suivi et screening' (*Q.R.*, Chambre, 2016-2017, 3 mars 2017, nº 108, p. 296, Q. nº 618)

Question de G. Calomne au ministre de l'Intérieur sur 'les forces de police affectées à la sécurité des gares et du métro bruxellois' (*C.R.I.*, Chambre, 2016-2017, 8 mars 2017, COM 613, p. 1, Q. nº 17084)

Question de J.-M. Nollet au ministre de l'Intérieur sur 'la présence de plongeurs travaillant avec de faux certificats dans la centrale nucléaire de Tihange' (*C.R.I.*, Chambre, 2016-2017, 8 mars 2017, COM 613, p. 29, Q. nº 17052)

Question de K. Jadin au ministre de la Mobilité sur 'le technicien radicalisé remercié' (*Q.R.*, Chambre, 2016-2017, 10 mars 2017, nº 109, p. 317, Q. nº 2015)

Question de F. Kir au ministre de l'Intérieur sur 'la recrudescence d'agressions envers les gardiens de parking' (*C.R.I.*, Chambre, 2016-2017, 15 mars 2017, COM 621, p. 2, Q. nº 16957)

Question d'E. Kir au ministre de l'Intérieur sur 'le rapatriement à Bagdad d'un suspect de terrorisme' (*C.R.I.*, Chambre, 2016-2017, 15 mars 2017, COM 621, p. 6, Q. nº 17093)

Question d'E. Kir au ministre de l'Intérieur sur 'les propos du ministre dans la presse dans le cadre de la lutte contre le terrorisme' (*C.R.I.*, Chambre, 2016-2017, 15 mars 2017, COM 621, p. 31, Q. nº 17237)

Question de Ph. Pivin au ministre de l'Intérieur sur 'la situation des djihadistes belges de retour de Syrie et d'Irak' (*C.R.I.*, Chambre, 2016-2017, 16 mars 2017, PLEN 161, p. 13, Q. nº 1914)

Question de D. Ducarme au ministre de l'Intérieur sur 'les attentats de Londres' (*C.R.I.*, Chambre, 2016-2017, 23 mars 2017, PLEN 162, p. 40, Q. nº 1946)

Question de K. Metsu au ministre de la Justice sur les 'allocations perçues par les combattants partis en Syrie' (*Q.R.*, Chambre, 2016-2017, 24 mars 2017, nº 111, p. 250, Q. nº 644)

Question de K. Metsu au ministre de la Justice sur le 'suivi des combattants rentrés de Syrie et des tentatives de départ' (*Q.R.*, Chambre, 2016-2017, 24 mars 2017, nº 111, p. 260, Q. nº 1226)

Question de A. Top au ministre de la Défense sur 'la critique du président syrien Bachar Al-Assad' (*C.R.I.*, Chambre, 2016-2017, 29 mars 2017, COM 632, p. 2, Q. nº 16561)

Questions jointes de G. Vanden Burre et W. Demeyer au ministre de la Justice sur 'le potentiel attentat évité à Anvers et la réaction du bourgmestre Bart De Wever' (*C.R.I.*, Chambre, 2016-2017, 30 mars 2017, COM 634, p. 24, Q. nºs 17514 et 17558)

Questions jointes de S. Van Hecke et A. Top au ministre l'Intérieur, sur 'la conférence de presse organisée par le bourgmestre d'Anvers et le chef de corps de la police en dépit de l'avis rendu par le parquet fédéral' (*C.R.I.*, Chambre, 2016-2017, 30 mars 2017, PLEN 163, p. 16, Q. n^{os} 1957 à 1959)

Question de P. Pivin au ministre de la Justice sur les 'services de renseignements – échanges d'information avec les pays étranger' (*Q.R.*, Chambre, 2016-2017, 31 mars 2017, n^{o} 112, p. 142, Q. n^{o} 1051)

Question de C. Van Cauter au ministre de la Justice sur 'les avis de la Sûreté de l'État dans le cadre de la reconnaissance des mosquées' (*Q.R.*, Chambre, 2016-2017, 31 mars 2017, n^{o} 112, p. 169, Q. n^{o} 1739)

Question de D. Ducarme au secrétaire d'État à l'Asile et la Migration sur le 'recrutement de personnes radicalisées dans les centres d'asile allemands' (*Q.R.*, Chambre, 2016-2017, 31 mars 2017, n^{o} 112, p. 290, Q. n^{o} 829)

Question de D. Ducarme au secrétaire d'État à l'Asile et la Migration sur la 'lutte contre le terrorisme – « screening »' (*Q.R.*, Chambre, 2016-2017, 31 mars 2017, n^{o} 112, p. 292, Q. n^{o} 838)

Question de M. De Coninck au secrétaire d'État à l'Asile et la Migration sur 'la gestion des combattants de Syrie' (*Q.R.*, Chambre, 2016-2017, 31 mars 2017, n^{o} 112, p. 319, Q. n^{o} 913)

Question de W. De Vriendt au secrétaire d'État à l'Asile et la Migration sur 'la procédure de régularisation médicale' (*Q.R.*, Chambre, 2016-2017, 31 mars 2017, n^{o} 112, p. 341, Q. n^{o} 953)

Question de D. Ducarme au ministre de la Justice sur la 'concrétisation du protocole créant la Belgian Intelligence Academy' (*Q.R.*, Chambre, 2016-2017, 7 avril 2017, n^{o} 113, p. 171, Q. n^{o} 1362)

Question de J.-M. Nollet au ministre de la Justice sur 'l'intervention de la Sûreté de l'État dans les entreprises' (*Q.R.*, Chambre, 2016-2017, 7 avril 2017, n^{o} 113, p. 176, Q. n^{o} 1608)

Question de B. Pas au ministre de la Justice sur 'les activités du groupe islamiste Hizb ut-Tahrir' (*Q.R.*, Chambre, 2016-2017, 7 avril 2017, n^{o} 113, p. 177, Q. n^{o} 1573)

Question de B. Pas au ministre de la Justice sur 'les mineurs entretenant des liens avec les milieux terroristes' (*Q.R.*, Chambre, 2016-2017, 7 avril 2017, n^{o} 113, p. 186, Q. n^{o} 1706)

Question de B. Pas au ministre de la Justice sur les 'organisations humanitaires qui se servent de la coopération au développement comme couverture à leurs activités d'extrémisme et de terrorisme' (*Q.R.*, Chambre, 2016-2017, 7 avril 2017, n^{o} 113, p. 189, Q. n^{o} 1747)

Question de K. Jadin au ministre de l'Intérieur sur 'les mineurs placés pour leurs liens avec le terrorisme' (*Q.R.*, Chambre, 2016-2017, 24 avril 2017, n^{o} 115, p. 110, Q. n^{o} 1867)

Question de B. Pas au ministre de l'Intérieur sur 'la déradicalisation' (*Q.R.*, Chambre, 2016-2017, 24 avril 2017, n^{o} 115, p. 117, Q. n^{o} 1887)

Question de K. Metsu au ministre de la Justice sur 'les mesures prises pour lutter contre le terrorisme – le screening des prédicateurs' (*Q.R.*, Chambre, 2016-2017, 24 avril 2017, n^{o} 115, p. 177, Q. n^{o} 1172)

Question de B. Pas au ministre de la Justice sur 'les imams en Belgique' (*Q.R.*, Chambre, 2016-2017, 24 avril 2017, n^{o} 115, p. 180, Q. n^{o} 1410)

Question de G. Dallemagne au ministre de la Justice sur les 'transferts de fonds étrangers au bénéfice de mosquées en Belgique – travaux de la CTIF' (*Q.R.*, Chambre, 2016-2017, 24 avril 2017, nº 115, p. 183, Q. nº 1465)

Question de B. Pas au ministre de la Justice sur 'le prêcheur de haine Hamzat Chumakov' (*Q.R.*, Chambre, 2016-2017, 24 avril 2017, nº 115, p. 191, Q. nº 1568)

Question de B. Pas au ministre de la Justice sur 'le financement du terrorisme' (*Q.R.*, Chambre, 2016-2017, 24 avril 2017, nº 115, p. 211, Q. nº 1673)

Question de B. Pas au secrétaire d'État à l'Asile et la Migration sur 'la délivrance de visas à des imams (*Q.R.*, Chambre, 2016-2017, 24 avril 2017, nº 115, p. 394, Q. nº 680)

Question d'O. Maingain au ministre des Affaires étrangères sur 'l'espionnage par l'ambassade turque de sa diaspora en Belgique' (*C.R.I.*, Chambre, 2016-2017, 26 avril 2017, COM 648, p. 15, Q. nº 17764)

Question de M. De Coninck au secrétaire d'État à l'Asile et la Migration sur 'les visas délivrés aux imams' (*C.R.I.*, Chambre, 2016-2017, 3 mai 2017, COM 651, p. 35, Q. nº 17921)

Question d'A. Top au ministre de la Mobilité sur 'les mesures antiterrorisme pour les gares bruxelloises' (*C.R.I.*, Chambre, 2016-2017, 3 mai 2017, COM 655, p. 8, Q. nº 17826)

Question de B. Pas au ministre de la Justice sur 'l'opération « Vigilant Guardian »' (*Q.R.*, Chambre, 2016-2017, 5 mai 2017, nº 116, p. 446, Q. nº 1117)

Question de B. Pas au ministre de l'Intérieur sur les 'polices fédérale et locale – évolution' (*Q.R.*, Chambre, 2016-2017, 16 mai 2017, nº 117, p. 132, Q. nº 1291)

Question de K. Lalieux au ministre de l'Intérieur sur 'la sécurité dans les transports en commun' (*Q.R.*, Chambre, 2016-2017, 16 mai 2017, nº 117, p. 150, Q. nº 1921)

Question de K. Jadin au ministre de l'Intérieur sur les 'pistolets à impulsion électrique pour les polices locales' (*Q.R.*, Chambre, 2016-2017, 16 mai 2017, nº 117, p. 173, Q. nº 2024)

Question de D. Ducarme au ministre de l'Intérieur sur 'l'utilisation du taser' (*Q.R.*, Chambre, 2016-2017, 16 mai 2017, nº 117, p. 184, Q. nº 2058)

Question d'E. Kir au ministre de l'Intérieur sur la 'gare du Nord – contrôles de police dans le cadre de la lutte contre le terrorisme' (*Q.R.*, Chambre, 2016-2017, 16 mai 2017, nº 117, p. 241, Q. nº 2145)

Question de Ph. Goffin au ministre de la Justice sur 'les conseillers islamiques auprès des établissements pénitentiaires' (*Q.R.*, Chambre, 2016-2017, 16 mai 2017, nº 117, p. 306, Q. nº 208)

Question de B. Pas au secrétaire d'État à l'Asile et la Migration sur 'les prédicateurs de haine' (*Q.R.*, Chambre, 2016-2017, 16 mai 2017, nº 117, p. 456, Q. nº 897)

Questions jointes de R. Hedebouw, B. Pas, V. Caprasse et W. De Vriendt au Premier ministre sur 'la mobilisation des effectifs policiers en vue du sommet OTAN et de la venue des présidents Trump et Erdogan en Belgique' (*C.R.I.*, Chambre, 2016-2017, 18 mai 2017, PLEN 169, p. 1, Q. nºs 2056, 2057, 2072 et 2059)

Échange de vues et questions jointes de R. Hedebouw, W. De Vriendt, P. Pirlot, V. Yüksel, A. Capoen, S. Crusnière et G. Dallemagne au ministre des Affaires étrangères sur 'le sommet de l'Otan du 25 mai 2017 à Bruxelles' (*C.R.I.*, Chambre, 2016-2017, 23 mai 2017, COM 670, p. 1, Q. nºs 18244, 18437, 18439, 18441, 18589, 18602, 18677, 18683 en 18748)

Questions jointes d'A. Carcaci, G. Dallemagne et D. Ducarme au ministre de l'Intérieur sur 'le phénomène de la radicalisation et l'attentat de Manchester' (*C.R.I.*, Chambre, 2016-2017, 24 mai 2017, PLEN 170, p. 6, Q. nos 2080, 2081 et 2082)

Question d'A. Lambrecht au ministre de la Justice sur 'l'agrément des mosquées' (*C.R.I.*, Chambre, 2016-2017, 30 mai 2017, COM 677, p. 20, Q. no 18513)

Question d'I. De Coninck au ministre de la Mobilité sur 'les trains supprimés' (*Q.R.*, Chambre, 2016-2017, 30 mai 2017, no 119, p. 177, Q. no 2002)

Question d'A. Lambrecht au ministre de la Justice sur 'la concertation relative à l'agrément des mosquées' (*C.R.I.*, Chambre, 2016-2017, 7 juin 2017, COM 681, p. 18, Q. no 18998)

Questions jointes d'O. Maingain et Ph. Blanchart au ministre de l'Intérieur sur 'la sécurité des écoles considérées comme liées à la mouvance güleniste' (*C.R.I.*, Chambre, 2016-2017, 7 juin 2017, COM 684, p. 4, Q. nos 17765 et 18321)

Questions jointes de B. Vermeulen, K. Jadin, H. Bonte et S. Lahaye-Battheu au ministre de l'Intérieur sur 'les Cellules de sécurité locale intégrale et les 'task forces' locales' (*C.R.I.*, Chambre, 2016-2017, 7 juin 2017, COM 684, p. 18, Q. nos 18182, 18889, 18969 et 19107)

Question de K. Jadin au ministre de l'Intérieur sur 'l'OCAM' – traque des radicaux' (*Q.R.*, Chambre, 2016-2017, 7 juin 2017, no 120, p. 160, Q. no 1964)

Question de F. Schepmans au ministre de l'Intérieur sur 'les mesures de sécurité des aéroports' (*Q.R.*, Chambre, 2016-2017, 7 juin 2017, no 120, p. 210, Q. no 2165)

Question de F. Dewinter au ministre de l'Intérieur sur 'le lien entre l'attentat de Manchester et la Belgique' (*C.R.I.*, Chambre, 2016-2017, 8 juin 2017, PLEN 172, p. 29, Q. no 2125)

Questions jointes d'A. Carcaci et Ph. Pivin au ministre de l'Intérieur sur 'le message de l'État islamique menaçant la Belgique' (*C.R.I.*, Chambre, 2016-2017, 8 juin 2017, PLEN 172, p. 32, Q. nos 2126 et 2127)

Questions jointes de K. Jadin, P. Buysrogge, A. Top et G. Calomne au ministre de la Défense sur 'les services de cybersécurité de la Défense' (*C.R.I.*, Chambre, 2016-2017, 14 juin 2017, COM 687, p. 2, Q. nos 18203, 18606, 19024 et 19163)

Question de K. Jadin au ministre de la Défense sur 'les essais de munitions et d'armes au Lager Elsenborn' (*C.R.I.*, Chambre, 2016-2017, 14 juin 2017, COM 687, p. 10, Q. no 18193)

Questions jointes de K. Jadin et V. Yüksel au ministre de la Défense sur 'les signes de radicalisation dans les casernes' (*C.R.I.*, Chambre, 2016-2017, 14 juin 2017, COM 687, p. 14, Q. nos 18655 et 19222)

Interpellation et questions jointes de G. Calomne et S. Crusnière au ministre de l'Intérieur sur ''intégration des empreintes digitales dans les cartes d'identité' (*C.R.I.*, Chambre, 2016-2017, 14 juin 2017, COM 688, p.14, Q. no 18737 et 224)

Question d'E. Kir au ministre de l'Intérieur sur 'le niveau de la menace à la suite des attentats de Londres' (*C.R.I.*, Chambre, 2016-2017, 14 juin 2017, COM 688, p. 33, Q. no 19082)

Question de F. Schepmans au ministre de l'Intérieur sur 'les exercices anti-terroristes' (*Q.R.*, Chambre, 2016-2017, 20 juin 2017, no 122, p. 139, Q. no 1740)

Question d'E. Burton au ministre de l'Intérieur sur 'le développement des CSIL dans les communes' (*Q.R.*, Chambre, 2016-2017, 20 juin 2017, no 122, p. 163, Q. no 2181)

Question de F. Schepmans au ministre de la Justice sur 'la collaboration entre l'EU INTCEN et la Sûreté de l'État' (*Q.R.*, Chambre, 2016-2017, 20 juin 2017, nº 122, p. 187, Q. nº 871)

Question de B. Pas au ministre de la Justice sur 'les conseillers islamiques dans les prisons' (*Q.R.*, Chambre, 2016-2017, 20 juin 2017, nº 122, p. 189, Q. nº 985)

Question de F. Dewinter au ministre de la Justice sur 'les services de renseignement – traitement des données' (*Q.R.*, Chambre, 2016-2017, 20 juin 2017, nº 122, p. 192, Q. nº 1191)

Question de S. de Coster-Bauchau au ministre de la Justice sur la 'Sûreté de l'État – recrutement d'agents' (*Q.R.*, Chambre, 2016-2017, 20 juin 2017, nº 122, p. 205, Q. nº 1799)

Question de F. Dewinter au ministre de la Justice sur 'le screening des combattants de l'État islamique parmi les candidats à l'asile' (*Q.R.*, Chambre, 2016-2017, 20 juin 2017, nº 122, p. 207, Q. nº 1831)

Questions jointes de R. Terwingen et K. Jadin au ministre de l'Intérieur sur 'les CSIL dans le suivi du radicalisme' (*C.R.I.*, Chambre, 2016-2017, 21 juin 2017, COM 694, p. 6, Q. nºs 19143 et 19217)

Questions jointes de B. Pas, G. Dallemagne, K. Degroote, Ph. Pivin, H. Vuye, S. Van Hecke, H. Bonte, A. Frédéric, S. Verherstraeten en P. Dewael au Premier ministre sur 'l'attentat manqué à Bruxelles-Central Belgique' (*C.R.I.*, Chambre, 2016-2017, 22 juin 2017, PLEN 174, p. 1, Q. nºs 2158 et 2167)

Question d'E. Kir au ministre de l'Intérieur sur la 'Banque de données nationale générale. – fichage des citoyens belges' (*Q.R.*, Chambre, 2016-2017, 27 juin 2017, nº 123, p. 174, Q. nº 2247)

Question d'E. Van Hoof au ministre de l'Intérieur sur 'les signalements de discrimination à l'IEFH' (*C.R.I.*, Chambre, 2016-2017, 4 juillet 2017, COM 700, p. 1, Q. nº 19034)

Questions jointes de G. Dallemagne, K. Degroote et R. Miller au Premier ministre sur 'l'attaque terroriste imminente' (*C.R.I.*, Chambre, 2016-2017, 6 juillet 2017, PLEN 178, p. 1, Q. nºs 2201 à 2203)

Question de G. Calomne au ministre de l'Intérieur sur 'la protection des représentations diplomatiques étrangères' (*Q.R.*, Chambre, 2016-2017, 7 juillet 2017, nº 124, p. 196, Q. nº 2255)

Questions jointes de Ph. Pivin au ministre de l'Intérieur sur 'la coopération avec les entités fédérées dans le cadre de la lutte contre la radicalisation' (*C.R.I.*, Chambre, 2016-2017, 12 juillet 2017, COM 712, p. 5, Q. nºs 19295 et 19870)

Question de G. Dallemagne au ministre de l'Intérieur sur 'l'adoption par les services de sécurité d'un modèle standard pour objectiver les processus de radicalisation' (*C.R.I.*, Chambre, 2016-2017, 12 juillet 2017, COM 712, p. 20, Q. nº 19621)

Question de V. Yüksel au ministre de l'Intérieur sur 'l'actualisation de la liste de l'OCAM' (*C.R.I.*, Chambre, 2016-2017, 12 juillet 2017, COM 712, p. 36, Q. nº 19843)

Question de P. Pivin au ministre de l'Intérieur sur 'le radicalisme et l'endoctrinement via internet et les réseaux sociaux' (*C.R.I.*, Chambre, 2016-2017, 12 juillet 2017, COM 712, p. 46, Q. nº 19866)

Questions jointes de J. Van den Bergh, D. Geerts et K. Jadin au ministre de la Mobilité sur 'le contrôle des voyageurs sur les trains internationaux' (*C.R.I.*, Chambre, 2016-2017, 12 juillet 2017, COM 714, p. 1, Q. nºs 18790, 18797 et 18874)

Question de B. Pas au ministre de l'Intérieur sur 'les cellules de sécurité intégrale locale' (*Q.R.*, Chambre, 2016-2017, 14 juillet 2017, nº 125, p. 139, Q. nº 2157)

Question de K. Jadin au ministre de l'Intérieur sur 'la mise en place d'une cellule belge en Turquie' (*Q.R.*, Chambre, 2016-2017, 14 juillet 2017, nº 125, p. 162, Q. nº 2302)

Question de K. Jadin au ministre de l'Emploi sur le 'versement d'allocations de chômage aux personnes liées à des activités terroristes' (*Q.R.*, Chambre, 2016-2017, 27 juillet 2017, nº 126, p. 202, Q. nº 934)

Question de K. Jadin au ministre de de l'Intérieur sur 'les personnes placées sous protection' (*Q.R.*, Chambre, 2016-2017, 27 juillet 2017, nº 126, p. 153, Q. nº 2294)

Question de B. Pas au ministre de la Justice sur 'le nombre d'attentats déjoués' (*Q.R.*, Chambre, 2016-2017, 27 juillet 2017, nº 126, p. 360, Q. nº 1590)

Question de B. Pas au ministre de la Justice sur 'le financement des mosquées au départ de l'étranger' (*Q.R.*, Chambre, 2016-2017, 27 juillet 2017, nº 126, p. 363, Q. nº 1633)

Question de Ph. Pivin au ministre de la Justice sur la 'gestion et contrôle des lieux de cultes' (*Q.R.*, Chambre, 2016-2017, 27 juillet 2017, nº 126, p. 368, Q. nº 1735)

Question de K. Van Vaerenbergh au ministre de la Justice sur les 'prisons – mesures contre le radicalisme' (*Q.R.*, Chambre, 2016-2017, 27 juillet 2017, nº 126, p. 376, Q. nº 1856)

Question d'A. Frédéric au ministre de la Justice sur le 'personnel détaché au sein du cabinet' (*Q.R.*, Chambre, 2016-2017, 27 juillet 2017, nº 126, p. 387, Q. nº 1880)

Question de M. Van Hees au ministre de la Défense sur 'les résultats du sommet de l'OTAN' (*Q.R.*, Chambre, 2016-2017, 27 juillet 2017, nº 126, p. 491, Q. nº 1225)

Question de F. Dewinter au ministre de l'Intérieur sur 'le retour de combattants partis en Syrie ou de membres d'organisations islamiques violentes actives au Moyen-Orient' (*Q.R.*, Chambre, 2016-2017, 16 août 2017, nº 127, p. 221, Q. nº 2026)

Question de D. Ducarme au ministre de l'Intérieur sur le 'suivi des personnes revenues ou ayant échoué à se rendre en Syrie' (*Q.R.*, Chambre, 2016-2017, 16 août 2017, nº 127, p. 260, Q. nº 930)

Question d'E. Kir au ministre de l'Intérieur sur 'les propos dans la presse du ministre de l'Intérieur dans le cadre de la lutte contre le terrorisme' (*Q.R.*, Chambre, 2016-2017, 16 août 2017, nº 127, p. 296, Q. nº 1873)

Question de L. Onkelinx au ministre de la Justice sur le 'contrôle budgétaire – moyens de la Sûreté de l'État' (*Q.R.*, Chambre, 2016-2017, 16 août 2017, nº 127, p. 326, Q. nº 1982)

Question de S. de Coster-Bauchau au ministre de l'Intérieur sur 'les blocs en béton anti camions-béliers' (*Q.R.*, Chambre, 2016-2017, 23 août 2017, nº 128, p. 245, Q. nº 2338)

Question de G. Dallemagne au ministre de l'Intérieur sur 'la sécurisation des évènements privés ouverts au public' (*Q.R.*, Chambre, 2016-2017, 23 août 2017, nº 128, p. 169, Q. nº 2159)

Question de Ph. Pivin au ministre de l'Emploi sur le 'contrôle de l'interdiction de vente des produits TATP' (*Q.R.*, Chambre, 2016-2017, 4 septembre 2017, nº 129, p. 160, Q. nº 1599)

Question de Ph. Blanchart au ministre de l'Intérieur sur 'la situation des écoles considérées comme liées au mouvement güleniste' (*Q.R.*, Chambre, 2016-2017, 4 septembre 2017, nº 129, p. 193, Q. nº 2211)

Question de Ph. Blanchart au ministre de l'Intérieur sur 'la situation des écoles considérées comme liées au mouvement güleniste' (*Q.R.*, Chambre, 2016-2017, 4 septembre 2017, nº 129, p. 202, Q. nº 2249)

Question de G. Calomne au ministre de l'Intérieur sur 'les mesures de protection des espaces culturels' (*Q.R.*, Chambre, 2016-2017, 4 septembre 2017, nº 129, p. 205, Q. nº 2254)

Question de K. Gabriëls au ministre de l'Intérieur sur 'la surveillance privée technologique' (*Q.R.*, Chambre, 2016-2017, 4 septembre 2017, nº 129, p. 209, Q. nº 2295)

Question de G. Dallemagne au ministre de l'Intérieur sur les 'returnees belges – rapport du Centre d'analyse du terrorisme' (*Q.R.*, Chambre, 2016-2017, 4 septembre 2017, nº 129, p. 215, Q. nº 2312)

Question de W. Demeyer au ministre de l'Intérieur sur les 'annonces faites à l'issue du Conseil des ministres exceptionnel du 14 mai 2017' (*Q.R.*, Chambre, 2016-2017, 11 septembre 2017, nº 130, p. 52, Q. nº 2272)

Question de Ph. Pivin au ministre de l'Intérieur sur la 'détection de radicalisation au sein des centres fermés' (*Q.R.*, Chambre, 2016-2017, 11 septembre 2017, nº 130, p. 69, Q. nº 2381)

Question de G. Dallemagne au ministre de l'Intérieur sur 'le recrutement et la formation des agents des renseignements (l'OCAM et la Sûreté de l'État)' (*C.R.I.*, Chambre, 2016-2017, 20 septembre 2017, COM 727, p. 23, Q. nº 20176)

Question d'O. Chastel au ministre de l'Intérieur sur 'la Sûreté de l'État – informateurs dans les milieux de l'islam radical' (*Q.R.*, Chambre, 2016-2017, 20 septembre 2017, nº 131, p. 63, Q. nº 2477)

Question de B. Pas au ministre de la Justice sur 'le démantèlement de lieux de culte prêchant le djihadisme' (*Q.R.*, Chambre, 2016-2017, 20 septembre 2017, nº 131, p. 106, Q. nº 1480)

Question de B. Pas au ministre de la Justice sur 'la circulaire du 18 juillet 2016 relative aux prédicateurs de haine' (*Q.R.*, Chambre, 2016-2017, 20 septembre 2017, nº 131, p. 121, Q. nº 1755)

Question de B. Pas au ministre de la Justice sur 'les rapports de la Sûreté de l'État concernant des mosquées du réseau Diyanet' (*Q.R.*, Chambre, 2016-2017, 20 septembre 2017, nº 131, p. 126, Q. nº 1839)

Question de F. Dewinter au ministre de la Justice sur 'la venue à l'occasion du Ramadan de 67 imams et morchidates en provenance du Maroc' (*Q.R.*, Chambre, 2016-2017, 20 septembre 2017, nº 131, p. 144, Q. nº 1955)

Question de B. Pas au ministre de la Justice sur les 'conseillers islamiques auprès des établissements pénitentiaires' (*Q.R.*, Chambre, 2016-2017, 20 septembre 2017, nº 131, p. 151, Q. nº 2006)

Question de Ph. Pivin au ministre de la Justice sur la 'détection de radicalisation au sein des centres fermés' (*Q.R.*, Chambre, 2016-2017, 20 septembre 2017, nº 131, p. 154, Q. nº 2036)

Question de Ph. Pivin au ministre de Finances sur la 'douane – contrôle de l'interdiction des produits précurseurs explosifs' (*Q.R.*, Chambre, 2016-2017, 20 septembre 2017, nº 131, p. 315, Q. nº 1722)

Questions jointes de G. Dallemagne au ministre de la Justice sur 'la réception par un détenu d'une lettre de recrutement de l'État islamique' (*C.R.I.*, Chambre, 2016-2017, 28 septembre 2017, PLEN 185, p. 10, Q. nº 2286)

Question de F. Dewinter au ministre de l'Intérieur sur 'la Grande Mosquée de Bruxelles' (*C.R.I.*, Chambre, 2017-2018, 5 octobre 2017, PLEN 186, p. 31, Q. nº 2319)

Question de F. Dewinter au ministre de la Justice sur 'le suivi des combattants de retour de Syrie' (*Q.R.*, Chambre, 2016-2017, 6 octobre 2017, nº 132, p. 466, Q. nº 1194)

Question de G. Calomne au ministre de la Défense sur les 'externalisation de missions de service public – risque de fuite de données sensibles' (*Q.R.*, Chambre, 2016-2017, 6 octobre 2017, nº 132, p. 585, Q. nº 1256)

Question de F. Dewinter au ministre de la Défense sur 'les demandeurs d'asile soupçonnés de terrorisme ou de complicité de terrorisme' (*Q.R.*, Chambre, 2016-2017, 6 octobre 2017, nº 132, p. 591, Q. nº 1265)

Question de J.-J. Flahaux au ministre de la l'Intérieur sur 'de nouveaux types de menaces terroristes' (*C.R.I.*, Chambre, 2017-2018, 18 octobre 2017, COM 755, p. 18, Q. nº 20620)

Question de B. Hellings au ministre de la Justice sur 'la mise à disposition des archives classifiées de la Sûreté de l'État en vue d'éclairer l'enquête des Nations Unies sur la mort suspecte de Dag Hammarskjöld' (*C.R.I.*, Chambre, 2017-2018, 18 octobre 2017, COM 756, p. 2, Q. nº 20973)

Question d'A. Frédéric au ministre de l'Intérieur sur 'la collaboration entre la police fédérale et les services de renseignements' (*C.R.I.*, Chambre, 2017-2018, 18 octobre 2017, COM 756, p. 27, Q. nº 21141)

Question de Ph. Pivin au ministre des Affaires étrangères sur la 'STIB – agents de sécurité – screening ANS' (*Q.R.*, Chambre, 2017-2018, 20 octobre 2017, nº 133, p. 232, Q. nº 987)

Question de G. Calomne au ministre de la Justice sur 'la communication par Interpol d'une liste de présumés terroristes.' (*Q.R.*, Chambre, 2017-2018, 20 octobre 2017, nº 133, p. 249, Q. nº 2074)

Question d'A. Top au ministre de la Défense sur 'le budget et l'effectif du SGRS' (*Q.R.*, Chambre, 2017-2018, 20 octobre 2017, nº 133, p. 326, Q. nº 1275)

Question de P. Buysrogge au ministre de la Justice sur 'VSSE et SGRS – fonds pour la rémunération des informateurs – rapport d'enquête de contrôle' (*Q.R.*, Chambre, 2017-2018, 20 octobre 2017, nº 134, p. 415, Q. nº 1224)

Questions jointes de B. Hellings, J. Fernandez, M. Van Hees, M. De Coninck et I. Poncelet au secrétaire d'État à l'Asile et la Migration sur 'les effets et les suites du jugement du tribunal de première instance de Liège concernant les rapatriements forcés actuels et futurs de ressortissants soudanais' (*C.R.I.*, Chambre, 2017-2018, 25 octobre 2017, COM 758, p. 1, Q. nºs 21184, 21332, 21481, 21486, 21555, 21564 et 21581)

Questions jointes d'I. De Coninck et V. Yüksel au ministre de la Mobilité sur 'l'engagement d'un combattant de Syrie comme conducteur de train' (*C.R.I.*, Chambre, 2017-2018, 7 novembre 2017, COM 761, p. 41, Q. nºs 21064 et 21110)

Question de B. Pas au ministre de la Justice sur 'la construction d'une mégamosquée à Gand' (*C.R.I.*, Chambre, 2017-2018, 8 novembre 2017, COM 765, p. 6, Q. nº 21463)

Question d'A. Top au ministre de la Justice sur 'la Belgian Intelligence' (*C.R.I.*, Chambre, 2017-2018, 8 novembre 2017, COM 765, p. 33, Q. nº 21597)

Questions jointes de R. Terwingen et J.-J. Flahaux au ministre de la Justice sur 'le rôle des TFL et des CSIL dans la nouvelle circulaire relative aux aspects de sécurité lors de la reconnaissance des communautés religieuses' (*C.R.I.*, Chambre, 2017-2018, 8 novembre 2017, COM 765, p. 8, Q. nºs 21135, 21398 et 21399)

Question de R. Deseyn au Premier ministre sur les 'smartphones sécurisés' (*Q.R.*, Chambre, 2017-2018, 15 novembre 2017, nº 135, p. 79, Q. nº 262)

Question de R. Deseyn au Premier ministre sur 'ransomware – Windows XP' (*Q.R.*, Chambre, 2017-2018, 15 novembre 2017, nº 135, p. 220, Q. nº 2233)

Question d'O. Chastel au ministre de l'Intérieur sur le 'service de protection rapprochée' (*Q.R.*, Chambre, 2017-2018, 15 novembre 2017, nº 135, p. 272, Q. nº 2476)

Question de B. Pas au ministre de l'Intérieur sur 'la protection des personnes menacées' (*Q.R.*, Chambre, 2017-2018, 15 novembre 2017, nº 135, p. 290, Q. nº 2535)

Question de B. Hellings au ministre de l'Intérieur sur la 'procédure de délivrance des documents de voyage aux réfugiés reconnus' (*Q.R.*, Chambre, 2017-2018, 15 novembre 2017, nº 135, p. 370, Q. nº 1170)

Question de B. Pas au ministre de la Justice sur 'les imams, mosquées et associations prêchant le radicalisme islamique' (*Q.R.*, Chambre, 2017-2018, 15 novembre 2017, nº 135, p. 375, Q. nº 1708)

Question de B. Pas au ministre de l'Intérieur sur 'le point de contact radicalisation de Fedasil' (*Q.R.*, Chambre, 2017-2018, 15 novembre 2017, nº 135, p. 498, Q. nº 905)

Question de B. Pas au ministre de l'Intérieur sur la 'radicalisation dans les centres d'asile' (*Q.R.*, Chambre, 2017-2018, 15 novembre 2017, nº 135, p. 533, Q. nº 1102)

Question de K. Jadin au ministre de l'Intérieur sur 'le retrait temporaire de la carte d'identité' (*Q.R.*, Chambre, 2017-2018, 21 novembre 2017, nº 136, p. 49, Q. nº 2415)

Question de G. Calomne au ministre de l'Intérieur sur 'les effectifs de police dans les gares bruxelloises' (*Q.R.*, Chambre, 2017-2018, 21 novembre 2017, nº 136, p. 54, Q. nº 2431)

Question de N. Lijnen au ministre de l'Intérieur sur 'les pratiques de guérison de l'homosexualité' (*Q.R.*, Chambre, 2017-2018, 21 novembre 2017, nº 136, p. 57, Q. nº 2485)

Question de G. Dallemagne au ministre de la Défense sur 'l'implication militaire belge au Mali' (*Q.R.*, Chambre, 2017-2018, 21 novembre 2017, nº 136, p. 179, Q. nº 1315)

Question de F. Dewinter au ministre de l'Intérieur sur 'la venue à l'occasion du Ramadan de 67 imams et morchidates en provenance du Maroc' (*Q.R.*, Chambre, 2017-2018, 21 novembre 2017, nº 136, p. 266, Q. nº 1187)

Question de G. Calomne au ministre de la Justice sur 'la signature d'un protocole de coopération avec le FBI' (*C.R.I.*, Chambre, 2017-2018, 22 novembre 2017, COM 767, p. 18, Q. nº 21956)

Question de G. Calomne au ministre de l'Intérieur sur 'le 'Blue Light Mobile' pour les situations de crise' (*C.R.I.*, Chambre, 2017-2018, 22 novembre 2017, COM 770, p. 36, Q. nº 21402)

Question de F. Dewinter au ministre de l'Intérieur sur 'la lutte contre les prédicateurs de la haine' (*C.R.I.*, Chambre, 2017-2018, 23 novembre 2017, PLEN 198, p. 21, Q. nº 2419)

Question de J.-J. Flahaux au ministre de l'Intérieur sur les 'éventuelles conséquences des returnees suite aux victoires territoriales kurdes contre l'EI en Syrie' (*Q.R.*, Chambre, 2017-2018, 28 novembre 2017, nº 137, p. 190, Q. nº 2591)

Question de G. Calomne au ministre des Finances sur 'le gel des avoirs bancaires des personnes soupçonnées de terrorisme' (*Q.R.*, Chambre, 2017-2018, 28 novembre 2017, nº 137, p. 373, Q. nº 1755)

Question de G. Calomne au ministre de l'Intérieur sur la 'lutte contre le terrorisme. – implication des services douaniers' (*Q.R.*, Chambre, 2017-2018, 28 novembre 2017, nº 137, p. 384, Q. nº 1770)

Questions jointes de K. Jadin et P. Buysrogge au ministre de la Défense sur 'les discussions autour d'une cyberarmée belge' (*C.R.I.*, Chambre, 2017-2018, 29 novembre 2017, COM 771, p. 1, Q. nºs 21290 et 21375)

Question de P. Buysrogge au ministre de la Défense sur 'le SGRS' (*C.R.I.*, Chambre, 2017-2018, 29 novembre 2017, COM 771, p. 13, Q. nº 21381)

Questions jointes de G. Dallemagne, G. Calomne et G. Vanden Burre au ministre de la Défense sur 'les émeutes à Bruxelles' (*C.R.I.*, Chambre, 2017-2018, 29 novembre 2017, COM 773, p. 45, Q. nºs 22063, 22105 et 22148)

Question de G. Calomne au ministre de l'Intérieur sur 'la signature d'un protocole de coopération avec le FBI' (*C.R.I.*, Chambre, 2017-2018, 29 novembre 2017, COM 773, p. 42, Q. nº 21955)

Question de K. Degroote au ministre de l'Intérieur sur 'les dispenses pour la fonction de garde champêtre particulier' (*C.R.I.*, Chambre, 2017-2018, 6 décembre 2017, COM 777, p. 13, Q. nº 22260)

Question de M. De Coninck au ministre de l'Intérieur sur 'l'avenir de la formation de gardien de patrimoine' (*Q.R.*, Chambre, 2017-2018, 11 décembre 2017, nº 139, p. 222, Q. nº 2329)

Question de Ph. Pivin au ministre de l'Intérieur sur la 'cellule belge de contrôle des potentiels returnees' (*Q.R.*, Chambre, 2017-2018, 11 décembre 2017, nº 139, p. 225, Q. nº 2374)

Question d'O. Chastel au ministre de l'Intérieur sur 'les départs en Syrie' (*Q.R.*, Chambre, 2017-2018, 11 décembre 2017, nº 139, p. 253, Q. nº 2585)

Question de K. Jadin au ministre de l'Intérieur sur 'l'avis du CTED' (*Q.R.*, Chambre, 2017-2018, 11 décembre 2017, nº 139, p. 259, Q. nº 2627)

Question de V. Yüksel au ministre de l'Intérieur sur 'l'approche adoptée concernant les convertis des FTF et HTF' (*Q.R.*, Chambre, 2017-2018, 11 décembre 2017, nº 139, p. 272, Q. nº 2650)

Question de M. De Coninck au secrétaire d'État à l'Asile et la Migration sur 'l'octroi d'un visa à des imams' (*Q.R.*, Chambre, 2017-2018, 11 décembre 2017, nº 139, p. 415, Q. nº 947)

Question de B. Pas au secrétaire d'État à l'Asile et la Migration sur 'l'octroi d'un visa à des imams' (*Q.R.*, Chambre, 2017-2018, 11 décembre 2017, nº 139, p. 433, Q. nº 1094)

Question de G. Calomne au secrétaire d'État à l'Asile et la Migration sur 'l'identification de cas de radicalisation parmi les candidats réfugié' (*Q.R.*, Chambre, 2017-2018, 11 décembre 2017, nº 139, p. 446, Q. nº 1192)

Question de B. Pas au secrétaire d'État à l'Asile et la Migration sur 'le Memorandum of Understanding signé avec le Maroc' (*Q.R.*, Chambre, 2017-2018, 11 décembre 2017, nº 139, p. 455, Q. nº 1235)

Question de G. Dallemagne au ministre de la Justice sur 'la convention de concession de la Grande Mosquée de Bruxelles et du Centre Islamique et Culturel de Belgique' (*C.R.I.*, Chambre, 2017-2018, 13 décembre 2017, COM 780, p. 5, Q. nº 22286)

Question de G. Calomne au ministre de la Justice sur 'les enquêtes de sécurité sur les personnes' (*Q.R.*, Chambre, 2017-2018, 18 décembre 2017, nº 140, p. 253, Q. nº 2141)

Question de B. Pas au secrétaire d'État à l'Asile et la Migration sur 'l'accord administratif avec l'Algérie – état des lieux' (*Q.R.*, Chambre, 2017-2018, 18 décembre 2017, nº 140, p. 472, Q. nº 1311)

ANNEXE D.
LES RECOMMANDATIONS DU COMITÉ PERMANENT R (2006-2016)

PRÉAMBULE

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. Ces recommandations découlent essentiellement des divers avis et enquêtes de contrôle. Elles figurent systématiquement dans le rapport d'enquête et sont ensuite reprises dans les rapports d'activités du Comité.[179]

Le *Rapport d'activités 2006* avait déjà offert un aperçu des recommandations les plus pertinentes que le Comité permanent R et ses Commissions de suivi successives avaient émises entre 1994 et 2005, ainsi qu'un aperçu du suivi qui leur avait été réservé.[180] Un exercice similaire a été réalisé dans le présent document pour la période 2006-2016. Il répond ainsi à une demande de la Commission d'enquête parlementaire.[181]

Les très nombreuses recommandations formulées au cours de cette période qui, dans l'intervalle, ont été concrétisées par les services de renseignement et de sécurité et par l'OCAM, n'ont plus été reprises. En revanche, le Comité a vérifié si les recommandations qui n'ont pas encore été mises en œuvre sont toujours d'actualité et, si cela s'avérait nécessaire et utile, les a reformulées.

En ce qui concerne la présentation des recommandations, la structure établie par les experts de la Commission d'enquête 'attentats terroristes' a été respectée. Une distinction a été opérée entre les recommandations destinées au pouvoir législatif, les recommandations adressées au pouvoir exécutif et, enfin, celles qui concernent les services eux-mêmes. Le Comité fait remarquer qu'une partie des recommandations qu'il avait avancées ont été

179 Le premier chapitre des rapports d'activités respectifs énumère les principales initiatives prises par les différents acteurs, dans la lignée des recommandations précédentes. Une attention particulière est portée aux recommandations que le Comité estime essentielles, mais qui n'ont pas encore été mises en œuvre. Le dernier chapitre du rapport d'activités recense les nouvelles recommandations.

180 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 1-20.

181 Dans le cadre de la discussion du *Rapport d'activités 2015*, il a en effet été suggéré que le Comité dresse *'une liste des recommandations non encore exécutées et que la Commission consacre une réunion aux recommandations afin de voir quelles initiatives elle pourrait prendre'* cf. *Doc. parl.* Chambre 2016-17, n°54-2185/001 (Rapport d'activités 2015 du Comité permanent de Contrôle des services de renseignement et de sécurité, Rapport fait au nom de la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de contrôle des services de renseignement et de sécurité), 7.

confirmées par les rapporteurs des Commissions d'enquête parlementaire. À noter que les recommandations reprises ci-après ne se limitent pas au domaine du terrorisme et du radicalisme ; il s'agit de recommandations – tant générales que très spécifiques (détaillées) – portant sur le fonctionnement des services de renseignement et de sécurité et de l'OCAM.

I. POUVOIR LÉGISLATIF

I.1 Généralités

I.1.1 International

1. Un cadre légal clair pour l'échange d'informations à caractère personnel avec l'étranger
En ce qui concerne la collaboration avec les services étrangers, le Comité a déjà insisté à plusieurs reprises pour que le Conseil national de sécurité élabore une directive en exécution des articles 19 et 20 L.R&S. En septembre 2016, les ministres de la Justice et de la Défense ont soumis au Conseil national de sécurité, dans une note, la '*Richtlijn aangaande de relaties van Belgische inlichtingendiensten met buitenlandse inlichtingendiensten*' (Directive concernant les relations des services de renseignement belges avec les services de renseignement étrangers' (traduction libre)), classifiée 'Confidentiel Loi 11.12.1998'. Cependant, la transmission d'informations et de données à caractère personnel à des services étrangers n'y est abordée que très sommairement. Le Comité maintient dès lors ses recommandations antérieures et estime qu'une initiative en la matière constitue une priorité.[182]

I.1.2 National

2. Une possibilité de rectifier en externe la classification définie par les services de renseignement
Par le passé, le Comité permanent R avait déjà recommandé la création d'un système permettant de rectifier la classification donnée par les services de renseignement belges si elle ne répondait pas aux dispositions légales. Le Comité a émis cette recommandation car il veut pouvoir faire rapport de manière significative à la Commission de suivi. En effet, si une classification qui s'avère injustifiée n'empêche pas le Comité de prendre connaissance des données qui ont fait l'objet d'une classification, il en va autrement lors de la rédaction d'un rapport final destiné à la Commission de suivi. Dans l'état actuel de la législation, on ne peut que faire appel au sens des responsabilités (sans engagement) de celui qui a classifié l'information. Le Comité a avancé la même recommandation dans un souci de préservation des droits du citoyen.

3. Définition des différents rôles de la VSSE
La VSSE rend divers avis aux autorités. Le Comité permanent R estimait que la définition des différents rôles attribués à la VSSE devait être précisée, par exemple, dans le cadre des procédures d'acquisition de la nationalité belge. La réglementation en matière de

[182] Il faut de toute façon veiller au respect du principe de prudence auxquels sont tenus les services de renseignement dans le cadre des échanges d'informations.

vérifications et d'enquêtes de sécurité peuvent constituer une source d'inspiration à cet égard.[183]

I.2 Modification de la Loi organique des services de renseignement et de sécurité

4. Banques de données communes et interconnexion entre les banques de données
Il faut s'efforcer de développer un meilleur échange d'informations et un meilleur flux au niveau horizontal. Il est vrai que cela nécessite un effort colossal pour élaborer, interconnecter et unifier les banques de données (communes). Cela requiert aussi plus de temps et de moyens que ce dont disposent les services actuellement. Cette problématique doit être clarifiée, et la position juste et propre à chaque service de renseignement doit être garantie.

5. Interprétation correcte de la notion d''assistance technique'
S'agissant de 'l'assistance technique' prêtée à la justice (art. 20 § 2 L.R&S), le Comité a déjà explicitement souligné à plusieurs reprises que cette disposition n'autorisait pas la VSSE (ni le SGRS) à utiliser les compétences de renseignement à des fins judiciaires. Les services de renseignement doivent y veiller en permanence.

6. Combler une lacune dans la loi en matière de rétention de données
Lors de l'élaboration de la réglementation relative au recours à des opérateurs, la nouvelle compétence de la VSSE et du SGRS, consistant à suivre les activités des services étrangers sur le territoire belge, n'a pas été prise en considération. Le Comité permanent R recommande que le législateur spécifie un délai maximum pour la prise de connaissance de métadonnées.

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

8. Révision de la réglementation en matière d'interceptions de communications étrangères
Dans des recommandations antérieures, le Comité avait attiré l'attention sur l'importance de réviser la réglementation en matière d'interceptions de communications étrangères effectuées par le SGRS. Des éléments pertinents à cet égard sont la mesure dans laquelle les interceptions doivent être ciblées ou non, la portée exacte de la possibilité de 'chercher' des signaux, le degré de précision du Plan d'écoute annuel, la

183 Il conviendrait également de prévoir explicitement la possibilité pour le procureur du Roi de recevoir, de traiter et d'utiliser des informations classifiées dans le cadre des procédures d'acquisition de la nationalité. Les droits de la personne concernée doivent évidemment être pris en considération. Il faudrait aussi réexaminer le court laps de temps dont dispose la VSSE pour formuler ses observations.

possibilité de faire du *datamining* dans des informations fournies en vrac, ainsi que la question de savoir s'il faut inscrire les opérations SIGINT étrangères dans le cadre d'un 'mandat international' plus large. Certains de ces aspects ont été précisés dans la Loi du 30 mars 2017, tandis que d'autres doivent encore être concrétisés.

9. Une réglementation légale relative au travail avec les informateurs
Il convient d'élaborer une réglementation légale claire en matière de travail avec les informateurs. Il convient aussi de réfléchir à l'opportunité de prévoir – dans des cas tout à fait exceptionnels et moyennant un contrôle démocratique approfondi – l'octroi d'une 'contrepartie' bien définie (financière ou non) à des informateurs qui peuvent disposer d'informations cruciales pour la sécurité de l'État de droit.

10. Une base légale pour le screening des informateurs
Pour pouvoir évaluer la pertinence et la fiabilité des informations fournies ou à fournir, les services de renseignement doivent pouvoir se faire une idée aussi précise que possible de l'intéressé (screening). Il faut dès lors prévoir une base légale qui fixe les grandes lignes de ce genre de contrôle.

11. Une réglementation légale relative à l'infiltration par des civils
Il arrive qu'un informateur soit suivi ou guidé de manière à opérer à certains moments comme infiltrant civil, lequel se voit confier de véritables missions de renseignement. Cette forme de recueil de renseignements est, à plusieurs égards, encore plus problématique que le travail 'classique' avec des informateurs. D'autre part, le service dispose de moyens de contrôle limités sur la manière dont la personne remplit ses 'missions'. Par conséquent, le Comité permanent R a réitéré sa recommandation concernant l'élaboration d'une réglementation légale.

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

13. Le rôle des services de renseignement dans le cadre de certains investissements étrangers dans des secteurs présentant un intérêt militaire et stratégique
Le Comité permanent R a jugé souhaitable que soit élaborée une réglementation légale en matière de contrôle et de surveillance des investissements étrangers et des activités commerciales dans des secteurs qui sont considérés comme étant d'une importance stratégique et militaire pour la Belgique. Il conviendrait de définir le rôle des services de renseignement à cet égard. Le Comité permanent R a également estimé que l'intérêt militaire potentiel d'une entreprise établie en Belgique devrait faire l'objet d'une attention préventive du SGRS lors de son passage aux mains d'un groupe étranger.

1.4. Modification de la Loi relative à l'analyse de la menace

14. Définition de la notion de 'renseignements pertinents'
La notion de 'renseignements pertinents' (art. 6 L.OCAM) doit être clarifiée.

II. POUVOIR EXÉCUTIF

II.1. Généralités

II.1.1 International – Européen

15. Vers une meilleure approche (européenne) en ce qui concerne les informations classifiées (équipements techniques et homologation)
Le Comité permanent R a recommandé la plus grande prudence dans le choix des équipements techniques sécurisés qui seraient utilisés pour traiter les informations sensibles et classifiées. Les équipements techniques doivent être évalués, certifiés et homologués – en termes de fiabilité et de sécurité – selon des critères et procédures qui répondent aux normes de l'Union européenne. Le Comité permanent R a également recommandé que l'octroi de marchés à des fournisseurs de matériel de ce type soit assorti d'une obligation de disposer d'une habilitation de sécurité. Lors de l'enquête de sécurité préalable, une attention particulière devrait être portée aux liens éventuels de ces fournisseurs avec certains services de renseignement étrangers.

16. Coordination de la représentation des services de police, des services administratifs et des services de renseignement et de sécurité aux forums internationaux
Il faut coordonner la représentation des services de police, des services administratifs et des services de renseignement et de sécurité aux forums internationaux.

II.1.2 National

17. Attirer du personnel doté des connaissances requises et appropriées – Promouvoir la diversité au sein des services
Tant pour la gestion des informateurs dans les milieux radicaux (HUMINT) que pour le suivi des sources ouvertes (OSINT et SOCMINT), les services devraient pouvoir faire appel à des agents de collecte et à des analystes qui maîtrisent les différentes langues et qui connaissent bien la mentalité de ces personnes (diversité).[184] Par exemple, pour pouvoir suivre l'islamisme radical de manière adéquate, les services de renseignement doivent disposer d'un personnel suffisant doté de connaissances, notamment en langue arabe (et ses dialectes).

[184] Pour atteindre cet objectif, il faut avant tout particulièrement veiller à ce que les personnes qui possèdent de telles connaissances s'inscrivent effectivement aux tests de recrutement. De plus, ces tests doivent être adaptés à ces personnes pour qu'elles ne soient pas exclues *a priori* en raison d'éventuelles lacunes dans la connaissance de nos langues nationales. Enfin, il convient d'être attentif à la manière dont les enquêtes de sécurité sont menées à l'égard de personnes qui ont séjourné à l'étranger.

18. Professionnaliser le fonctionnement des LTF
Le Comité permanent R recommande que les différents participants aux LTF s'informent mutuellement de leurs possibilités et besoins respectifs, mais aussi de leurs limites.

19. Ne pas utiliser des compétences de renseignement à des fins judiciaires
En ce qui concerne 'l'assistance technique' prêtée à la justice (art. 20 § 2 L.R&S), le Comité a déjà explicitement souligné à plusieurs reprises que cette disposition n'autorisait pas la VSSE (ni le SGRS) à utiliser les compétences de renseignement à des fins judiciaires. Les services de renseignement doivent y veiller en permanence.

20. La création d'une plateforme d'informations en matière de protection stratégique du potentiel économique et scientifique (PES)
Le Comité permanent R recommande la création d'une plateforme d'informations, par exemple sous la direction du Conseil national de sécurité, pour la protection stratégique du PES. Dans ce cadre, il convient de rassembler les autorités régionales et fédérales en charge de l'économie, les représentants du secteur privé et du monde de la recherche, les deux services de renseignement, le Centre pour la cybersécurité Belgique, le FCCU, l'OCAM, le Centre de crise et l'Autorité nationale de sécurité. Le Comité a déjà pu constater que des organisations jouissant d'une certaine expertise, comme la CTIF et la Banque nationale, disposaient également d'une foule d'informations qui ne sont pas toujours suffisamment exploitées. Cette plateforme pourrait faire office de plateforme d'échange d'informations et servir de base à une politique intégrée dans laquelle les services de renseignement et l'OCAM verraient leurs rôles respectifs précisés. L'ensemble devrait contribuer à une répartition claire des tâches entre tous les participants et à leur collaboration. D'autre part, les efforts doivent être simultanément poursuivis pour améliorer la cybersécurité. Le Centre pour la cybersécurité Belgique peut jouer ici un rôle capital. Ce point nécessite également une évaluation du caractère approprié de la Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques.

21. Homologation des systèmes ICT et cryptage
La mission d'homologation de systèmes ICT produits en Belgique, y compris leur cryptage au niveau national, doit être confiée sans délai à un service public comme l'Autorité nationale de sécurité (ANS) ou au Centre pour la cybersécurité Belgique.

22. Recommandations relatives à la Joint Information Box
Les Comités permanents R et P ont formulé diverses recommandations en vue d'un réexamen approfondi de la *Joint Information Box* (JIB). Le rôle de chaque service participant doit être précisé. Il en va de même pour l'OCAM, qui en tant que service d'analyse, peut démontrer sa plus-value par rapport à des informations fournies par les services d'appui. 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, le 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 actifs sur le terrain. Les niveaux locaux doivent avoir la possibilité 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. Et pour cause, il s'avère 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 qu'un examen approfondi soit effectué sur 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, 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.

Les Comités permanents R et P appuient 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.

23. Un accord de coopération entre les services de renseignement et les services de police

Une concertation structurée doit être mise en place entre, d'une part, les services de renseignement et, d'autre part, les services de police (Police fédérale et Police locale) afin d'échanger des informations via des procédures bien déterminées. L'absence d'accord de coopération entre ces services constitue sans aucun doute une faille dans notre système de sécurité.

24. Instruction du Conseil national de sécurité en matière d'enquêtes de sécurité

Le Comité estime qu'il est indiqué que le Conseil national de sécurité élabore une instruction dans le cadre des enquêtes de sécurité et de la présence d'un observateur neutre, et ce, indépendamment du service qui mène l'enquête et du statut de la personne qui fait l'objet de l'enquête.

Par ailleurs, le Comité juge utile que le personnel des entreprises ou des institutions qui traitent des substances susceptibles d'être utilisées dans le développement d'armes NRBC, soient systématiquement soumises à des enquêtes ou des vérifications de sécurité.

25. Appliquer le système des avis de sécurité aux autorisations de séjour pour les étrangers

Le système des avis de sécurité devrait également s'appliquer aux autorisations de séjour pour les étrangers et à la dérogation à la condition de nationalité pour les enseignants. Cela requiert toutefois une décision motivée de l'autorité compétente.

26. Collaboration interdépartementale en matière de cybersécurité, ICT-security et Cyberintelligence

Certains aspects des révélations d'Edward Snowden ont mis en évidence des faiblesses dans les systèmes de protection de réseaux IT d'acteurs privés et d'institutions publiques. Par conséquent, le Comité a une nouvelle fois insisté sur la nécessité d'accorder plus d'attention à la cybersécurité et la sécurité ICT (INFOSEC), et sur le fait que ces problématiques (qui ne relèvent pas uniquement des missions des services de renseignement) nécessitent une coopération interdépartementale. Par exemple, le Conseil national de sécurité a un rôle crucial à jouer dans ce domaine.

27. Accords de coopération contre la prolifération
En vue de lutter efficacement contre la prolifération, le Comité permanent R a recommandé que les différentes autorités concluent des accords de coopération formels. Ces accords étaient rendus nécessaires au vu de la complexité du phénomène, tant sur le plan technique qu'en matière de réglementation et de compétence. Ces accords de coopération doivent, d'une part, être conclus entre le niveau fédéral et le niveau régional en ce qui concerne l'harmonisation de la réglementation et la définition des sanctions et, d'autre part, entre tous les services qui ont une responsabilité sur le terrain en matière de contrôle et de surveillance.

II.2. Les services de renseignement en général

28. Résorber les déficits et renforcer les services de renseignement et de sécurité
Le Comité a toujours plaidé pour que les services de renseignement disposent de moyens suffisants, non seulement en termes d'effectifs et logistiques, mais aussi au niveau législatif. Ces recommandations ne visaient évidemment pas exclusivement une amélioration dans la lutte contre le terrorisme ; l'octroi des moyens nécessaires doit permettre d'exécuter comme il se doit toutes les tâches énumérées dans Loi organique des services de renseignement et de sécurité. Dans ce contexte, le Comité a fait remarquer que les effectifs de la VSSE suivaient complètement l'évolution budgétaire du service. Un creux en termes d'effectifs a été atteint en 2015. Ainsi, le Comité a noté une diminution de 15 % d'équivalents temps plein (ETP) début janvier 2015 par rapport à 2010. Début 2016, une augmentation a été constatée à la faveur du recrutement de nouveaux inspecteurs et analystes. En ce qui concerne le SGRS, aucune trajectoire budgétaire n'a pu être dessinée. Et pour cause, ce service ne dispose pas d'un budget propre, puisqu'il est géré comme une entité au sein de la Défense. Les chiffres disponibles concernant le personnel employé au SGRS montrent la relative stabilité du nombre d'ETP depuis 2007. Enfin, le Comité a souligné l'importance pour l'OCAM de disposer d'un budget et d'un cadre adéquats. Depuis sa création en 2006, cet organe a, en effet, un rôle important à jouer dans la lutte contre le terrorisme et l'extrémisme.

29. Examen de l'efficacité des moyens d'action dont disposent les services de renseignement
Le Comité recommande que les autorités examinent l'efficacité des moyens d'action dont disposent les services de renseignement et de sécurité sur le terrain et les limitations actuelles (par exemple les cartes GSM anonymes prépayées).

30. Exécuter les obligations reprises aux articles 19 & 20 L.R&S
Les ministres compétents et le Conseil national de sécurité doivent préciser certains aspects des conditions de coopération, d'échange d'informations et d'assistance technique (cf. la directive actuelle), et ainsi exécuter toutes les obligations énoncées aux articles 19 et 20 L.R&S.

31. Directive relative au travail avec les informateurs
Une directive générale reprenant tous les aspects du travail avec les informateurs s'impose. Il convient de veiller plus particulièrement à l'élaboration d'une analyse de risques formelle, qui énumère les différents risques, et à laquelle participe une personne ou un département qui n'a pas pris part à la rédaction de la proposition initiale de

recrutement. Les deux services de renseignement doivent réfléchir à la mise en place d'un système qui leur permette de prendre mutuellement connaissance de l'identité des informateurs avec lesquels l'autre service a décidé de ne plus collaborer.

32. La nécessité d'une couverture politique des accords de coopération
Le Comité estime que les services de renseignement doivent faire preuve d'une plus grande ouverture concernant les accords de coopération bilatéraux ou multilatéraux existants, et ce, en premier lieu à l'égard des ministres compétents. En effet, de tels accords de coopération peuvent contenir des engagements ou des choix qui requièrent une évaluation et une couverture politiques. En d'autres termes, les ministres compétents doivent être correctement informés afin d'être toujours en mesure de prendre leurs responsabilités au niveau politique. Il convient de remarquer que ce qui peut être considéré comme 'politiquement pertinent', ou ce qui ne l'est pas, peut évoluer au fil du temps.

33. Une orientation politique à définir par le Conseil national de sécurité
Le Comité ministériel du renseignement et de la sécurité avait été créé en vue d'orienter politiquement le travail de renseignement. Il avait notamment pour missions de définir, par directives, la politique générale du renseignement et de déterminer les priorités des deux services de renseignement. Le Comité juge souhaitable que le (nouveau) Conseil national de sécurité et, par extension, le Comité stratégique et le Comité de coordination du renseignement et de la sécurité, assument leur rôle de 'pilote' dans divers domaines, en partie sur les indications des deux services de renseignement.

34. Répartition claire et contraignante des tâches entre l'OCAM et les services de renseignement
La lutte contre le terrorisme exige souvent une réaction rapide. Les analystes n'ont donc pas souvent la possibilité de réaliser des analyses stratégiques. La collecte d'informations est quant à elle axée sur les besoins immédiats plutôt que sur une analyse à long terme. La VSSE doit mener une réflexion sur sa particularité en tant que service de renseignement et sur son rôle dans la lutte contre le terrorisme.

II.3. VSSE

II.4. SGRS

35. Approbation formelle de la liste en matière de protection du PES
Le Comité signale l'absence d'approbation formelle (requise par la loi) par le Conseil national de sécurité de la liste des entreprises dont le PES doit être protégé par le SGRS.

III. AUTORITÉS ET SERVICES

III.3. Les services de renseignement en général

International

36. Ne pas accepter de pays tiers des données qui ont été recueillies de manière illégale
La VSSE et le SGRS peuvent naturellement recevoir des informations ou des renseignements de la part de partenaires étrangers. Ils peuvent eux-mêmes traiter ces

informations et/ou les transmettre aux services belges compétents (p. ex. l'OCAM). Dans ce contexte, le Comité avait déjà souligné par le passé que *'le service destinataire doit au moins s'efforcer de découvrir de quelle manière les renseignements concernés ont été obtenus*', et ce, pour pouvoir, le cas échéant, ne pas accepter de pays tiers des informations qui ont été collectées illégalement.

37. Évaluation critique des règles de la culture internationale du renseignement – Souci de l'exactitude des informations et du fondement juridique de leur transmission
La Commission Libertés civiles, Justice et Affaires intérieures du Parlement européen '*invite les États membres à s'abstenir d'accepter des données provenant de pays tiers et ayant été collectées illégalement, ainsi que d'accepter que des gouvernements ou agences de pays tiers effectuent sur leur territoire des activités de surveillance contraires au droit national ou ne satisfaisant pas aux garanties juridiques spécifiées dans les instruments internationaux ou européens, notamment la protection des droits de l'homme au titre du traité UE, de la CEDH et de la Charte des droits fondamentaux de l'Union européenne.*' Le Comité permanent R a toutefois observé que dans la pratique, les 'services de renseignement fournisseurs' protègent généralement leurs sources (et donc l'origine d'un renseignement), ce que les 'services destinataires' acceptent. Cette forme d'entente fait partie de la culture internationale du renseignement, au même titre que la règle du service tiers, le principe *do ut des* et le devoir de réserve. 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, de veiller tout particulièrement 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 éventuelles répercussions pour les intéressés. Il faut par ailleurs tenter 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, portant, par exemple, sur la création d'une fonction de médiation ou un contrôle externe sur ces listes. En effet, actuellement, les instances nationales telles que le Comité permanent R ne sont pas compétentes pour contrôler le bien-fondé et la légitimité de telles listes et de leur contenu.

38. Standardisation des procédures dans le cadre des échanges internationaux
Dans le cadre des échanges internationaux, et plus particulièrement de la gestion des demandes d'informations provenant de correspondants étrangers, le Comité permanent R recommande d'élaborer des procédures structurées et standardisées au niveau international. Les demandes d'informations doivent obligatoirement contenir des éléments tels que le degré d'urgence, les délais de réponse… Elles doivent en outre être complétées par tout élément utile ou nécessaire à l'exécution de la demande. Il en va de même pour les instruments qui sont indispensables dans le cadre de la lutte contre le terrorisme, c'est-à-dire les listes nationales et internationales. Les listes dans lesquelles figurent des noms de terroristes ou de personnes radicalisées devraient être standardisées.

39. La nécessité d'une couverture politique des accords de coopération
(*supra* 32.)

40. Un respect strict de l'article 33 L.Contrôle, y compris au niveau international
L'article 33 § 2 L.Contrôle stipule que '*les services de renseignement, l'Organe de coordination pour l'analyse de la menace et les autres services d'appui transmettent d'initiative au Comité permanent R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services.*' Le Comité permanent R a dû constater que cette obligation n'était pas strictement respectée (en particulier en ce qui concerne le SGRS, l'OCAM et les services d'appui). Cette obligation s'applique également aux conventions, aux lettres d'intention (*Memorandum of Understanding* – MOU) ou aux accords conclus au niveau international, qu'ils soient bilatéraux ou multilatéraux. L'application stricte de cet article par les services contrôlés est une condition *sine qua non* pour permettre au Comité d'être efficace dans l'exercice de sa mission. Pour ces raisons, le Comité a de nouveau souligné l'importance de prendre l'initiative de transmettre toutes ces données dans les délais impartis.

National

41. Une meilleure coopération et recherche de synergies
La coordination et la coopération entre les deux services de renseignement doivent être améliorées, plus précisément par une exploitation rationnelle des moyens, par l'échange d'informations et de renseignements et par la production d'analyses communes, sans que ces services perdent leur identité et leurs caractéristiques spécifiques.

Ainsi, dans le cadre de la problématique syrienne, la collaboration entre les deux services de renseignement s'est avérée limitée et ponctuelle. Le Comité permanent R recommande que les deux services examinent les synergies possibles et l'éventualité d'une coopération renforcée, notamment en matière d'OSINT, SOCMINT, (CYBER)HUMINT et SIGINT. Par ailleurs, une représentation du SGRS par la VSSE au sein de certains groupes de travail (par exemple, au sein des LTF ou lors des contacts avec l'administration pénitentiaire) peut être envisagée.

42. Approche planifiée des processus de renseignement
Les processus de renseignement nécessitent une approche planifiée, qui consiste à définir au préalable les questions d'enquête en ce qui concerne les phénomènes à suivre, la manière dont les informations devront être collectées (méthodes de collecte) et la manière dont elles seront analysées (méthodes d'analyse).[185]

43. Réaliser des analyses stratégiques associées à la formulation d'hypothèses et à la définition de scénarios : produire des 'renseignements prédictifs' – Élaborer une méthodologie basée sur une approche multidisciplinaire
Le Comité permanent R est d'avis que la production de 'renseignements prédictifs' fait partie de l'essence même d'un service de renseignement. Le Comité recommande que la VSSE et le SGRS examinent avec leurs 'clients' dans quelle mesure des renseignements prédictifs sont nécessaires ou utiles, ce que le concept recouvre précisément, ce qu'on

[185] Dans le cadre de la lutte contre le terrorisme, une réaction urgente est souvent requise. C'est une des raisons pour lesquelles les analystes ne sont pas souvent en mesure d'établir des analyses stratégiques. Le recueil d'informations est quant à lui orienté sur les besoins immédiats plutôt que sur une analyse à long terme.

peut en attendre et comment les services pourraient concrétiser leurs ambitions en la matière.

Une méthode importante consiste à élaborer divers scénarios (p. ex. les 'scénarios du pire') et à poser des hypothèses qui pourront être confirmées ou infirmées par la suite. Ce précieux instrument méthodologique devrait pouvoir être davantage utilisé. Le Comité estime que de tels scénarios se conçoivent de préférence dans un cadre multidisciplinaire : un scénario terroriste a des composantes civiles *et* militaires, ce qui requiert une collaboration entre la VSSE et le SGRS.

44. La création d'une plateforme de coopération commune

Le Comité a dû constater qu'avant les révélations d'Edward Snowden, la VSSE et le SGRS n'avaient jamais échangé d'informations sur les menaces émanant de la captation massive de données et de l'espionnage politique et économique, et que cet échange mutuel n'a été que limité par la suite. Le Comité établit tout d'abord ce constat au regard de l'obligation légale qui incombe aux services en matière d'échange d'informations (art. 19 L.R&S). En outre, le Comité souligne l'existence d'un accord de coopération mutuel (Protocole d'accord du 12 novembre 2004), qui porte précisément sur la transmission spontanée d'informations relevant de la sphère de compétences de l'autre service. Après les révélations d'Edward Snowden, les mécanismes décrits dans ce Protocole d'accord auraient au moins dû être utilisés pour renforcer la position d'information des deux services. Le Comité a particulièrement mis en exergue la possibilité qui figure dans le Protocole de créer une 'plateforme de coopération *ad hoc*', au sein de laquelle des analyses communes peuvent être réalisées.

45. Interaction entre les banques de données des deux services

L'échange d'informations a toute son importance. Au niveau de la collecte de base, il y a sans aucun doute nettement plus d'informations au sein des différents services belges de police et de renseignement que ce à quoi la VSSE et le SGRS ont accès. Il faut donc s'efforcer de développer un meilleur échange d'informations et un meilleur flux au niveau horizontal. Il est vrai que cela nécessite un effort colossal pour élaborer, interconnecter et unifier les banques de données (communes). Cela requiert aussi plus de temps et de moyens que ce dont disposent les services actuellement. Cette problématique doit être clarifiée, et la position juste et propre à chaque service de renseignement doit être garantie.

46. Évaluer les principes du need to know et du need to share

Il a peut-être été compliqué pour le SGRS de se faire une idée globale des capacités et des stratégies SIGINT de grandes puissances étrangères, étant donné le nombre très restreint de personnes bénéficiant d'un accès direct aux informations SIGINT et la stricte confidentialité entourant ce genre d'informations. Aussi le Comité a-t-il estimé que le SGRS devrait réfléchir à la manière de mieux concilier les principes du *need to know* et du *need to share*.

47. Améliorer le recrutement et veiller à la diversité et aux connaissances linguistiques dans la gestion de la politique du personnel

(*supra* 17.)

48. Miser sur le HUMINT dans les milieux radicalisés et terroristes
Les informations recueillies via le HUMINT sont souvent décisives, en ce sens qu'elles contribuent utilement à l'élaboration d'une stratégie disruptive ou à empêcher un attentat. Même s'il n'est pas simple de recruter des sources dans les milieux terroristes et radicalisés, cela doit constituer une priorité.

49. Utilisation de techniques d'analyse standardisées
L'analyse est une composante essentielle du travail de renseignement. Il existe toutes sortes de techniques standardisées en la matière. L'utilisation de telles techniques n'a pas pour but de satisfaire à l'un ou l'autre axiome, mais bien d'éviter des manquements analytiques (erreurs cognitives ou factuelles). L'objectif est ici d'éviter des risques qui peuvent survenir dans les processus de renseignement et qui, au final, peuvent influencer la position d'information. Le Comité constate que les services ne recourent pas de façon cohérente à des méthodes d'analyse formelles. Par conséquent, il leur recommande de développer un plan déterminant clairement et en toute transparence leur position par rapport à cette problématique, la politique menée à cet égard et la manière dont ils maîtrisent les risques (analytiques).

50. Approche planifiée de phénomènes
Les processus de renseignement nécessitent une approche planifiée ou une 'conception', qui consiste à définir au préalable les questions d'enquête en ce qui concerne les phénomènes à suivre, la manière dont les informations doivent être collectées (méthodes de collecte) et la manière dont elles seront analysées (méthodes d'analyse). Ce genre de conception découle d'un niveau stratégique supérieur, mais diffère, par exemple, d'un plan de collecte classique, puisqu'il englobe tant les méthodes de collecte que d'analyse. La collecte et l'analyse peuvent ainsi gagner en rationalité, et les processus de renseignement, en efficacité. Les deux services en ont besoin. Le Comité permanent R recommande qu'ils intègrent une telle approche dans leur fonctionnement, et lors de la manifestation ou du développement d'un phénomène (comme par exemple la crise syrienne), qu'ils élaborent de façon réfléchie une conception globale de collecte et d'analyse. En principe, cette conception ne devrait pas seulement exister au sein de chaque service, mais devrait aussi prendre en considération (et idéalement utiliser) les capacités de collecte et d'analyse d'autres services.

51. Consultation des 'clients'
Le Comité permanent R réitère sa recommandation selon laquelle les deux services devraient demander explicitement à leurs 'clients' quels renseignements ils veulent exactement et comment ils les évaluent (*feedback*). Il s'agit d'une responsabilité partagée. D'une part, les services doivent spécifier à quelles conditions, comment et à qui ils veulent ou peuvent diffuser des renseignements et quelle 'ambition' on est en droit d'attendre du service à cet égard (renseignements descriptifs, explicatifs ou prédictifs). D'autre part, les clients doivent naturellement collaborer, c'est-à-dire préciser leurs attentes et leurs besoins (en renseignements).

52. Formation continue et contrôle réel de la qualité des rapports de collecte
Le Comité est conscient que dans le travail de renseignement, il n'est pas toujours évident de déterminer, au moment de la collecte, quelles informations se révéleront un jour

pertinentes ou non. Toujours est-il que les exigences en la matière, telles que celles décrites dans la L.R&S et dans la Loi relative à la protection de la vie privée (principe de finalité, adéquation, exactitude…), doivent être respectées. Ce qui signifie, par exemple, que la mention d'un événement donné dans un rapport de collecte et la façon dont il y est repris sont d'une importance capitale. La manière dont cet *input* doit avoir lieu devrait faire l'objet d'une formation continue et être soumise à un contrôle de qualité sérieux.

53. Forme, contenu et timing des 'produits d'analyse'
Le Comité avait déjà formulé une recommandation selon laquelle il faudrait donner une indication sur la ou les source(s) des informations dans les produits d'analyse destinés à d'autres autorités. En effet, cela peut aider le destinataire à évaluer la fiabilité du produit. Le Comité réitère cette recommandation. De plus, il convient d'émettre des instructions sur le moment où les produits d'analyse doivent être envoyés à d'autres autorités, ainsi que sur la forme sous laquelle ils doivent l'être. Il faut par ailleurs spécifier qui sont les destinataires.

54. Analyse de la menace commune en matière de PES
Les deux services de renseignement, l'OCAM et le Centre pour la cybersécurité Belgique doivent analyser ensemble le phénomène de la menace émanant de systèmes d'interception étrangers pour le PES belge et les infrastructures critiques.

55. Notification aux personnes qui font l'objet d'une enquête de sécurité
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.

56. L'organisation de sessions d'informations régulières sur l'utilisation des fonds spéciaux
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.

57. Expliciter l'attitude générale à adopter en termes de loyauté sur les réseaux sociaux
Le Comité permanent R recommande que les directions respectives des services de renseignement prennent des initiatives pour rendre plus explicite le cadre normatif (lois, arrêtés royaux, directives internes, code de déontologie) qui s'applique aux membres des services de renseignement. Il s'agit de préciser l'attitude générale de loyauté et de prudence attendue de ceux-ci, en particulier sur les réseaux sociaux, et les moyens de contrôle susceptibles d'être mis en œuvre à cet effet. Le Comité recommande également aux directions des services de prendre des dispositions particulières portant sur le caractère proactif du contrôle de l'utilisation de l'ICT et du comportement des agents sur les réseaux sociaux, à des fins professionnelles et/ou privées. Ces dispositions devront naturellement tenir compte des principes de finalité, de proportionnalité et de transparence, mais être adaptées ici aussi à la mission particulière des services. En outre, une procédure doit être mise en place pour permettre d'évaluer, en cas d'incident, les éventuels dommages pour l'intéressé et, pour le service, de réagir de manière appropriée et de prendre les mesures correctrices pour éviter une répétition d'un tel incident.

58. Transmission de toutes les informations pertinentes à l'OCAM
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.

59. La conclusion d'un accord de coopération entre les services de renseignement et les services de police
(*supra* 23.)

60. Notification aux personnes qui font l'objet d'une menace
Les services de renseignement doivent définir des critères de notification aux personnes qui font l'objet d'une menace (art. 19 L.R&S).

61. Intérêt pour la captation massive de données et pour l'espionnage politique et économique
Les deux services de renseignement doivent s'intéresser davantage aux risques inhérents aux nouvelles technologies en matière de captation massive de données et d'espionnage économique et politique, et ce, même si ces risques émanent de 'partenaires stratégiques'. À cet égard, il conviendrait de procéder à des analyses de risques prenant également en considération la présence d'institutions internationales sur le territoire belge. La VSSE et le SGRS doivent prêter attention à ces phénomènes afin de se forger une bonne position d'information. Cela leur permettrait de connaître les possibilités dont disposent d'autres services ainsi que leurs méthodes de travail, non seulement pour pouvoir, le cas échéant, informer les autorités, mais aussi pour prendre des contre-mesures et pour évaluer leurs propres techniques de recueil.

62. Décisions motivées, consultables et vérifiables
Le Comité était conscient de l'impossibilité pour un service de renseignement de suivre (aussi intensivement) quiconque représenterait une menace, ce qui s'explique aisément par les moyens limités dont il dispose. Il faut donc faire des choix. Ceux-ci doivent s'appuyer sur des analyses réelles aboutissant à une décision motivée, consultable et vérifiable. En l'espèce, le Comité a attiré l'attention sur le fait que la VSSE en a elle-même reconnu la nécessité dans son '*Instruction pour la collaboration bilatérale avec les correspondants*'. Sous l'en-tête '*Transparence et traçabilité*', une '*trace administrative*' est requise pour chaque action, entre autres en vue du contrôle exercé par le Comité permanent R.

III.4. VSSE

63. Respect de l'article 36bis de la Loi Vie privée
Le Comité recommande à la VSSE de prendre les initiatives nécessaires pour satisfaire à l'obligation énoncée à l'article 36*bis* de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel dans le cadre de l'échange d'informations avec l'administration pénitentiaire. Aux termes de cette disposition, les services doivent obtenir l'autorisation préalable du Comité sectoriel pour

l'autorité fédérale pour *'toute communication électronique de données personnelles par un service public fédéral'*.

64. Examen des flux d'informations et des moyens ICT
Le Comité permanent R recommande à la VSSE d'examiner ses processus de travail, les flux d'informations et les moyens ICT qui supportent l'ensemble.

65. Un nouveau protocole de coopération entre la VSSE et la DG EPI
Le Comité permanent R estime que le protocole de coopération entre la VSSE et la DG Établissements Pénitentiaires est dépassé dans sa forme actuelle. Le protocole doit être adapté ou réécrit pour pouvoir anticiper les défis futurs, tels que de nouveaux phénomènes et de nouvelles évolutions en termes d'usages et de méthodes. De plus, des pratiques qui se sont développées au fil des ans en marge du protocole actuel doivent être intégrées à ce dernier ou régularisées. Il convient de reprendre dans le protocole toutes les initiatives que la VSSE avait prises en dehors de celui-ci.

66. Un meilleur échange d'informations et un meilleur traitement des informations entre la VSSE et la DG EPI
Dans le cadre des échanges d'informations, le Comité permanent R estime que, puisque les informations doivent être concentrées au siège de Bruxelles, il faut privilégier un point de contact fixe (POC) pour l'échange d'informations via des postes provinciaux de la VSSE. Le Comité permanent R rappelle également que les différentes listes doivent être utilisées avec prudence (la liste de la DG EPI, la liste JIB…), et que leur finalité doit être clairement établie et respectée. Il convient aussi de trouver une solution pour l'échange d'informations 'défédéralisées' et de lever certaines ambiguïtés (comme la différenciation inutile des différentes modalités d'échange d'informations).

67. Accords de travail documentés entre la VSSE et le SPF Affaires étrangères
Bien qu'en matière de 'suivi du suivi de certaines diasporas', le SPF Affaires étrangères soit considéré comme le principal client de la VSSE, et bien qu'il soit le service tout indiqué pour aider la VSSE à contrer les activités des services de renseignement étrangers sur le territoire belge, il est surprenant de constater l'absence d'accords de travail documentés entre ces deux institutions.

68. Modification de la réglementation des fonds spéciaux
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.

69. Élaboration d'un code déontologique
Le Comité avait déjà recommandé 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 Sûreté de l'État, la VSSE élabore un(e) (proposition de) code de déontologie et la/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 définir les règles de 'bon usage' des médias sociaux par les agents des services de renseignement, aussi bien de la VSSE que du SGRS.

70. Finalisation du règlement de travail
Le Comité permanent R recommande que la VSSE ne tarde pas à finaliser et à valider son règlement de travail. Ce document devra au moins couvrir 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 que la VSSE se dote rapidement d'une structure *ad hoc* afin d'honorer ses obligations légales. La VSSE doit notamment désigner un conseiller en prévention et créer un réseau de personnes de confiance.

71. La conclusion d'un protocole d'accord avec les institutions européennes établies à Bruxelles
La présence sur le territoire belge d'institutions internationales telles que l'OTAN, le SHAPE et l'Union européenne fait de notre pays une cible privilégiée de l'espionnage international. La Belgique se doit dès lors de disposer de services de contre-espionnage efficaces. À la lumière de l'enquête de contrôle sur l'espionnage dans le bâtiment Juste Lipse, le Comité a réitéré sa recommandation d'octroyer à la VSSE et au SGRS suffisamment de moyens humains, techniques et légaux pour être en mesure de remplir efficacement cette mission. Le Comité permanent R recommandait plus spécifiquement que la VSSE conclue un protocole d'accord avec les institutions européennes établies à Bruxelles afin de mieux réglementer la collaboration et l'échange d'informations.

72. Examiner les processus de travail, le flux d'informations et les moyens ICT
En ce qui concerne la VSSE, le Comité a constaté que les concepts qui sous-tendent l'organisation de la banque de données posaient des problèmes de fond. Et pour cause, ils n'étaient pas interprétés de manière univoque ou appliqués en tant que tels. Le travail de renseignement risquait dès lors de perdre en efficacité et en efficience, puisque (tous) les rapports appropriés risquaient de ne pas 'remonter à la surface' lorsque cela s'avérerait nécessaire pour le travail d'analyse. Il y avait aussi un risque de tirer des conclusions erronées. Le Comité permanent R a recommandé à la VSSE de se pencher sur ses processus de travail, sur les flux d'informations et sur les moyens ICT qui supportent l'ensemble.

73. Actualisation des informations disponibles dans le cadre des naturalisations
Le Comité a recommandé que les informations fournies par la VSSE dans le cadre de l'obtention de la nationalité belge soient systématiquement actualisées si elles portent sur des '*faits personnels graves*'. De telles informations peuvent en effet constituer une contre-indication à l'octroi de la nationalité belge.

74. Restrictions en matière de recueil d'informations auprès de personnes (morales)
La VSSE est autorisée à recueillir, auprès de toute personne ou de toute organisation relevant du secteur privé, des informations relatives aux menaces qu'elle suit (art. 16 L.R&S). Il est vrai que la personne concernée reste liée par le secret professionnel auquel elle est tenue le cas échéant, ainsi que par les exigences de la Loi relative au traitement des

données à caractère personnel. Ces réglementations imposent des restrictions quant à la communication de données à des tiers (comme la VSSE). En outre, le citoyen a le droit de ne pas collaborer à une enquête de renseignement. Le Comité permanent R recommande que, dans leurs contacts avec des particuliers, les membres de la VSSE soient attentifs à la manière dont leur intervention est perçue par des personnes qui ne sont pas habituées à être en contact avec le service. Parallèlement, il convient de prêter attention, dans le cadre de la formation, à l'attitude correcte que les membres de la VSSE doivent adopter à l'égard des citoyens avec lesquels ils entrent en contact.

III.5. SGRS

75. Une gestion plus efficace et une harmonisation des banques de données (première étape) – une banque de donnée centralisée (seconde étape)
Le Comité permanent R recommande – et ce n'est pas la première fois – d'œuvrer de toute urgence au développement des banques de données du SGRS (saisie de données, classification univoque et générale des données, droits d'accès des différentes divisions), d'accélérer l'informatisation des collections papier, d'élaborer des systèmes de recherche performants et d'aborder en priorité plusieurs problèmes qui y sont liés (par exemple RFIMS, classement des informations entrantes au CCIRM).

76. Des traducteurs qualifiés pour le SIGINT
Le Comité a constaté la nécessité, pour la section SIGINT du SGRS, de disposer de traducteurs qualifiés.

77. Une description plus précise et l'envoi à temps de la liste d'interceptions
La liste d'interceptions est trop souvent transmise avec retard, ce qui empêche le Comité d'assurer pleinement sa mission de contrôle. Par conséquent, le Comité recommande que cette liste lui soit envoyée à temps. Par ailleurs, il a une nouvelle fois insisté sur l'importance d'une description plus précise des personnes et des organisations visées.

78. Sens critique dans l'analyse du comportement des personnes
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 liberté de culte reconnue à tout un chacun, d'autres attitudes révélatrices d'une dérive radicale et sectaire.

79. Modification de la réglementation sur les fonds spéciaux
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). En ce qui concerne les autres caisses, 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, soulignant 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 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.

80. Vigilance à l'égard de signes de conversion à l'islam radical
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 conseille donc au commandement du SGRS de fournir des instructions claires en ce sens à ses sections compétentes, en leur assignant la tâche d'identifier des indicateurs clairs 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. Il doit être particulièrement attentif 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 être sensibilisés à la problématique, notamment par l'organisation régulière de briefings d'information. Enfin, il est conseillé d'évaluer les canaux et les procédures de communication, tant avec les autorités disciplinaires au sein de la Défense 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 des mesures à prendre, notamment en matière d'habilitations de sécurité. Les défaillances éventuellement constatées dans les flux d'informations devraient être signalées au ministre afin qu'il puisse y remédier.

81. Révision du règlement de sécurité
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 affirmait avoir commencé à y travailler.

82. Rapport circonstancié en cas d'incident de sécurité
Le SGRS doit établir un rapport circonstancié de 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, éventuellement avec un projet de conclusion.

83. Conclusion de protocoles d'accord entre le SGRS et la DG EPI, l'Office des étrangers et le Commissariat général aux réfugiés et apatrides

84. Optimaliser les flux d'informations et les applications ICT
En ce qui concerne les flux d'informations et les applications ICT au sein du SGRS, le Comité avait, en son temps, formulé les recommandations concrètes suivantes : le système de *Request for Information* (RFI) améliorerait (considérablement) le traitement et le suivi des demandes d'information. Il fallait poursuivre et accélérer autant que possible l'intégration de la collecte de données et des banques de données. Le SGRS devait prendre diverses initiatives pour pouvoir gérer le volume important de données et de documentation. Il convenait tout d'abord de déterminer quelles étaient les informations nécessaires à la réalisation des objectifs et des produits à fournir. De plus, il fallait veiller à une bonne collaboration entre les services de collecte et les bureaux d'analyse. Enfin, il convenait d'investir dans les moyens humains et l'ICT qui sont absolument nécessaires. De manière générale, le Comité recommandait d'investir suffisamment de moyens dans les technologies de l'information et la communication (ICT), et ce, plus rapidement que ce qui était prévu dans les plans d'investissements. En 2016, le Comité a toutefois constaté que le système de gestion des données du SGRS n'était toujours pas au point. Il a de nouveau recommandé que le service s'y attelle d'urgence.

85. La protection des données à caractère personnel en dehors des sites protégés
Le SGRS n'a pas ménagé ses efforts pour protéger les données classifiées qui sortent des sites protégés. Le Comité permanent R recommande toutefois que ces mêmes efforts soient axés sur la protection des données à caractère personnel qui ne sont pas nécessairement classifiées. En effet, il est stipulé à l'article 16 § 4 de la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel que la personne responsable du traitement prenne les mesures techniques et organisationnelles adéquates pour protéger les données à caractère personnel, entre autres contre une perte accidentelle. À titre complémentaire, le Comité permanent R a recommandé l'élaboration de règles entourant l'éventuelle communication d'un incident de sécurité aux personnes dont les données ont été perdues. Bien entendu, il convient d'évaluer les risques pour le service et les intérêts de la personne concernée.

86. Une représentation garantie au sein de la Canpan
Le Comité a souligné l'importance de la présence d'un membre du SGRS aux réunions de la Canpan. Or, il s'est avéré que ce n'était pas toujours le cas. La contribution du service de renseignement militaire à cet organe consultatif doit être garantie. Cette absence est bien évidemment une des conséquences d'un problème plus structurel : le SGRS déploie une capacité d'analyse trop faible en matière de suivi de la prolifération.

87. Recommandations dans le cadre des missions du SGRS à l'étranger
Le Comité permanent R recommandait que le SGRS définisse les liens devant être établis entre les renseignements opérationnels, tactiques et stratégiques et les missions légales

décrites dans la L.R&S. Il conseillait au SGRS de rassembler les textes qui sont d'application lors d'un déploiement du SGRS, en y incluant les règles internationales et nationales. À ce propos, une meilleure intégration et une plus grande cohérence du contenu s'imposaient. Le Comité estimait nécessaire de renforcer la formation du personnel avant un départ en mission et exhortait le SGRS à poursuivre les améliorations déjà entreprises. Il jugeait également nécessaire que le SGRS applique la méthode C*omprehensive Preparation of the Operational Environnement* (ou toute autre méthodologie qui vise le même objectif) et prenne surtout en considération les besoins exprimés par les partenaires militaires dans le cadre de la préparation des missions. Il recommandait que le SGRS adopte une attitude proactive à l'égard de ses clients pour pouvoir déterminer plus précisément leurs attentes, mais aussi pour leur donner une idée précise de ce que le SGRS peut leur fournir. Il invitait le SGRS à réaliser une estimation générale des risques encourus par le personnel civil et militaire déployé dans la zone de conflit et à formuler des propositions pour les gérer. Il exhortait le SGRS à définir de manière plus détaillée le rôle des analystes déployés dans un environnement de collecte de renseignements, en particulier pour garantir l'objectivité de la fonction d'analyse. Il conseillait au SGRS de développer une approche plus systématique lors du déploiement du personnel dans la zone de conflit. Une telle approche, qui prend pour point de départ les menaces que le SGRS doit suivre dans le cadre de la L.R&S, est essentielle pour déterminer les moyens humains et matériels à déployer. Enfin, le Comité estimait que le personnel du SGRS qui est déployé dans la zone de conflit devait disposer du matériel adéquat, en particulier des moyens de communication et des véhicules mis à la disposition du *Belgian National Intelligence Cell*.

88. Établir des rapports sur les sweepings
Le Comité a recommandé que le SGRS rédige des rapports concernant les *sweepings* qu'il effectue à la demande de diverses instances (les instances européennes établies à Bruxelles), d'autant plus que ceux-ci sont généralement effectués en dehors de tout protocole.

89. Audit – Recommandations relatives aux conditions organisationnelles requises pour une affectation adéquate des moyens
La fonction Personnel et Organisation (fonction P&O) du SGRS devait être renforcée d'urgence. Ce renforcement était une recommandation de changement et donc une condition *sine qua non* pour que la mise en œuvre d'autres recommandations ait une chance de succès. Le Comité recommandait qu'un processus récurrent soit lancé pour définir des objectifs clairs formulés conformément aux critères SMART, en termes de produits à fournir et de *service level agreements* (SLA). Il convenait de déterminer quelle était la collaboration opportune et requise entre et au sein des divisions pour réaliser ces objectifs. En outre, les utilisateurs et les 'clients' externes et internes devaient pouvoir évaluer les produits proposés et les SLA. La définition des produits et des SLA devait également passer par une estimation de l'investissement humain requis en temps et compétences. Une approche plus professionnelle s'imposait dans la gestion des compétences au sein du SGRS et dans l'harmonisation des tâches, fonctions et compétences. Le Comité permanent R estimait que la créativité était un atout précieux pour un service de renseignement et devait être stimulée. Pour chaque objectif, il fallait établir un planning,

une méthode de suivi et désigner les acteurs concernés. Il s'agissait d'une recommandation de changement. Tous les plans de collecte devaient mentionner quelles étaient les informations requises en vue d'élaborer les produits et qui pouvait fournir ces informations. Dans cette optique, il convenait de désigner un gestionnaire des informations et de faciliter la recherche automatisée dans les fichiers. Chaque division devait informer son propre personnel *et* le personnel d'autres divisions de 'qui' dispose de 'quelles' informations et de 'ce qui' peut être mis à disposition. Il convenait d'intégrer un mécanisme de *feedback* pour tous les produits fournis. Les clients internes et externes devaient aussi être systématiquement sondés afin de se faire une idée plus précise de leurs besoins et de ce qu'ils pouvaient attendre du SGRS. En fonction des budgets disponibles, le SGRS et la Direction générale *Material Resources* des Forces armées devaient toujours s'efforcer d'améliorer les moyens de fonctionnement et les conditions de travail. Dans ce cadre, il convenait de mettre clairement l'accent sur les moyens ICT, sans pour autant négliger les aspects liés à la sécurité (sécurisation des documents, de l'infrastructure et des personnes).

90. Audit – Recommandations relatives à la gestion et à la direction du personnel du SGRS
Le Comité permanent R recommandait que les fonctions soient clairement décrites. Il convenait de revoir complètement la formation (continue), de dresser la liste des compétences actuelles et requises, d'établir un plan de formation et d'inventorier l'offre de formations interne et externe. Le Comité permanent R estimait que la création d'une branche 'renseignement' pourrait (partiellement) résoudre un certain nombre des problèmes constatés et engendrer un réel changement. Il fallait remédier aux nombreuses différences administratives et pécuniaires qui existaient entre les diverses catégories du personnel au sein du SGRS et entre celles du SGRS et d'autres services du secteur du renseignement (VSSE et OCAM). Ces différences nuisaient, en effet, à une bonne gestion du personnel. Il convenait de porter une attention particulière au coaching, à l'accompagnement et au soutien du personnel du SGRS, en tenant compte de leur situation spécifique. Dans le cadre de la fonction P&O (renforcée), le Comité permanent R recommandait la création d'une cellule à laquelle le personnel civil pouvait s'adresser pour régler les problèmes spécifiques liés à son statut et à sa situation. L'évaluation du personnel du SGRS s'appuyait sur un cadre réglementaire qui dépassait ce service. La fonction P&O devait veiller à ce que les évaluations soient correctement effectuées et encadrées. Il convenait également de décrire la manière dont se déroulerait l'évaluation, par objectif et par produit à fournir. Le Comité permanent R recommandait de traiter les inégalités de statut du personnel du SGRS. À cet égard, il est préférable de suivre une 'logique fonctionnelle' plutôt qu'une 'logique de groupe'. La fonction d'analyse requérait ici une attention prioritaire, puisque les différences étaient les plus nombreuses et que les risques de discontinuité étaient les plus importants. Le Comité recommandait la création, au sein du SGRS, d'une fonction ayant pour mission principale 'la gestion de la communication interne'.

91. Audit – Recommandations relatives aux flux d'informations à l'ICT
Le Comité permanent R estimait que le nouveau système RFI *(Request for Information)* améliorerait (considérablement) le traitement et le suivi des demandes d'informations. Le Comité recommandait au SGRS d'examiner, seulement après une période-test, si une réorganisation complémentaire était toujours nécessaire. Dans l'intervalle, le SGRS pouvait se concentrer sur l'aspect technique du système de gestion RFI, sans être

d'emblée confronté à des questions organisationnelles. Le Comité recommandait de poursuivre et d'accélérer autant que possible l'intégration de la collecte de données et des banques de données. Le SGRS devait prendre diverses initiatives pour pouvoir gérer le grand volume de données et de documentation. Il fallait tout d'abord déterminer quelles étaient les informations nécessaires à la réalisation des objectifs et des produits à fournir. Il fallait aussi veiller à une bonne collaboration entre les services de collecte et les bureaux d'analyse. Enfin, il convenait d'investir dans les moyens humains et l'ICT qui sont absolument nécessaires. De manière générale, le Comité recommandait d'investir suffisamment de moyens dans les technologies de l'information et la communication (ICT), et ce, plus rapidement que ce qui est prévu dans les plans d'investissements.

92. Audit – Recommandations relatives à la gestion des risques
Le Comité recommandait de prendre des mesures pour limiter les risques en termes de discontinuité de l'exercice de fonctions et de perte de connaissances. Plus particulièrement, il convenait de mener une gestion prévisionnelle du personnel, d'envisager la création d'une branche 'renseignement' (où la perte de connaissances est moins importante et où les personnes peuvent être remplacées plus rapidement), et d'investir davantage (et de nouveau) dans l'ICT. Il était indiqué que le SGRS s'intéresse de près à la gestion des connaissances. Des instructions claires devaient être élaborées de manière à identifier les connaissances existantes, évaluer leur pertinence et prendre des mesures pour les stocker, les conserver et les diffuser. Le Comité recommandait également la désignation, au sein de chaque division, d'un gestionnaire des connaissances en appui au management des connaissances. Le Comité permanent R estimait que le risque résultant d'une 'définition pragmatique de priorités' était limité, mais que la vigilance devait être de mise. Un recrutement adéquat et un système élaboré de descriptions de fonctions pouvaient mieux circonscrire ce risque. Le Comité permanent R recommandait que le SGRS se penche sur le développement de la gestion des risques.

III.6 OCAM

93. Optimaliser le statut du personnel
Les Comités permanents R et P recommandent que l'OCAM ne procède plus au détachement d'agents non statutaires des services d'appui sans une éventuelle modification de la loi. Les Comités recommandent également de régulariser la situation administrative des personnes détachées, de constituer un dossier personnel pour chaque membre du personnel (qu'il ou elle soit statutaire, ou détaché(e), et même de la direction), de soumettre aux ministres compétents des propositions de modifications de l'Arrêté royal réglant le statut du personnel statutaire et détaché, et enfin de veiller à ce que toute décision de mettre fin à un détachement pour un motif disciplinaire *sensu lato* soit prise dans le respect du principe de bonne administration, en vertu duquel la personne concernée par la mesure doit être entendue.

94. L'utilisation des réseaux sociaux par les membres du personnel de l'OCAM
En ce qui concerne l'utilisation des réseaux sociaux par les membres du personnel de l'OCAM, les Comités R et P ont formulé les recommandations suivantes : les efforts que la direction de l'OCAM a déjà entrepris pour appréhender les risques de sécurité générés

par la présence de membres de son personnel sur les réseaux sociaux doivent être poursuivis (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. 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, des moyens de recherches ciblés doivent être mis en place pour vérifier la bonne application de ces règles, toujours susceptibles d'être adaptées à l'évolution des moyens de communication. Cela doit se faire aussi bien de manière préventive, par des contrôles aléatoires, que de manière 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 de l'ICT et le comportement des agents sur les réseaux sociaux 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, 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 pourront être prises : le retrait de l'habilitation de sécurité, l'engagement de poursuites disciplinaires conformément au régime disciplinaire des analystes de l'OCAM, 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'évaluer 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.

95. Contacts transparents et traçables de l'OCAM avec des services étrangers homologues
En leur qualité d'organes de contrôle, les Comités permanents R et P ont insisté pour pouvoir retracer, en toute transparence, les contacts établis par l'OCAM avec des services étrangers homologues (ou non). De plus, les deux Comités recommandent que certains éléments relatifs à ces contacts soient repris dans les rapports d'activités que l'OCAM doit leur transmettre via le Conseil national de sécurité (art. 10, § 4, L.OCAM).

96. Désigner des points de contact centraux dans les services d'appui de l'OCAM
Il est recommandé de désigner clairement un point de contact au sein de chaque service d'appui. Le point de contact central doit avoir une vue complète sur les échanges d'informations.

97. Garantir la traçabilité des renseignements des services d'appui
La traçabilité des renseignements doit être garantie au sein de chaque service d'appui.

98. Clarifier les procédures d'embargo
La confusion qui entoure les différentes procédures d'embargo doit être dissipée.

Il convient de préciser la portée de la procédure d'embargo pour le travail d'analyse de l'OCAM. Il faut prévoir une procédure en cas de différend entre l'utilisation et la diffusion d'informations fournies sous embargo. Et il faut pouvoir contrôler l'application de la procédure d'embargo.

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

ACTIVITEITENVERSLAG 2017
RAPPORT D'ACTIVITÉS 2017

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.
15) Vast Comité I, Activiteitenverslag 2016, 2017, 230 p.
16) Vast Comité I, Activiteitenverslag 2017, 2018, 152 p.

ACTIVITEITENVERSLAG 2017

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de inlichtingen-
en veiligheidsdiensten

intersentia
Antwerpen – Cambridge

Voorliggend *Activiteitenverslag 2017* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 5 september 2018.

(*getekend*)
Guy Rapaille, voorzitter
Pieter-Alexander De Brock, raadsheer
Laurent Van Doren, raadsheer
Wouter De Ridder, griffier

Activiteitenverslag 2017
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

ISBN 978-94-000-1003-1
D/2018/7849/116
NUR 823

INHOUD

LIJST MET AFKORTINGEN

ADIV	Algemene Dienst Inlichting en Veiligheid
ANG	Algemene Nationale Gegevensbank
BELPIU	*Belgian Passenger Information Unit*
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
CAC	*Conduct After Capture*
CAP	Centraal aanspreekpunt
CBPL	Commissie voor de bescherming van de persoonlijke levenssfeer
CFI	Cel voor Financiële Informatieverwerking
CHOD	*Chief of Defence*
CI	Counterintelligence
CNCIS	*Commission nationale de contrôle des interceptions de sécurité*
CNCTR	*Commission nationale de contrôle des techniques de renseignement*
COC	Controleorgaan voor politionele informatie
CRIV	Compte Rendu Intégral – Integraal Verslag
CTIVD	Commissie van Toezicht op de inlichtingen- en veiligheids-diensten
C-OPS	Operatie Center
DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
DG EPI	Directoraat-generaal Penitentiaire instellingen
DGSE	*Direction Générale de la Sécurité Extérieure*
DVZ	Dienst Vreemdelingenzaken
EVRM	Europees Verdrag voor de Rechten van de Mens
FOD	Federale overheidsdienst
FRA	*European Union Agency for Fundamental Rights*

FTF	*Foreign terrorist fighters*
GBA	Gegevensbeschermingsautoriteit
HTF	*Homegrown terrorist fighters*
Parl. St.	Parlementaire Stukken van Kamer en Senaat
Hand.	Handelingen
HUMINT	*Human intelligence*
ICCB	Islamitisch Cultureel Centrum van België
ICT	Informatie- en communicatietechnologie
IMINT	*Image intelligence*
IS	Islamitische Staat
ISTAR	*Intelligence, surveillance, target acquisition and reconnaissance*
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 FTF	Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de Wet op het politieambt
KB OCAD	Koninklijk besluit van 28 november 2006 tot uitvoering van de Wet van10 juli 2006 betreffende de analyse van de dreiging
LTF	*Local task force*
M.B.	Ministerieel besluit
MoU	*Memorandum of Understanding*
NAVO	Noord-Atlantische Verdragsorganisatie
NBB	Nationale Bank van België
NTF	Nationale Task Force
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open sources intelligence*
POC	*Point of contact*
POC	Parlementaire onderzoekscommissie
Privacycommissie	Commissie voor de bescherming van de persoonlijke levenssfeer
SIGINT	*Signals intelligence*
Sv.	Wetboek van Strafvordering

Sw.	Strafwetboek
TCCC	*Tactical Combat Casualty Fare*
TF	*Terrorist fighters*
Vast Comité I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten
VN	Verenigde Naties
Vr. en Antw.	Schriftelijke vragen en antwoorden (Kamer of Senaat)
VSSE	Veiligheid van de Staat
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.C&VM	Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
WEP	Wetenschappelijk en economisch potentieel
W.OCAD	Wet van 10 juli 2006 betreffende de analyse van de dreiging
WPA	Wet van 5 augustus 1992 op het politieambt
W.Toezicht	Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse

WOORD VOORAF

Het takenpakket van het Vast Comité I is de laatste jaren alsmaar meer uitgebreid. Bestaande opdrachten werden verruimd of kregen voor het eerst een invulling. Daarenboven kreeg het Comité er een aantal nieuwe, belangrijke taken bij. Dit alles vertaalde zich onvermijdelijk in een toegenomen werklast, zeker nu er niet werd voorzien in de noodzakelijke bijkomende middelen.

De 'verruiming van bestaande opdrachten' is het onrechtstreekse gevolg van de uitbreiding van de bevoegdheden en personele middelen van de te controleren diensten: de VSSE en de ADIV kregen meer armslag wat bijvoorbeeld betekent dat er meer en andere BIM-methoden moeten worden gecontroleerd. Hetzelfde fenomeen treedt op bij het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en –adviezen: meer sectoren worden aan een verplichte veiligheidsscreening onderworpen hetgeen resulteert in meer beroepen… Met de nieuwe Wet van 23 februari 2018 zal het aantal *screenings* en bijgevolg het aantal beroepen alleen nog maar toenemen.

Ook het feit dat de inlichtingendiensten nieuwe taken kregen toegewezen, heeft repercussies op het Vast Comité I: de ADIV bijvoorbeeld kreeg een centrale rol toebedeeld in het kader van de *cybersecurity*. Om een gedegen controle uit te oefenen op de wijze waarop deze inlichtingenactiviteit wordt uitgevoerd, moet het Comité kunnen investeren in personeel met specifieke expertises.

Daarnaast werd het Comité ook geconfronteerd met het feit dat bestaande opdrachten meer of zelfs voor het eerst dienden te worden opgenomen. Zo formuleerde het Comité de afgelopen drie jaren evenveel adviezen op verzoek van het Parlement of een minister als in de vijftien jaren voordien. Ook werd het Comité voor het eerst ingeschakeld door twee Parlementaire onderzoekscommissies. Het Comité verrichte daarin belangrijk werk, maar dit ging uiteraard ten koste van andere opdrachten.

Ten slotte zijn er de talrijke wettelijke bepalingen waarbij het Comité recent een nieuwe opdracht kreeg toebedeeld: de inspectie van de gemeenschappelijke databanken FTF (ondertussen *foreign fighters*) en 'haatpredikers' die worden beheerd door het OCAD, het toezicht op bepaalde opdrachten van het ISTAR-bataljon, de controle van de manier waarop de ADIV in het buitenland beeldopnames maakt en intrusies verricht in IT-systemen, een verscherpt toezicht op bepaalde gewone methoden, het toezicht van de wijze waarop de inlichtingendiensten functioneren binnen de Passagiersinformatie-eenheid (BELPIU) en de controle van de wijze waarop ze gebruik maken van bepaalde camerabeelden.

De impact van al deze recente opdrachten was nog niet goed in kaart gebracht, of midden 2018 werd duidelijk dat het Vast Comité I er nóg een opdracht bijkreeg:

het wordt de Gegevensbeschermingsautoriteit voor *quasi* alle persoonsgegevens die een band hebben met de 'nationale veiligheid'. Het Comité zal in dat kader niet alleen rekening moeten houden met individuele verzoeken, maar ook adviezen moeten opstellen en protocols moeten sluiten met andere gegevensbeschermingsautoriteiten.

De vele, nieuwe regelgevende initiatieven werken diep in op het precaire evenwicht tussen enerzijds de rechten en vrijheden van de burgers en anderzijds de beperking daarvan om redenen van veiligheid. Maar ook het Vast Comité I wordt met de zoektocht naar dit evenwicht geconfronteerd. Het Comité werd opgericht om onafhankelijk én onpartijdig zijn controleopdrachten te vervullen, onder meer om de burger te garanderen dat de hem bij (Grond)wet toegewezen rechten, gewaarborgd zijn en blijven. De kwaliteit van het werk dat het Vast Comité I kan afleveren, is niet alleen essentieel voor het waarborgen van de rechten van de burger, maar is tevens een noodzakelijke factor in het vertrouwen dat die burger moet kunnen stellen in de diverse staatsinstellingen.

Het Comité liet de afgelopen jaren geen kans onbenut om de bevoegde autoriteiten duidelijk te maken dat het niet volstond wettelijk te voorzien in een toezicht, zonder ook te investeren in de toezichthouder. Zo bijvoorbeeld bracht het Comité reeds in oktober 2016 zijn bekommernissen hieromtrent ter kennis van de Kamercommissie Justitie en dit naar aanleiding van de besprekingen van de wetswijziging van de Inlichtingenwet waarbij de inlichtingendiensten nieuwe bevoegdheden kregen die door het Comité moeten worden gecontroleerd. Er werd tevens een gezamenlijke brief opgesteld met alle dotatiegerechtigde instellingen die met hetzelfde probleem te kampen hebben en ook tijdens de audit die de Kamervoorzitter liet uitvoeren naar deze instellingen, kwam de problematiek van de tanende middelen uitvoerig aan bod. In die audit werden kritische kanttekeningen geplaatst bij het grote aantal ondersteunende personeelsleden. Het Vast Comité I deelt deze kritiek niet. Bepaalde opdrachten – zoals bijvoorbeeld de werking van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen waarvan het Comité de griffie verzorgt – vereisen een uitgebreide administratieve ondersteuning die volledig door het Comité gedragen wordt.

Als afscheidnemend voorzitter van het Vast Comité I kan ik alleen maar hopen dat die roep om bijkomende middelen wordt gehoord, zodat enerzijds de aangekondigde besparingen en anderzijds de toegenomen bevoegdheden en werklast geen negatief effect zullen hebben op de kwaliteit van de werking van een orgaan dat een fundamentele rol speelt in onze democratische rechtstaat.

Guy Rapaille,
Voorzitter van het Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

5 september 2018

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, het Coördinatieorgaan voor de dreigingsanalyse en – in beperkte mate – van zijn ondersteunende diensten. De aanbevelingen die het Comité in 2017 formuleerde, zijn opgenomen in het laatste hoofdstuk van dit activiteitenverslag.

In de voorbije jaren werden in het eerste hoofdstuk de belangrijkste initiatieven opgesomd die de diverse actoren in het afgelopen jaar namen in de lijn van voorgaande aanbevelingen en werd de aandacht gevestigd op aanbevelingen die het Comité essentieel achtte, maar die vooralsnog niet werden geïmplementeerd.

Eerder – in het *Activiteitenverslag 2006*[1] – werd een overzicht geboden van de belangrijkste aanbevelingen die het Vast Comité I en zijn Begeleidingscommissies gedurende de jaren 1994 tot 2005 hadden geformuleerd en welke gevolgen hieraan werden gegeven.

Het Vast Comité I nam zich voor eenzelfde oefening te maken voor de periode 2006-2016. Daarmee zou meteen ook uitvoering worden gegeven aan een vraag van de parlementaire Begeleidingscommissie. In het kader van de bespreking van het *Activiteitenverslag 2015* werd immers gesuggereerd dat het Comité *'een lijst van de nog niet uitgevoerde aanbevelingen zou opstellen en dat de commissie aan de aanbevelingen een vergadering zou wijden om te zien welke initiatieven zij kan nemen*'.[2]

Het Comité startte dit project in 2016 op. In de loop van 2017 werd de opdracht van de Begeleidingscommissie door het Vast Comité I hernomen en verfijnd: er werd bestudeerd welke aanbevelingen voor deze periode reeds werden gereali-

---

1 VAST COMITÉ I, *Activiteitenverslag 2006*, 1-21 ('Hoofdstuk I. De eerdere aanbevelingen van het Vast Comité I en de Begeleidingscommissies').

2 *Parl. St.* Kamer 2016-17, nr. 54K2185/001 (Activiteitenverslag 2015 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Verslag namens de Bijzondere commissie belat met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten), 7.

seerd en de nog niet-gerealiseerde aanbevelingen werden afgetoetst op hun actualiteitswaarde en, indien nuttig en noodzakelijk, geherformuleerd. Dit resulteerde in een omvangrijk document dat in december 2017 werd toegezonden aan de Begeleidingscommissie en in februari 2018 voorwerp van bespreking uitmaakte. Gezien de omvang van het document, werd geopteerd om het als 'Bijlage D' op te nemen in onderhavig activiteitenverslag.

HOOFDSTUK II
DE TOEZICHTONDERZOEKEN

In 2017 finaliseerde het Vast Comité I vijf toezichtonderzoeken, waarvan één samen met het Vast Comité P (II.1 tot II.5). Verder opende het Comité in dat jaar drie nieuwe onderzoeken, waarvan één gemeenschappelijk met het Vast Comité P. Twee onderzoeken werden ambtshalve opgestart, in één onderzoek werd het Vast Comité I gevat door de minister van Defensie (art. 32 W.Toezicht).[3] Een korte omschrijving van deze drie opgestarte onderzoeken, volgt in II.6.

In totaal ontving het Comité in 2017 35 klachten of aangiften. Sinds 2016 werd een aanvang genomen met een versoepeling, deformalisering en standaardisering van het werkproces 'klachten en aangiften'.[4] Na verificatie van een aantal objectieve gegevens wees het Comité 34 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 (bijv. het Vast Comité P, de Federale Politie, de procureur des Konings). Eén van de klachten uit 2017 gaf aanleiding tot het openen van een toezichtonderzoek.

Naast toezichtonderzoeken opent het Vast Comité I ook zogenaamde 'informatiedossiers' die moeten toelaten om een respons te bieden op vragen met betrekking tot de werking van de inlichtingendiensten en het OCAD.[5] Indien dergelijke dossiers aanwijzingen van disfuncties aan het licht brengen of van aspecten van de werking van inlichtingendiensten die nader onderzoek behoeven, kan het Comité overgaan tot het initiëren van een toezichtonderzoek. Indien echter duidelijk is dat een dergelijk onderzoek geen meerwaarde ressorteert vanuit de doelstellingen van het Vast Comité I, krijgt het informatiedossier geen ver-

---

3 Het feit dat het Comité gevat wordt door een lid van de uitvoerende macht, is eerder uitzonderlijk. Hierover: VAN LAETHEM, W. en VANDERBORGHT, J., 'Torture numbers, and they'll confess to anything. Een analyse van twintig jaar toezichtonderzoeken, studies en adviezen' in VAN LAETHEM, W. en VANDERBORGHT, J. (eds.), *Inzicht in toezicht*, Antwerpen, Intersentia, 2013, 266.

4 In eerste instantie wordt de ontvankelijkheid bestudeerd en vervolgens wordt de klacht door de Dienst Enquêtes I behandeld. Indien zich een generieke probleemstelling voordoet, kan door het Comité worden beslist tot het openen van een toezichtonderzoek, zoniet blijft het onderzoek beperkt tot de klacht *an sich* (een klachtonderzoek).

5 De aanleiding voor het opstarten van informatiedossiers is zeer divers: de directie van een inlichtingendienst maakt melding van een incident en het Comité wil nagaan hoe het werd afgehandeld; de media melden een voorval en het Comité wil weten of dit strookt met de realiteit en of er een meer algemene problematiek achter schuilgaat….

der gevolg. In 2017 werd onder meer een informatiedossier geopend over de ontplooiing van een inlichtingencapaciteit van ADIV in een conflictzone, wat leidde tot de opstart van een toezichtonderzoek in 2018.

Ten slotte worden ook zeer regelmatig briefings georganiseerd waarbij leden van de inlichtingendiensten het Comité voorlichten over actuele en belangrijke thema's binnen de *intelligence community* (bijv. over de werking van de Belgische Passagiersinformatie-eenheid BELPIU, over de implementatie van richtlijn inzake samenwerking met buitenlandse partnerdiensten, over de wijze waarop bepaalde landen hun invloed trachten te laten gelden op Belgische belangen, over de werking van de SIGINT-afdeling, over de technische nieuwigheden in het kader van bijzondere inlichtingenmethoden, over *risk-assessment* en terrorismebestrijding…). Deze briefings moeten een geïnformeerde discussie over de werking, de bevoegdheden en de controle op de inlichtingen- en veiligheidsdiensten en het OCAD alsook op het inlichtingenwerk bevorderen. Zij kunnen ook aanleiding geven tot het openen van een onderzoek.

II.1. EEN KLACHT OVER DRIE OPERATIES VAN DE ADIV

II.1.1. CONTEXT

In mei 2017 dient een officier van de ADIV een klacht in over operaties die door de Afdeling I/H[6] zouden zijn uitgevoerd, en waarbij naar zijn oordeel onregelmatigheden of zelfs onwettigheden plaatsvonden. Het Vast Comité I besliste hierop een toezichtonderzoek te openen.[7, 8] Dit onderzoek liep parallel met een gerechtelijk onderzoek; de betrokken officier had zich immers ook tot het parket gewend.[9]

De klacht was drieledig:

- de Afdeling I/H zou de intentie hebben gehad om op Belgisch grondgebied een 'actiecel' te creëren;
- een zending van leden van Afdeling I/H naar een conflictgebied was problematisch;
- de ADIV onderhield in België contacten met een persoon die banden heeft met een groepering die minstens nauw betrokken zou zijn bij een terreurorganisatie.

---

6 De Afdeling I/H vormt een onderdeel van de Divisie I van de ADIV en heeft als opdracht om netwerken van bronnen en informanten op te richten ten einde de ADIV toe te laten inlichtingen te verzamelen over buitenlandse fenomenen. De klager was een tweetal jaar werkzaam in deze afdeling.

7 De minister van Defensie en het Parlement werden op de hoogte gebracht van de opening op 10 mei 2017. Het onderzoek werd afgesloten op 14 juli 2017.

8 In 2018 werd beslist de Afdeling I/H aan een breder toezichtonderzoek te onderwerpen. Voorliggende enquête beperkte zich tot de klacht.

9 In het kader van dit strafonderzoek werd een beroep gedaan op enquêteurs van de Dienst Enquêtes I. Deze enquêteurs werden niet betrokken in het toezichtonderzoek.

II.1.2. EEN NIEUWE 'ACTIECEL' BINNEN DE MILITAIRE INLICHTINGENDIENST?

II.1.2.1. Elementen aangebracht door de klager

De klager stelde dat binnen de Afdeling I/H een embryonaal type van een 'actiedienst' bestond. Deze zou inlichtingen inwinnen, maar ook – naar het voorbeeld van actiecellen van het Franse DGSE – 'acties opzetten'. Terwijl een dergelijke actiedienst in principe slechts in het buitenland opereert, zou de idee gerezen zijn om tevens operaties in het binnenland te ondernemen.

De klager zag de voorbereidingen voor de oprichting gestaafd door diverse elementen: een medewerker van de Afdeling I/H zou een private schietstand hebben gehuurd om daar met oorlogswapens aan een persoon (een niet-militair) schietonderricht te geven; de klager maakte gewag van een uitwisseling van tekstberichten tussen de Commandant van de Afdeling I/H en zijn Divisieoverste waarin sprake zou zijn van het inzetten van een 'actiedienst' in het binnenland; er zou voor externen een *survival training* in het buitenland worden georganiseerd en de leden van de afdeling volgden een *Conduct After Capture*-opleiding (CAC).[10]

II.1.2.2. Vaststellingen door het Vast Comité I

De Afdeling I/H huurde effectief op drie verschillende tijdstippen een private, doch officieel vergunde schietstand. Dit gebeurde met de formele goedkeuring van de hiërarchie van de Divisie I. Het afhuren van een private schietstand is reeds langer een bestaand gebruik (ook voor de leden van de Afdeling I/Ops en de Divisie CI). Het gebruik van een militaire schietstand blijkt immers aan allerlei beperkingen onderhevig.[11] De persoon die een initiatie kreeg, was een bron die in het verleden in een zeer gevaarlijke situatie in het buitenland verkeerde en waarvan de Afdeling I/H het opportuun achtte om eenmalig de basishandelingen i.v.m. het omgaan met een vuurwapen toe te lichten. Blijkbaar was de vormingscel binnen Afdeling I/H niet op de hoogte gesteld van de huur van de schietstand. Maar aangezien het om een technische vorming ging, verklaarde de vormingsofficier dat diens tussenkomst niet vereist was.

Daarnaast kon het Comité vaststellen dat in een sms-uitwisseling tussen enerzijds de Commandant van de Afdeling I/H en anderzijds het Hoofd van de Divisie

---

10 Het gaat om een opleiding die in eerste instantie voor piloten van de Belgische luchtmacht wordt georganiseerd om hen voor te bereiden indien zij achter vijandelijke linies zouden worden neergehaald.

11 Er moet lange tijd vooraf een strikt tijdschema worden opgegeven, wat niet steeds mogelijk is wanneer medewerkers naar het buitenland moeten vertrekken. Bovendien kon de eigenaar van de schietstand ook andere dan de standaard-wapens van het Belgische leger ter beschikking stellen waarmee de leden van Afdeling I/H tijdens buitenlandse missies zouden kunnen worden geconfronteerd.

I, de inzet van de Afdeling I/H in het binnenland ter sprake kwam en dat er een verwijzing was naar een 'actiedienst'. Deze verwijzing moet volgens het Comité echter in zijn tijdcontext worden gezien. Ze deed zich voor daags na de terreuraanslagen in Parijs, toen in België het dreigingsniveau 4 werd afgekondigd. Het lag daarbij niet in de bedoeling om binnen België een 'actiedienst' te ontplooien, maar wel bood de Commandant van Afdeling I/H aan dat zijn medewerkers zo nodig de Divisie CI in België zouden bijstaan indien daar nood toe was, maar louter om inlichtingen te vergaren. In de praktijk echter werd er geen beroep gedaan op de leden van Afdeling I/H om in België op te treden.

Begin januari 2015 stuurde de Afdeling I/H een persoon van Belgische nationaliteit maar die niet tot de ADIV behoort, naar een meerdaagse *survival-training* in het buitenland. Het Comité kon vaststellen dat het ging om een nieuwe bron van de Afdeling I/H, die voor zijn eigen veiligheid tijdens opdrachten nood had aan zelfvertrouwen en weerstand. De training kwam tot stand in samenwerking met de interne vormingsdienst van de Afdeling I/H, die na een psychologische profielschets van betrokkene tot het besluit kwam dat deze opleiding inderdaad geschikt was om hem bijkomende vaardigheden bij te brengen.

Wat betreft de CAC-opleiding waaraan leden van de Afdeling I/H zouden hebben deelgenomen, kon het Comité het volgende vaststellen: twee leden – waaronder de verantwoordelijke van de vormingscel – van de Afdeling I/H volgden een '*light* versie' van de opleiding. Doel was te evalueren of deze vorming interessant kon zijn voor de leden van de afdeling. De conclusie viel negatief uit.

Het Vast Comité I besloot dan ook dat er geen redenen waren om aan te nemen dat er plannen waren om de Afdeling I/H tot 'actiedienst' uit te bouwen of in het binnenland actief te maken. Daarenboven verliepen alle vormingen volgens de binnen Defensie geldende regels.

II.1.3. DE MISSIE NAAR EEN CONFLICTGEBIED EN DE STEUN AAN EEN ORGANISATIE TER PLAATSE

II.1.3.1. Elementen aangebracht door de klager

De kwestie betrof een missie naar een conflictgebied in juli 2015, uitgevoerd door enkele leden van de Divisie I. Tijdens de missie werd contact genomen met een inlichtingendienst van een organisatie ter plaatse, maar werd ook medisch materiaal geleverd en, naar luid van de klager, ook schietinstructies gegeven aan lokale troepen.

II.1.3.2. De vaststellingen door het Vast Comité I

In februari 2015 begaven militairen van de Divisie I zich naar een conflictgebied. Het doel van de operatie bestond er in om contacten uit te bouwen met (militaire) actoren en om ter plaatse een beveiligde informaticaverbinding te installeren

waarlangs inlichtingen naar België konden worden doorgeseind. In het gebied konden zich Belgische *foreign terrorist fighters* (FTF) bevinden die zich bij IS hadden aangesloten of die op doortocht waren. Er werd getracht om via deze lokale actoren inlichtingen te kunnen bekomen over de FTF. Bijkomend was er de idee om vriendschappelijke contacten uit te bouwen met de daar aanwezige milities in geval een Belgische F-16 in die regio zou worden neergehaald en de piloot naderhand zou moeten worden geëxfiltreerd.[12]

De operatie werd geïnitieerd op vraag van de toenmalige Chef van de ADIV. De normale commandoketen werd gevolgd[13] en er werd regelmatig overleg gepleegd over de te nemen stappen en de uit te voeren missies. Bij de terugkeer stelden de betrokken leden van de Afdeling I/H steeds omstandige verslagen op.

De missie van februari 2015 was reeds in september 2014 gestart via een contact met de betrokken ambassade in België. In oktober en december 2014 vonden de eerste contacten in het buitenland plaats. In juli 2015 vertrok een volgende missie; de Belgische delegatie (leden van de Afdeling I/H) bezocht een trainingskamp van de lokale troepen en er werden – in ruil voor de inlichtingen die de ADIV van de lokale inlichtingendiensten kreeg – rugzakken met medisch materiaal geschonken, bedoeld om eerste hulp toe te dienen in gevechtsomstandigheden.[14] Een daartoe opgeleid lid van de ADIV demonstreerde het gebruik van de uitrusting ter plaatse.

II.1.3.3. Het algemeen kader voor de inzet van militairen in het buitenland

Naar luid van de CHOD bleek dat een dergelijke zending in een tweevoudig kader is in te passen. Enerzijds wordt de zending 'gedekt' door het algemeen Operatieplan van Defensie, opgemaakt op het niveau van de CHOD en goedgekeurd door de regering. Dit plan voorziet in de capaciteit om voor inlichtingenoperaties een aantal militairen voor buitenlandse opdrachten in te zetten, en dit zonder verdere specificatie. Anderzijds is er het door de minister van Defensie goedgekeurd Inlichtingenstuurplan. Hierin wordt het verzamelen van inlichtingen ten aanzien van de betrokken regio als een prioriteit naar voor geschoven (gelet op het feit dat het om een operatiegebied van de Belgische Defensie gaat).

---

12 In die zin was de inlichtingoperatie in lijn met de regeringsbeslissing van eind 2014, waarin beslist werd de Belgische F-16 in te zetten en aan het *Building Partner Capacity Program* deel te nemen.

13 Het bestaan van de operatie werd ook aan de toenmalige CHOD gemeld tijdens een briefing op 29 maart 2015.

14 Het gaat om de training *Tactical Combat Casualty Care* (TCCC). Daarbij wordt het gebruik van het materieel in 'realistische' omstandigheden gegeven, d.w.z. deels op een echt oefenterrein en met deelnemers in gevechtsuitrusting en soms zelfs terwijl er werkelijk wordt gevuurd. Dit kan verkeerdelijk als 'schietinstructie' worden beschouwd, maar maakt deel uit van de manier waarop gewonden onder vuur kunnen worden geëvacueerd. Dergelijke opdrachten maken normaliter deel uit van interventies of trainingsmissies door operationele eenheden van Defensie (Special Forces of OPS/Trn). De opdracht *in casu* was van inlichtingenaard. De korte initiatie bij het geleverde materiaal vormde enkel een praktische modaliteit.

Op het moment van het opstarten van de operatie bestonden er nog geen officiële (politieke) richtlijnen uitgaande van de Nationale Veiligheidsraad, waarbij criteria werden vooropgesteld om te bepalen met welke externe inlichtingendiensten samenwerking mogelijk is.[15]

II.1.3.4. De informatie naar militaire en politieke echelons

Binnen de Afdeling I/H en de ADIV werd de normale commandoketen gevolgd: I/H kreeg de formele goedkeuring om de missie uit te voeren en hield de hiërarchie op de hoogte van de operaties. De CHOD kreeg, weliswaar na de missie van februari 2015, een briefing en ook het Hoofd van de Luchtcomponent werd geïnformeerd (zonder operationele details).

Buiten de militaire keten werden ook het Vast Comité I en de VSSE – tevens zonder operationele details – gebriefd (april 2016).

In eerdere toezichtonderzoeken[16] stelde het Comité dat er bij het aangaan van engagementen in het kader van internationale samenwerkingsverbanden in bepaalde gevallen een politieke aftoetsing en dekking vereist is. Het Comité beval destijds aan dat de bevoegde ministers afdoende zouden worden geïnformeerd opdat zij in de mogelijkheid zouden zijn ten aanzien van het Parlement hun politieke verantwoordelijkheid op te nemen. *In casu* werd de minister van Defensie en zijn kabinet op de hoogte gebracht. Een aantal elementen hebben daartoe bijgedragen: het feit dat de operatie en de missie uitgevoerd werden door een bijzonder bureau van de Afdeling I/H; het feit dat het ging om een operatie in een conflictgebied en, meer nog, in een lucht-operatiegebied van de Belgische Defensie (en dat in het centrum van de Belgische militaire en politieke belangstelling staat, zodat operaties ter plaatse op politiek niveau gevolgen kunnen hebben); en dat er bijzondere operationele risico's zijn voor de betrokken leden van de ADIV. Deze elementen kunnen beschouwd worden als risico's die in acht moeten worden genomen wanneer er over een operatie wordt beslist: hoe hoger het risico, hoe sneller de minister moet worden ingelicht.

Gelet op de voorgaande elementen, was het Vast Comité I dan ook van mening dat een briefing van de minister van Defensie inderdaad voor de hand lag. Het komt aan het hoofd van de dienst toe om daartoe het juiste moment te kiezen. De ADIV handelde in deze correct.

Wel stelde het Vast Comité I vast dat er geen gestructureerd raamwerk is en dat de – zowel strategisch-beleidsmatige als de operationele – risicoanalyse niet werd geformaliseerd.[17] Toch waren verschillende evaluatiemomenten aanwezig.

---

15 Deze richtlijn zag pas later het licht (Richtlijn aangaande de relaties van de Belgische inlichtingendiensten met buitenlandse inlichtingendiensten dd. 26 september 2016).

16 Zie o.m. VAST COMITÉ I, *Activiteitenverslag 2014,* 31 en 113.

17 Voor de zendingen naar deze conflictgebieden in maart en april 2017 maakte de Afdeling I/H voor het eerst gebruik van een specifiek document voor het bepalen van de operationele risico's.

Daarnaast stelde het Comité vast dat het medisch materiaal waarvan sprake via een privé-verzendingsdienst ter plaatse werd gebracht. Dit vormde een bijzonder risico voor de betrokken persoon en werd klaarblijkelijk niet vooraf onderzocht.

II.1.4. DE CONTACTEN MET EEN GROEPERING DIE GELINKT ZOU ZIJN AAN EEN NIET-ISLAMISTISCHE TERREURORGANISATIE

II.1.4.1. Elementen aangebracht door de klager

Een derde door de klager aangebracht onderwerp betrof de contacten van de ADIV en van de Afdeling I/H met een persoon die zou behoren tot een groepering – actief in een conflictgebied – dewelke deel zou uitmaken of minstens nauwe banden hebben met een niet-islamistische terreurorganisatie. De ADIV zou echter niet enkel contacten hebben onderhouden met (de persoon uit) deze niet-gouvernementele groepering, maar ook een faciliterende rol hebben vervuld bij de contacten tussen de betrokken persoon en een Belgische firma. Via hun vertegenwoordiger poogde de groepering immers bepaalde materialen te bekomen, weliswaar van niet-lethale aard.

II.1.4.2. Vaststellingen door het Vast Comité I

Het Vast Comité I stelde vast dat de ADIV inderdaad contacten had met een groepering, actief in een conflictgebied, en dit zowel in België als in het conflictgebied zelf. Het doel van de operatie was om het inlichtingennetwerk van de ADIV te versterken. De groepering vormde immers een belangrijke actor in dit gebied en mogelijks een bron van inlichtingen over de Belgische *foreign terrorist fighters*. Via dat kanaal werden zelfs mogelijke toegangen tot bronnen in andere conflictgebieden in het vooruitzicht gesteld.

De vraag stelde zich naar de tegenprestatie (*do-ut-des*) die de ADIV aan deze groepering kon geven in ruil voor de inlichtingen. Tijdens een voorbereidende vergadering was daarbij het niet-lethale materiaal ter sprake gekomen.

Wat betreft de kwalificatie van de groepering als 'terroristisch' of 'gelinkt aan een terroristische organisatie' stelde het Comité vast dat de analysediensten van de Divisie I de betrokken groepering in 2015 omschreven als een 'franchise' van een niet-islamistische terreurorganisatie. Ook in een aantal verslagen van de Afdeling I/H werd melding gemaakt van deze niet-islamistische terreurorganisatie wanneer er gesproken werd over de vertegenwoordiger van de er aan gelinkte groepering in België. Ten slotte bestempelt een regionale grootmacht de groepering als de vleugel van een terreurorganisatie en dus – per definitie – zelf ook als een terroristische groepering.

Anderzijds staat de betrokken groepering niet op een internationale lijst van terroristische organisaties, ook al stelde de groepering in het oorlogsgebied bepaalde handelingen die kwestieus kunnen zijn. Ook was de ADIV niet de enige dienst die met deze groepering contacten onderhield; het leger van een bevriende mogendheid steunde de groepering reeds in september 2014 en leverde er sinds mei 2017 ook wapens aan.

Het Comité besloot dan ook dat de groepering formeel gezien tot nader order geen terroristische organisatie is, maar dat het duidelijk was dat het om contacten van 'gevoelige aard' ging.

Het Vast Comité I stelde vast dat het om een aan het Inlichtingstuurplan conforme inlichtingenoperatie ging, maar dat er bijzondere elementen aanwezig waren die tot voorzichtigheid aanmaanden.

II.1.4.3. De informatie naar de militaire en politieke echelons

De hiërarchie van de Afdeling I/H werd stelselmatig op de hoogte gehouden van de contacten, en dit zowel binnen de Divisie I als op het niveau van het Commando. Ook het Departement CI van de Divisie SI was op de hoogte.[18] Andere militaire autoriteiten werden niet geïnformeerd, ook niet de CHOD.[19] De CHOD werd pas eind april 2017 op de hoogte gebracht.

De Afdeling I/H had bij de aanvang van de operatie contact met de gerechtelijke autoriteiten (eerst met Federale Gerechtelijke Politie, naderhand met de Federaal magistraat) om hen/hem ervan op de hoogte te brengen dat de betrokken persoon in een inlichtingenoperatie figureerde. Ook een vertegenwoordiger van de VSSE was bij de vergadering aanwezig. Van zodra de operatie aan de gang was, bleven de verschillende diensten met elkaar in contact.

De minister van Defensie werd vooraf niet gebrieft over deze operatie; hij werd pas eind april 2017 op de hoogte gebracht. Toch waren dezelfde elementen aanwezig als bij de vorige operatie (*supra*): ze werd uitgevoerd door de Afdeling I/H en was daardoor per definitie zeer delicaat en het betrof een missie naar een conflictgebied met verhoogde operationele risico's in een invloedregio van een NAVO-partner van wie geweten was dat deze de betrokken groepering niet gunstig gezind was. Deze elementen moesten meegenomen worden in de afweging of en wanneer de bevoegde minister door de inlichtingendienst moest worden gebrieft. Daarenboven bestond een band tussen de betrokken organisatie en een terreurgroep (ook al stond de organisatie zelf niet op een internationale terrorismelijst), was er een verband met een lopend gerechtelijk onderzoek en was geweten dat de

---

18 De Afdeling I/H was bij de start van de operatie door CI op de hoogte gebracht dat de betrokken persoon genoemd was in een gerechtelijk onderzoek door het Federaal Parket, bevoegd voor terrorisme.

19 Het zou, aldus de CHOD, wel nuttig zijn om C-OPS van dergelijke operaties te informeren (misschien eerder nog dan aan de CHOD zelf), zodat C-OPS er zich van bewust zou zijn dat Belgische militairen covert in het gebied aanwezig zijn.

contacten een impact konden hebben op de relatie van de VSSE met een partnerdienst alsook de mogelijke compromittering van de operatie door deze partnerdienst. Rekening houdend met het belang van de operatie voor de ADIV en ook het gevoelige, zelfs risicovolle karakter ervan, ook voor de internationale relaties van België, had de Chef ADIV de Administrateur-generaal van de VSSE over de operatie moeten informeren, zodanig dat er op het hoogste niveau een gemeenschappelijk standpunt kon worden ingenomen.

Aangezien het om een *high-risk* operatie ging, was het Vast Comité I van oordeel dat een briefing van de minister van Defensie zich opdrong. Het Comité meende dat het aan het hoofd van de dienst toekwam om hiertoe het juiste moment te kiezen. Hierover ondervraagd, verklaarde deze dat hij meende dat de operatie zich nog in een 'embryonaal' stadium bevond en dat de minister van Defensie (en de CHOD) wel degelijk zouden worden ingelicht wanneer er meer concrete vooruitgang zou zijn geboekt. Het Vast Comité I meent dat dit laatste – het al dan niet tijdig informeren van de minister – een opportuniteitskeuze is die ultiem enkel door de minister zelf kan worden beoordeeld. Aangezien het kabinet van de minister van Defensie hierover verklaarde dat de minister – die weliswaar pas na het uitlekken van de operatie de feiten kende – dit volledig dekte, kan verondersteld worden dat de minister van mening was dat de ADIV juist handelde.

Ten slotte werden ook bij deze operatie weliswaar elementen van een risicoanalyse in diverse documenten aangebracht – zo bijvoorbeeld werd besloten om de groepering niet in België te ontmoeten gezien het gevaar voor compromittering door het partnerland – maar was er geen overkoepelende risicobeoordeling. Van specifiek belang bij de operatie was dat de ADIV een dergelijke beoordeling ook had kunnen opentrekken naar de VSSE toe. Het was immers aan de ADIV bekend dat de VSSE een relatie onderhield met een NAVO-partnerdienst én dat deze dienst de Belgische contacten met groepering niet welgevallig zou zijn.

II.2. HET MOGELIJK ONGEOORLOOFD OPVRAGEN VAN BANKVERRICHTINGEN EN HET BEROEPSGEHEIM

II.2.1. EEN TWEELEDIGE KLACHT

Bij monde van een advocaat ontving het Vast Comité I halfweg augustus 2017 een klacht van de gedelegeerd bestuurder van een accountancybedrijf. De klacht was gericht tegen een inspecteur van de VSSE en bevatte twee onderdelen: enerzijds werd aangehaald dat de inspecteur druk uitoefende op de gedelegeerd bestuurder in die zin dat deze verplicht werd om haar beroepsgeheim[20] te schenden; ander-

[20] Ex art. 58 lid 4 van de Wet van 22 april 1999 betreffende de boekhoudkundige en fiscale beroepen en art. 458 Sw.

zijds werd gesteld dat de opgevraagde informatie het voorwerp had moeten uitmaken van een bijzondere inlichtingenmethode (art. 18/15 W.I&V).

II.2.2. RECONSTRUCTIE VAN DE FEITEN

De inspecteur van de VSSE nam halfweg juli 2017 telefonisch contact op met de accountancyfirma. De gedelegeerd bestuurder bleek afwezig, waarop de inspecteur zijn contactgegevens opgaf. Hij verklaarde zich te hebben aangemeld als een personeelslid van de FOD Justitie die inlichtingen wou verkrijgen in het kader van een witwasonderzoek.

De bestuurder nam bij haar terugkeer telefonisch contact op en ging vervolgens akkoord met een ontmoeting begin augustus 2017. Daar identificeerde hij zich onmiddellijk als lid van de Veiligheid van de Staat, toonde zijn officieel identificatiebewijs (dienstkaart) en lichtte de ware toedracht van zijn bezoek toe (een onderzoek naar mogelijke spionageactiviteiten). De VSSE toonde belangstelling voor een klant van de accountancyfirma. Er werd informatie gevraagd over de totstandkoming van de contacten, inzage gevraagd van de aan- en verkoopboeken, afschriften van e-mailberichten opgevraagd… Ook werd een kopie van de jaarrekening van de target overhandigd.

De verklaringen liepen uiteen waar het ging over de 'verplichting' om mee te werken: de gedelegeerd bestuurder stelde dat de inspecteur verklaarde dat zij 'verplicht' was om mee te werken. De inspecteur daarentegen verklaarde dat hij niet expliciet over een 'verplichting' sprak, maar wel verwees naar de Inlichtingenwet.

Er was geen verder contact tussen de VSSE en het accountancybedrijf.

II.2.3. BEOORDELING

Het optreden van de inspecteur van de VSSE kwam voor het Vast Comité I niet als ontoelaatbaar over. Hij nam telefonisch contact om een afspraak vast te leggen en identificeerde zich als een personeelslid van Justitie, hetgeen correct is. Hij had het wel over 'witwaspraktijken' (wat niet met de realiteit strookte), maar telefonisch kon geen geclassificeerde informatie worden gegeven. Het gebruik van een *coverstory* bij een eerste contact, zeker telefonisch, is aanvaardbaar maar daarbij mag niet de indruk gewekt worden dat men over specifieke bevoegdheden beschikt.

Het onderzoek kon niet uitmaken of de betrokkene werkelijk over een 'verplichting' sprak, en zo ja, wat hij daarmee dan zou bedoeld hebben.[21] Het Vast Comité I was niet bij machte om de exacte bewoordingen van het gesprek te

[21] 'Morele' verplichting, wettelijke verplichting die gesanctioneerd kan worden, 'plicht' als een goed burger….

reconstrueren, maar kon niet vaststellen dat de inspecteur zich onheus, intimiderend of onbeleefd zou gedragen hebben.

Daarnaast stelde de gedelegeerd bestuurder dat zij gehouden was tot een specifiek beroepsgeheim, en dat dit ook ten aanzien van de VSSE geldt. Zij zou er ten onrechte toe gebracht zijn dit te schenden. Artikel 16 W.I&V zoals gewijzigd bij Wet van 30 maart 2017 (en dus van toepassing in augustus 2017 toen het onderhoud tussen de VSSE en de gedelegeerd bestuurder plaatsvond), bepaalt dat private personen en organisaties informatie en persoonsgegevens aan de inlichtingendiensten mogen mededelen indien deze nuttig zijn voor de opdrachten van deze diensten en, omgekeerd, dat de inlichtingendiensten dergelijke gegevens mogen vragen. Deze bepaling legt geen beperkingen op die te maken hebben met het beroepsgeheim van de privépersonen of instellingen, tenzij voor wat betreft het beroepsgeheim van advocaten en geneesheren en het bronnengeheim van journalisten. *A contrario* kan dus geconcludeerd worden dat andere vormen van beroepsgeheim niet gelden in relatie tot de VSSE. Wel was het Comité van oordeel dat het aangewezen zou zijn dat de wetgever op meer expliciete wijze zou bepalen of en in welke gevallen andere vormen van beroepsgeheim ter zijde kunnen worden geschoven, mede gelet op het feit dat dergelijke handelingen rechtstreeks kunnen ingrijpen op de privacy van personen zoals vervat in artikel 8 EVRM.

Bleef de vraag of er een BIM-methode had moeten worden toegepast? Artikel 18/15 W.I&V bepaalt dat de inlichtingendiensten de lijsten van bankrekeningen, bankkluizen of financiële instrumenten, de bankverrichtingen in een bepaald tijdvak of de gegevens met betrekking tot de titularissen van bankkluizen of gevolmachtigden, kunnen opvragen bij een bank of financiële instelling. Het was weliswaar zo dat de afgevaardigd bestuurder de aan- en verkoopdagboeken van het bedrijf overhandigde en dat daarin ook financiële gegevens voorkomen en dus ook bankverrichtingen en bankrekeningen. Niettemin is dit niet wat bedoeld wordt in artikel 18/15 W.I&V. Het feit dat er in de door de accountancyfirma medegedeelde gegevens ook bankgegevens voorkwamen, betekende dus niet dat de VSSE daarvoor een BIM-methode had moeten toepassen. De bankgegevens kwamen slechts 'incidenteel' in de opgevraagde gegevens voor en de VSSE vroeg in elk geval geen 'lijst van bankrekeningen of bankverrichtingen' op, hetgeen de firma trouwens ook niet had kunnen leveren.[22]

---

22 In de marge van deze casus is er de vraag of de 'aard' van de instantie waaraan de VSSE een lijst van bankgegevens vraagt, determinerend is om te bepalen of art. 18/15 W.I&V al dan niet van toepassing is. De wet spreekt immers over 'banken of financiële instellingen'. Het Vast Comité I besliste in een vorige *casus* dat er sprake was van een methode zoals bedoeld in art. 18/15 W.I&V wanneer het ging om het opvragen van gegevens bij het Centraal Aanspreekpunt (CAP) van de Nationale Bank van België. Het Comité onderzocht 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. 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

II.3. MISBRUIK VAN DE DIENSTKAART DOOR EEN LID VAN DE VSSE

In mei 2017 richtte een lid van de Veiligheid van de Staat zich tot het Vast Comité I met een klacht over een collega. Deze laatste zou misbruik gemaakt hebben van zijn hoedanigheid als lid van de inlichtingendienst, en zich met voorlegging van zijn dienstkaart bij een logiesverstrekker aangemeld hebben om informatie te krijgen over de klager. Tussen beiden personen bestond reeds enige tijd een persoonlijk conflict.

De klager had vooraf contact opgenomen met de hiërarchie bij de VSSE, die daarop een intern onderzoek had gestart en die had aangeraden om strafklacht neer te leggen. De klager had dit echter niet gedaan.

Het Vast Comité I stelde vast dat de persoon tegen wie de klacht gericht was, de feiten zelf had erkend in een document dat deel uitmaakte van een burgerlijke procedure tussen beide betrokken personen. De enquêtedienst was van mening dat de klacht dus inderdaad best door de gerechtelijke overheid zou worden behandeld gelet op het mogelijk strafbaar karakter van de feiten (misbruik van de officiele hoedanigheid van een ambtenaar/dienstkaart voor persoonlijke doel-einden).

Het Vast Comité I nam twee initiatieven. Enerzijds bracht het de VSSE op de hoogte van het indienen van de klacht, waarbij ook werd aangeduid dat er klaarblijkelijk bedreigingen waren geuit door de persoon die het voorwerp uitmaakte van de klacht en die nog over zijn dienstwapen beschikte. Het Comité vernam nadien dat de VSSE het dienstwapen aan betrokkene had onttrokken en dat het een tuchtonderzoek had opgestart. Anderzijds deed het Comité bij toepassing van artikel 29 Sv. aangifte bij de Procureur des Konings. Deze laatste vorderde de Dienst Enquêtes I om een aantal onderzoekdaden uit te voeren (art. 40 W.Toezicht).

Het dossier werd door het Parket zonder gevolg geklasseerd.

---

methode vormde (met name deze voorzien in art. 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 art. 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 art. 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.

II.4. KLACHT NAAR AANLEIDING VAN EEN NEGATIEVE BESLISSING IN HET KADER VAN EEN VEILIGHEIDSMACHTIGING

II.4.1. VOORWERP VAN DE KLACHT

In februari 2017 werd mondeling klacht ingediend tegen de ADIV.[23] De klacht had betrekking op de wijze waarop de militaire inlichtingendienst een veiligheidsonderzoek had gevoerd dat tot doel had een veiligheidsmachtiging van het niveau 'Geheim' toe te kennen, noodzakelijk voor zijn functies bij Defensie en de Federale Politie.[24] De grieven van de klager luidden als volgt:

- het gebrek aan transparantie van de procedure voor toekenning van de veiligheidsmachtiging;
- het gebrek aan professionalisme vanwege de agenten die belast waren met het dossier;
- een discriminerende behandeling ten aanzien van de klager en zijn vriendin;
- de vernederende en tergende houding vanwege de agenten die hem hebben ondervraagd.

II.4.2. VASTSTELLINGEN

II.4.2.1. Gebrek aan transparantie van de procedure voor toekenning van de veiligheidsmachtiging

De wijze waarop een veiligheidsonderzoek wordt gevoerd, wordt bepaald door de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, -attesten en -adviezen (W.C&VM), meer bepaald door de artikelen 16 tot 22.

De persoon die een veiligheidsmachtiging moet krijgen, wordt op de hoogte gebracht van het niveau en het doel van de machtiging, alsmede van de types van gegevens die gedurende het veiligheidsonderzoek kunnen worden onderzocht of geverifieerd, van de wijze waarop het onderzoek verloopt en van de geldigheidsduur van de veiligheidsmachtiging (art. 16 W.C&VM). Het akkoord van de betrokkene is vereist om het veiligheidsonderzoek te kunnen uitvoeren. Deze informatie is opgenomen in het formulier dat toegevoegd wordt in het koninklijk besluit van 24 maart 2000. Het gaat om het document dat de aanvra-

[23] De Begeleidingscommissie werd op 14 december 2017 op de hoogte gebracht van de resultaten van voorliggend klachtonderzoek.

[24] Voor een veiligheidsmachtiging binnen de Federale Politie is de Nationale Veiligheidsoverheid (NVO) de veiligheidsoverheid, terwijl dit voor een veiligheidsmachtiging binnen Defensie, de Chef ADIV is.

ger van de veiligheidsmachtiging moet ondertekenen en waaruit zijn akkoord blijkt.[25, 26]

Voor het overige voorziet de wet niet in de toepassing van eender welk door de klager ingeroepen transparantiebeginsel gedurende de veiligheidsonderzoeken en evenmin in de noodzaak van een tegensprekelijk debat met de aanvrager van de machtiging voorafgaand aan de beslissing van de veiligheidsoverheid.[27]

Aangezien de klager de wettelijke waarschuwing heeft gekregen en ingestemd heeft met de uitvoering van het veiligheidsonderzoek, vond het veiligheidsonderzoek wat dit aspect betreft plaats conform de voorschriften van de W.C&VM. De eerste grief betreffende het gebrek aan transparantie van de procedure bleek dan ook ongegrond.

II.4.2.2. Het gebrek aan professionalisme vanwege de agenten die belast waren met het dossier

Uit het onderzoek bleek dat de termijnen zoals bepaald door artikel 25 van het koninklijk besluit van 24 maart 2000 tot uitvoering van de W.C&VM, niet in acht waren genomen. Er verliep abnormaal veel tijd tussen de eerste aanvraag tot veiligheidsmachtiging (november 2012) en de eerste beslissing van de ADIV met de weigering om aan de klager een veiligheidsmachtiging toe te kennen (mei 2016).

Er waren meerdere oorzaken voor die aanzienlijke vertraging. Het Vast Comité I stelde vast dat het eerste beroep van de klager bij het Beroepsorgaan wegens het uitblijven van een beslissing met betrekking tot zijn aanvraag tot veiligheidsmachtiging dateert van april 2016, terwijl hij zijn eerste aanvraag al in november 2012 had ingediend. Voorts bleek dat er effectief sprake was van vertragingen en tekortkomingen op het vlak van zowel de interne informatieverstrekking bij de ADIV als de informatie-uitwisseling tussen die dienst en andere diensten. De tweede grief was bijgevolg gedeeltelijk gegrond.

II.4.2.3. De discriminerende behandeling ten aanzien van de klager en zijn vriendin

De klager vond het 'discriminerend' dat zijn vriendin, met wie hij niet samenwoonde, een veiligheidsonderzoek moest ondergaan alsook dat hijzelf meerdere gesprekken moest voeren.

---

25 De klager heeft een eerste formulier ondertekend op 13 december 2012 en een tweede op 27 oktober 2015.

26 De Nationale Veiligheidsraad stelt de omvang van het veiligheidsonderzoek vast voor elk machtigingsniveau. Alleen de agenten van de inlichtingendiensten, de Nationale Veiligheidsoverheid en het Vast Comité I krijgen kennis van de beslissing die de Nationale Veiligheidsraad neemt met betrekking tot de omvang van de onderzoeken (art. 18 W.C&VM).

27 In geval van beroep voor het Beroepsorgaan mogen de klager en zijn advocaat echter het onderzoeksdossier of het onderzoeksverslag raadplegen op de griffie van het Beroepsorgaan (onder voorbehoud van bepaalde informatie die geheim moet blijven bij toepassing van art. 5 § 3 van de Wet tot oprichting van een Beroepsorgaan); de klager heeft dat gedaan in oktober 2016 en januari 2017.

Het verhoor van een partner van een aanvrager van een veiligheidsmachtiging is niet verplicht gesteld in de W.C&VM wanneer die persoon niet onder hetzelfde dak woont. De wetgever verbiedt de diensten die belast zijn met een veiligheidsonderzoek echter niet om, wanneer ze dat nuttig achten, inlichtingen in te winnen over de personen met wie de aanvrager van een veiligheidsmachtiging omgaat.

Gelet op het veiligheidsdossier van de klager, meende het Comité dat de redenen voor het verzoek tot verhoor van zijn vriendin, gerechtvaardigd waren en zeker niet de uiting waren van een discriminerende intentie jegens hem en/of zijn vriendin. Bovendien meende het Comité dat dat verhoor het voor de klager wellicht mogelijk zou hebben gemaakt de toelichting te verschaffen die de dienst wenste te verkrijgen met betrekking tot bepaalde elementen van zijn privéleven. De weigering van de partner van de klager om te verschijnen op een verhoor kon op zich echter geen reden vormen voor de negatieve beslissing die ten aanzien van de klager is genomen.

De derde grief was bijgevolg niet gegrond.

II.4.2.4. Een vernederende en tergende houding vanwege de agenten

Uit het verslag van het gewraakte verhoor bleek duidelijk dat dit van start was gegaan in een gespannen sfeer; het verslag bevatte echter geen enkele vermelding of beoordeling die zou kunnen worden beschouwd als vernederend of tergend ten aanzien van wie dan ook.

Ook de interne verslagen van het veiligheidsonderzoek met betrekking tot de klager en zijn partner, bevatten niet de minste commentaar die erop zou kunnen wijzen dat zijn aanvraag tot veiligheidsmachtiging niet op neutrale wijze zou zijn behandeld. Integendeel, alle door de ADIV verzamelde inlichtingen leken naar oordeel van het Vast Comité I met veel omzichtigheid te zijn onderzocht en op onpartijdige wijze te zijn beoordeeld. Uiteindelijk bleek het ontbreken van inlichtingen over bepaalde aspecten van het privéleven van de klager de argwaan van de ADIV in stand te hebben gehouden en aanleiding gegeven tot de negatieve beslissing.

De vierde grief was niet gegrond.

II.4.3. DAN TOCH EEN TOEKENNING VAN EEN MACHTIGING

Na afloop van het veiligheidsonderzoek door de Afdeling Veiligheidsmachtigingen van de ADIV weigert de Chef ADIV in mei 2016 de veiligheidsmachtiging toe te kennen. Hierop tekent de klager beroep aan bij het Beroepsorgaan inzake veiligheidsmachtigingen, dat in januari 2017 beval dat een veiligheidsmachtiging van het niveau 'Geheim' aan de betrokkene moest worden toegekend.

II.5. DE INFORMATIEPOSITIE VAN HET OCAD VOORAFGAAND AAN DE AANSLAGEN IN PARIJS

Vrijwel onmiddellijk na de aanslagen in Parijs in november 2015 opende het Vast Comité I een toezichtonderzoek over de informatiepositie van de twee Belgische inlichtingendiensten.[28] Ook het Vast Comité P startte een toezichtonderzoek op naar de werking van de politiediensten. Op verzoek van de parlementaire Begeleidingscommissie en in toepassing van artikel 53, 6° W.Toezicht, werd door de Vaste Comités I en P eind januari 2016 beslist ook een gemeenschappelijk toezichtonderzoek op te starten over de '*informatiepositie van het OCAD, voorafgaand aan 13 november 2015 's avonds, over de individuen of groepen die de aanslagen te Parijs hebben uitgevoerd of hierbij betrokken waren*'. Het opzet bestond erin na te gaan over welke informatie het OCAD beschikte met betrekking tot personen die betrokken waren bij de terreuraanslagen en te bestuderen of het coördinatieorgaan voorafgaand aan de aanslagen informatie had opgevraagd en/of verkregen van de diverse steundiensten en buitenlandse partnerdiensten.

Omdat beide Comités midden 2016 andere – meer prioritaire – onderzoeksopdrachten dienden uit te voeren voor de parlementaire onderzoekscommissie 'terroristische aanslagen', werd het onderzoek opgeschort. Aangezien daarenboven de directeur van het OCAD nadien meerdere keren werd gehoord door de parlementaire onderzoekscommissie dat *de facto* de onderzoeksvragen overnam, achtte de Comités het hervatten van de onderzoekverrichtingen niet langer relevant. De twee Comités beslisten in hun gemeenschappelijke vergadering van 13 juni 2017 het toezichtonderzoek af te sluiten en geen eindverslag op te stellen. De voorzitter van de Begeleidingscommissie werd hiervan op 15 juni 2017 op de hoogte gebracht en maakte geen bezwaar.

II.6. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2017 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2017 WERDEN OPGESTART

II.6.1. INTERNATIONALE GEGEVENSUITWISSELING OVER *FOREIGN TERRORIST FIGHTERS*

Al in 2016 werd, tijdens een internationale vergadering met verschillende Europese toezichthouders[29], beslist een gelijkaardig toezichtonderzoek op te starten in

[28] Hierover: VAST COMITÉ I, *Activiteitenverslag 2016*, 18-36 ('II.3. De informatiepositie van de twee inlichtingendiensten voor de aanslagen in Parijs').

[29] Het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, de Nederlandse Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD), de Zwitserse

alle deelnemende landen over de internationale samenwerking tussen de diverse inlichtingendiensten met betrekking tot de strijd tegen de *foreign terrorist fighters* (FTF). Dit initiatief kreeg nadien de uitdrukkelijke steun van de voorzitter van de Begeleidingscommissie. Het ligt daarbij in de bedoeling dat elke toezichthouder, met zijn eigen perspectief en bevoegdheid maar vanuit eenzelfde filosofie en met een zekere gemeenschappelijke aanpak, dit thema bestudeert.

Het opzet van het Belgische luik van het onderzoek[30] bestaat erin om een zo duidelijk en volledig mogelijk beeld te krijgen op de formele (maar ook informele) bilaterale of internationale informatie-uitwisseling tussen de VSSE en de ADIV enerzijds en buitenlandse diensten, werkgroepen of samenwerkingsverbanden anderzijds en dit met betrekking tot de problematiek van de FTF.

De uiteindelijke finaliteit van het onderzoek is te komen tot een beoordeling over de informatie-uitwisseling en desgevallend tot aanbevelingen om deze te optimaliseren zodat de informatiepositie van de betrokken diensten kan worden verbeterd, zonder dat daarbij de fundamentele rechten van de burger worden uitgehold.

In 2017 werden op nationaal als op internationaal niveau diverse onderzoeksopdrachten uitgevoerd zowel bij de VSSE als de ADIV. De resultaten van het Belgisch toezichtonderzoek zullen – waar mogelijk gezien de restricties inzake classificatie – worden aangewend om het internationale onderzoek te stofferen. In dat kader vond in mei 2017 een expertenmeeting plaats in Oslo.

II.6.2. TOEZICHTONDERZOEK NAAR DE WERKING VAN DE DIRECTIE COUNTERINTELLIGENCE (CI) VAN DE ADIV

In uitvoering van artikel 32 W.Toezicht verzocht de minister van Defensie het Vast Comité I eind december 2016 een onderzoek te voeren naar de werking van de Directie Counterintelligence (CI) van de ADIV. Immers, *'een disfunctionele dienst roept vragen op die een onafhankelijk onderzoek noodzakelijk maakt',* aldus de minister. Rechtstreekse aanleiding tot die uitspraak vormde een schrijven van half december 2016 van een groot deel van het kaderpersoneel CI. Daarmee werd de minister op de hoogte gebracht van de bezorgdheid omtrent het functioneren van de dienst en de omstandigheden waarin ze hun wettelijke opdrachten dienen te vervullen.

Strategic Intelligence Service Supervision en delegaties vanuit Zweden (*Commission on Security and Integrity Protection*), Noorwegen (*Parliamentary Oversight Committee*) en Denemarken (*Intelligence Oversight Board*). Hierover VAST COMITÉ I, *Activiteitenverslag 2015*, 80-81.

30 Het onderzoek werd opgestart eind augustus 2016, nadat het initiatief eerder werd voorgelegd aan en goedgekeurd door de Begeleidingscommissie van de Kamer van Volksvertegenwoordigers.

Het Vast Comité I opende op 13 januari 2017 zijn toezichtonderzoek.[31]

Het onderzoek liep van januari 2017 tot april 2018. Een tussentijds rapport werd in juli 2017 gestuurd naar de Kamervoorzitter alsook naar de minister van Defensie. Daarin werd onder meer aandacht besteed aan de personeelssituatie van de dienst (inclusief de problematiek van het statuut), de gebrekkige infrastructuur, ICT en materiële omstandigheden en ten slotte de procedures en organisatie en het graduele verlies aan autonomie. Het eindverslag werd gefinaliseerd in mei 2018.

Het is duidelijk dat het Vast Comité I tijdens zijn toezichtonderzoek werd geconfronteerd met een organisatie in transitie: het Nationaal Strategisch Inlichtingenplan was in volle voorbereiding, de structuur werd (opnieuw) hertekend, bijkomend personeel werd aangetrokken en de aanbevelingen van de parlementaire onderzoekscommissie naar de terroristische aanslagen dienden te worden geïmplementeerd… Het Vast Comité I stelde voorop dat de nationale veiligheid een sterke en betrouwbare militaire inlichtingendienst vergt. Daarom ook is het Comité ervan overtuigd dat de Directie CI belang heeft bij een organisatie en sturing die beantwoordt aan de standaarden van een doelmatige (effectieve) en doeltreffende (efficiënte) overheidsdienst. Uit het eerste tussentijdse verslag bleek dat aan deze standaarden niet werd voldaan.

II.6.3. DE UITVOERING VAN VEILIGHEIDSVERIFICATIES DOOR INLICHTINGENDIENSTEN

De VSSE en de ADIV onderzoeken jaarlijks enkele duizenden personen die een of andere vergunning of toelating willen bekomen of die een bepaalde functie willen bekleden. Met deze onderzoeken willen ze nagaan of de betrokkenen voldoende garanties bieden op het vlak van betrouwbaarheid.

De rol die de inlichtingendiensten spelen in het kader van betrouwbaarheidsonderzoeken is niet altijd dezelfde. Soms beperkt deze zich tot het doorgeven aan andere overheden van persoonsgegevens die ze in hun bezit hebben. Soms gaan ze actief op zoek naar bijkomende gegevens. Soms verlenen ze een gemotiveerd advies en in enkele specifieke gevallen nemen ze (alleen of als onderdeel van een veiligheidsoverheid) ook de uiteindelijke beslissing omtrent het al dan niet toekennen of intrekken van de vergunning of toelating.

---

[31] Eerder in 2010 voerde het Comité, daarin geruggensteund door de toenmalige Senatoriële Begeleidingscommissie, een gelijkaardige audit uit. Deze 'prestatie-audit' bood een zicht op de toestand van de gehele militaire inlichtingendienst en wou een dynamiek op gang brengen die, waar nodig, tot reële verandering en verbetering zou leiden… VAST COMITE I, *Activiteitenverslag 2011*, 7-14 ('II.1. Een audit bij de militaire inlichtingendienst'). Het Comité formuleerde een omstandig aantal aanbevelingen (104-107, 'IX.2.1. Aanbevelingen met betrekking tot de audit bij de ADIV').

In casu lag een klacht aan de oorsprong van het toezichtonderzoek. Een medewerker op de nationale luchthaven van Brussel zag zijn toegangsbadge ingetrokken na een negatief advies[32] van de Nationale Veiligheidsoverheid (NVO). Hij diende beroep in bij het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen alsook een beroep tot nietigverklaring en tot schorsing voor de Raad van State. Het Beroepsorgaan verklaarde de klacht onontvankelijk – want ingediend tegen de beslissing van de FOD Mobiliteit en Transport en niet tegen het advies van de NVO. Ook de Raad van State verwierp de klacht. Daarop richtte de klager zich naar het Vast Comité I, zonder evenwel het voorwerp van klacht te definiëren. Hij verklaarde niet te begrijpen waarom een negatief advies werd genomen waardoor hij zijn werk verloor alsook zijn pilotenlicentie geschorst zag.

Het Comité achtte het legitiem om, vertrekkende vanuit die individuele klacht, een breder toezichtonderzoek te openen naar de wijze waarop de inlichtingendiensten veiligheidsverificaties uitvoeren.[33] Omwille van andere prioriteiten, konden de eerste onderzoeksverrichtingen pas worden uitgevoerd in oktober 2017.

II.6.4. DE ONDERSTEUNENDE DIENSTEN VAN HET OCAD

Met de Wet van 10 juli 2006 betreffende de analyse van de dreiging werd het Coördinatieorgaan voor de dreigingsanalyse (OCAD) opgericht. Het doel van dit orgaan is de politieke, bestuurlijke en gerechtelijke overheden een zo accuraat mogelijk beeld te geven van de terroristische of extremistische dreiging in of tegen België en hen toe te laten op gepaste wijze te reageren.[34] De kerntaak bestaat er in punctuele of strategische evaluaties te maken. Deze taak berust bij analisten en bij – vanuit de zogenaamde 'ondersteunende diensten' gedetacheerde – experten. De ondersteunende diensten vormen voor het coördinatieorgaan de belangrijkste informatiebron. In 2017 waren de ondersteunende diensten de VSSE, de ADIV, de geïntegreerde politie, de Administratie der Douane en Accijnzen van de FOD Financiën, de Dienst Vreemdelingenzaken van de FOD Binnenlandse Zaken, de FOD Mobiliteit en Vervoer en de FOD Buitenlandse Zaken

32 Dat luidde als volgt: *'overwegende dat betrokkene contacten met een radicale familiale omgeving heeft; overwegende dat die contacten een mogelijk veiligheidsrisico met zich meebrengen'*.

33 'Toezichtonderzoek over de manier waarop de VSSE en de ADIV veiligheidsverificaties uitvoeren, de gegevens evalueren nodig bij het toekennen van veiligheidsattesten of het formuleren van veiligheidsadviezen, dit in toepassing van artikelen 22*bis* tot 22*sexies* van de Wet van 11 december betreffende de classificatie en de veiligheidsmachtigingen, -attesten en –adviezen (W.C&VM)'. Het onderzoek werd geopend op 13 februari 2017.

34 W. VAN LAETHEM, 'Het coördinatieorgaan voor de dreigingsanalyse: een punctuele analyse', *Vigiles*, 2007, Afl. 4, 109-127. Zie tevens: Belgian Standing Committee I, *All Source threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, Antwerpen, Intersentia, 2010, 220 p.

(art. 2, 2. W.OCAD). Het betreft zeer uiteenlopende diensten, elk met een eigen cultuur en grootte.[35]

Eerder, in 2010, voerde het Vast Comité I samen met het Vast Comité P een gemeenschappelijk toezichtonderzoek uit naar de informatiestromen tussen het OCAD en de ondersteunende diensten, met bijzondere aandacht voor de twee inlichtingendiensten en de Federale en Lokale Politie.[36]

Op de gemeenschappelijke plenaire vergadering van december 2017 werd besloten een toezichtonderzoek te openen naar de 'andere' ondersteunende diensten.[37] Met dit gemeenschappelijk onderzoek wensen de Vaste Comités I en P een *status quaestionis* op te maken van de informatiestroom tussen het OCAD en de overige ondersteunende diensten en dit aan de hand van een uitgebreide bevraging.

35 De wetgever liet toe om nog andere instellingen toe te voegen aan de lijst van 'ondersteunende diensten'.

36 Hierover VAST COMITÉ I, *Activiteitenverslag 2010*, 46 ('II.12.6. Mededeling van inlichtingen aan het OCAD door de ondersteunende diensten) en meer uitgebreid *Activiteitenverslag 2011*, 25-32 ('II.4. De informatiestromen tussen het OCAD en zijn ondersteunende diensten').

37 Toezichtonderzoek betreffende de ondersteunende diensten van het OCAD met uitsluiting van de geïntegreerde politie en de inlichtingendiensten.

HOOFDSTUK III
DE CONTROLE OP DE BIJZONDERE EN BEPAALDE GEWONE INLICHTINGENMETHODEN

Dit hoofdstuk biedt een overzicht van de inzet van de bijzondere inlichtingenmethoden door de VSSE en de ADIV in 2017 en van de wijze waarop het Vast Comité I zijn jurisdictionele controletaak hierop heeft waargenomen. Het is gebaseerd op het verslag dat door het Vast Comité I werd opgesteld in uitvoering van artikel 35 § 2 van de Toezichtwet van 18 juli 1991.

Het bevat nadere cijfers over de inzet door de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) van de bijzondere en bepaalde gewone methoden en over de wijze waarop het Vast Comité I zijn jurisdictionele controletaak op de bijzondere methoden waarneemt.

Vooreerst moet echter melding worden gemaakt van de belangrijke wetswijziging die in 2017 in werking trad (meer bepaald op 8 mei 2017) met betrekking tot de taken en bevoegdheden van de inlichtingendiensten in het algemeen en de inzet van specifieke en uitzonderlijke methoden in het bijzonder. Bij Wet van 30 maart 2017 (*BS* 28 april 2017) werd de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten ingrijpend gewijzigd, ook wat betreft de inzet van bijzondere inlichtingenmethoden. Globaal genomen kan gesteld worden dat de VSSE en de ADIV meer bevoegdheden hebben gekregen. Het is binnen het bestek van dit activiteitenverslag onmogelijk om op elke wijziging in te gaan. In de mate waarin de wijziging een weerslag heeft gehad op de (inzet van) specifieke en uitzonderlijke inlichtingenmethoden, zal er in navolgende onderdelen echter wel worden bij stilgestaan.

III.1. CIJFERS MET BETREKKING TOT DE BIJZONDERE EN BEPAALDE GEWONE METHODEN

Tussen 1 januari en 31 december 2017 werden door de twee inlichtingendiensten samen 1923 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 1822 door de VSSE (waarvan 1612 specifieke en 210 uitzonderlijke) en 101 door de ADIV (waarvan 79 specifieke en 22 uitzonderlijke).

Onderstaande tabel maakt een vergelijking met de cijfers van de afgelopen jaren.

	ADIV		VSSE		TOTAAL
	Specifieke methoden	**Uitzonderlijke methoden**	**Specifieke methoden**	**Uitzonderlijke methoden**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923

Deze tabellen tonen aan dat het aantal door de ADIV ingezette methoden laag blijft en een dalende trend vertoont, terwijl de stijging bij de VSSE blijft aanhouden. Hetzelfde beeld zien we bij de gewone methode van vorderingen gericht aan operatoren om bepaalde communicatiemiddelen te identificeren. De VSSE formuleerde niet minder dan 4327 vorderingen tegenover 257 vorderingen door de ADIV.[38]

	Vorderingen door ADIV	**Vorderingen door VSSE**
2016	216	2203
2017	257	4327

In wat volgt, worden per dienst vier rubrieken onderscheiden: cijfers over bepaalde gewone methoden, over de specifieke methoden, cijfers over de uitzonderlijke methoden en cijfers inzake de dreigingen en de te verdedigen belangen die door de bijzondere methoden geviseerd worden (cijfers over de dreigingen en belangen bij de gewone methoden zijn vooralsnog niet voorhanden).

III.1.1. METHODEN MET BETREKKING TOT DE ADIV

III.1.1.1. De gewone methoden

Bij Wet van 5 februari 2016 tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie (*BS* 19 februari 2016) werd – in navolging van de aanbevelingen van het Vast Comité I[39] – de identificatie van de

[38] Er werden geen bankgegevens gevorderd in het kader van de problematiek van prepaid-kaarten (zie ook verder onder III.1.1.1.).

[39] VAST COMITÉ I, *Activiteitenverslag 2012*, 69.

gebruiker van telecommunicatie (bijv. gsm-nummer of IP-adres) of van een gebruikt communicatiemiddel als een gewone methode beschouwd in de mate waarin dit gebeurt via een vordering aan of een rechtstreekse toegang tot de klantenbestanden van een operator. Voorheen vormde dit een specifieke methode. De wijziging gebeurde door de invoeging van een nieuw artikel 16/2 in de Wet van 30 november 1998.

Wanneer de identificatie met behulp van een technisch middel verloopt (en dus niet via de vordering aan een operator) blijft de collecte een specifieke methode. Hiertoe werd artikel 18/7 § 1 W.I&V aangepast.

De regeling voorziet in een verplichting voor de VSSE en de ADIV om een register bij te houden van alle gevorderde identificaties en van alle via rechtstreekse toegang verkregen identificaties. Het Vast Comité I ontvangt maandelijks een lijst van de gevorderde identificaties en van elke toegang.[40] Ingevolge artikel 35 § 2, eerste lid, van de Toezichtwet van 18 juli 1991 rapporteert het Comité hierover aan de Kamer in zijn jaarlijks verslag.

Daarnaast werd bij Wet van 1 september 2016 (*BS* 7 december 2016) een nieuwe gewone methode ingevoerd in datzelfde artikel 16/2 W.I&V: '§ 2. *De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een bank of financiële instelling om over te gaan tot het identificeren van de eindgebruiker van de in artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie bedoelde voorafbetaalde kaart, op basis van de referentie van een elektronische banktransactie die verband houdt met de voorafbetaalde kaart en die voorafgaand meegedeeld is door een operator of verstrekker in toepassing van paragraaf 1.*' De VSSE en de ADIV moeten – net zoals bij de identificatie van de gebruiker van telecommunicatie of van een gebruikt communicatiemiddel – een register bijhouden van alle gevorderde identificaties. Ingevolge artikel 35 § 2, eerste lid, van de Toezichtwet van 18 juli 1991 moet het Comité ook hierover aan de Kamer rapporteren in zijn jaarlijks verslag.[41]

---

40 In de praktijk krijgt het Comité maandelijks een brief met daarin het aantal vorderingen. Het Comité besliste dat het zich kon vinden in deze werkwijze maar voegt eraan toe dat het enerzijds zal toezien op de wijze waarop de inlichtingendiensten intern het gebruik van deze methode controleren én anderzijds jaarlijks steekproefsgewijs een aantal vorderingen zal controleren. Dit impliceert dat de diensten de gevorderde verkregen gegevens te allen tijde ter beschikking moeten houden van het Vast Comité I.

41 Bij Wet van 25 december 2016 (*BS* 25 januari 2017) werd de mogelijkheid ingebouwd voor de VSSE en de ADIV om toegang te krijgen tot informatie die berust bij de Passagiersinformatie-eenheid (art. 16/3 W.I&V). Het Comité wordt in kennis gesteld van deze methode en kan ze desgevallend verbieden. Anders dan voor de methoden opgenomen in art. 16/2 W.I&V werd niet voorzien in een verplichte verslaggeving aan het Parlement; art. 35 § 2 W.Toezicht werd immers niet aangepast. Het Vast Comité I beveelt aan om dit alsnog te doen, temeer over het opvragen van vervoers- en reisgegevens op basis van art. 18/6/1 W.I&V wél moet gerapporteerd worden omdat dit een specifieke methode vormt. Het Comité is overigens van oordeel dat dergelijke rapportage ook aangewezen is voor de bij Wet van 21 maart 2018 (*BS* 16 april

Onderstaande tabel biedt een overzicht van (1) het aantal vorderingen aan operatoren (er waren in 2017 rechtstreekse toegangen (3) noch vorderingen aan bankinstellingen (4)) en (2) het aantal nummers waarop die vorderingen betrekking hadden (in één vordering worden soms tientallen nummers hernomen).

	Identificaties i.v.m. telecommunicatie			**Identificatie i.v.m. telecommunicatie via rechtstreekse toegang (3)**	**Identificatie i.vm. pre-paid kaart (4)**
	Aantal methoden	**Aantal vorderingen (1)**	**Aantal nummers (2)**		
2013	66	niet gekend	niet gekend	niet van toepassing	niet van toepassing
2014	67	niet gekend	niet gekend	niet van toepassing	niet van toepassing
2015	55	niet gekend	niet gekend	niet van toepassing	niet van toepassing
2016	niet gekend	216	niet gekend	0	niet van toepassing
2017	niet gekend	257	1058	0	niet van toepassing

III.1.1.2. De specifieke methoden

Onderstaande tabel geeft de cijfers weer over de toepassing van de specifieke methoden door de ADIV. Vooreerst wordt uitleg verschaft bij de verschillende rubrieken. Er kunnen zeven specifieke methoden onderscheiden worden. Gelet op de tussengekomen wetswijziging werd de draagwijdte van elke methode vanaf 8 mei 2017 gewijzigd (lees: verruimd). Echter, om de zaak niet nodeloos complex te maken, werden de cijfers van voor en na de wetswijziging niet uitgesplitst.

A. Voor 8 mei 2017 – Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel (art. 18/2 § 1, 1° en 18/4 W.I&V)
   Na 8 mei 2017 – Observeren in publiek toegankelijke plaatsen met een technisch middel of al dan niet met behulp van een technisch middel observeren in een niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is (art. 18/4 W.I&V)
B. Voor 8 mei 2017 – Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel (art. 18/2 § 1, 2° en 18/5 W.I&V)
   Na 8 mei 2017 – Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (18/5 W.I&V)
C. Voor 8 mei 2017 – Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/2 § 1, 3° en 18/6 W.I&V)
   Na 8 mei 2017 – Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)

2018) ingevoerde mogelijkheid tot het gebruik van in databestanden opgeslagen camerabeelden (art. 16/4 W.I&V).

D. Voor 8 mei 2017 – Niets voorzien
   Na 8 mei 2017 – Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)
E. Heel 2017 – De identificatie met behulp van een technisch middel, van de elektronische communicatiediensten en –middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt en de vordering van de operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst tot het bekomen van de gegevens betreffende de betalingswijze, de identificatie van het betalingsmiddel en het tijdstip van betaling voor het abonnement of voor het gebruik van de elektronische communicatiedienst (art. 18/7 W.I&V)
F. Heel 2017 – Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8 W.I&V)
G. Heel 2017 – Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator (art. 18/8 W.I&V).

Specifieke methoden (ADIV)	**Aantal toelatingen**
Observatie	7
Doorzoeking	0
Identificatie postverkeer	0
Vervoers- en reisgegevens	0
Identificatie abonnee of communicatie- of betaalmiddel	4
Opsporen verkeersgegevens	36
Kennisname lokalisatiegegevens	32
TOTAAL	**79**

Wat betreft de inzet van specifieke methoden door de ADIV zijn er geen opvallende trends te melden.

III.1.1.3. De uitzonderlijke methoden

Ook de uitzonderlijke methoden werden op sommige vlakken gewijzigd door de Wet van 30 maart 2017. Hieronder wordt hieronder duidelijk om welke wijzigingen het ging.

A. Voor 8 mei 2017 – Al dan niet met behulp van technische middelen, in private plaatsen die niet toegankelijk zijn voor het publiek, in woningen of in een door een woning omsloten eigen aanhorigheid in de zin van de artikelen 479, 480 en 481 van het Strafwetboek, of in een lokaal aangewend voor beroepsdoeleinden of als woonplaats door een advocaat, een arts of een journalist observeren

en deze plaatsen betreden om in het kader van een observatie een technisch middel te installeren, herstellen of terug te nemen (art. 18/2 § 2, 1° en 18/11 W.I&V);
Na 8 mei 2017 – Al dan niet met behulp van technische middelen, observeren in niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en betreden van al dan niet aan het zicht onttrokken niet voor het publiek toegankelijke plaatsen om te observeren, een technisch middel te installeren, een voorwerp te openen of mee te nemen (art. 18/11 W.I&V)

B. Voor 8 mei 2017 – Al dan niet met behulp van technische middelen, deze plaatsen doorzoeken (art. 18/2 § 2, 2° en 18/12 W.I&V)
Na 8 mei 2017 – Al dan niet met behulp van technische middelen niet voor het publiek toegankelijke plaatsen doorzoeken, evenals al dan niet vergrendelde voorwerpen die zich daar bevinden (art. 18/12 W.I&V)

C. Voor 8 mei 2017 – Oprichten of gebruiken van een rechtspersoon ter ondersteuning van operationele activiteiten en gebruiken van agenten van de dienst, onder de dekmantel van een fictieve identiteit of hoedanigheid (art. 18/2 § 2, 3° en 18/13 W.I&V)
Na 8 mei 2017 – Een rechtspersoon als bedoeld in art. 13/3 § 1 W.I&V inzetten om gegevens te verzamelen (art. 18/13 W.I&V)

D. Heel 2017 – Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V);

E. Heel 2017 – Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)

F. Heel 2017 – Binnendringen in een informaticasysteem (art. 18/16 W.I&V)

G. Heel 2017 – Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)

Uitzonderlijke methoden (ADIV)	**Aantal toelatingen**
Observatie	7
Doorzoeking	10
Fictieve rechtspersoon	0
Openen post	0
Verzamelen bankgegevens	2
Binnendringen informaticasystemen	1
Afluisteren communicatie	1
TOTAAL	**22**

III.1.1.4. De opdrachten en de dreigingen die de inzet van de bijzondere methoden rechtvaardigen[42]

Sinds de inwerkingtreding van de Wet van 29 januari 2016 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, mag de ADIV specifieke en de uitzonderlijke methoden aanwenden in het kader van vier opdrachten. Dit betekent dat deze methoden alleen niet kunnen ingezet worden in het kader van veiligheidsonderzoeken of andere door bijzondere wetten aan de ADIV toevertrouwde opdrachten (bijv. het verrichten van veiligheidsverificaties voor kandidaat-militairen). Bij Wet van 30 maart 2017 werden wel wijzigingen aangebracht aan deze vier opdrachten. Zij kunnen voortaan als volgt worden samengevat:

1. **De inlichtingenopdracht (art. 11, 1° W.I&V)**
   Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties.
   Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die volgende belangen bedreigt of zou kunnen bedreigen:
   - de onschendbaarheid van het nationaal grondgebied of het voortbestaan van de gehele of een deel van de bevolking;
   - de militaire defensieplannen;
   - het wetenschappelijk en economisch potentieel op vlak van defensie;
   - de vervulling van de opdrachten van de strijdkrachten;
   - de veiligheid van de Belgische onderdanen in het buitenland.
2. **De zorg voor het behoud van de militaire veiligheid (art. 11, 2° W.I&V)**
   - de militaire veiligheid van het personeel dat onder de minister van Landsverdediging ressorteert;
   - de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen;
   - in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten.
3. **De bescherming van geheimen (art. 11, 3° W.I&V)**
   Het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen,

42 Per toelating kunnen meerdere opdrachten en dreigingen aan de orde zijn.

geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de minister van Landsverdediging beheert.

4. **Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied (art. 11, 5° W.I&V).**

Sinds de inwerkingtreding van de Wet van 30 maart 2017 is de inzet van bijzondere methoden niet meer beperkt tot het Belgische grondgebied (art. 18/1, 2° W.I&V).

In acht genomen dat per toelating verschillende dreigingen aan de orde kunnen zijn, kunnen onderstaande cijfers worden opgetekend:

AARD VAN DE OPDRACHT	AANTAL 2017
1. Inlichtingenopdracht	48
2. Militaire veiligheid	2
3. Bescherming geheimen	5
4. Activiteiten buitenlandse diensten in België opvolgen	46

AARD DREIGING	AANTAL 2017
1. Spionage	77
2. Terrorisme (en radicaliseringsproces)	16
3. Extremisme	4
4. Inmenging	4
5. Criminele organisatie	0
6. Andere	0

In dit refertejaar zijn voor het eerst cijfers beschikbaar over de opvolging van activiteiten van buitenlandse diensten in België. Het cijfer ligt meteen zeer hoog. Toch mag hier niet uit worden afgeleid dat de ADIV in 2017 een nieuw soort dreiging opvolgt. De opvolging van buitenlandse diensten werd voorheen immers sneller aangeknoopt bij de 'inlichtingenopdracht' in het kader van de strijd tegen 'spionage'.

III.1.2. METHODEN MET BETREKKING TOT DE VSSE

III.1.2.1. De gewone methoden

Onderstaande tabel biedt een overzicht van (1) het aantal vorderingen aan operatoren (er waren in 2017 rechtstreekse toegangen (3) noch vorderingen aan bank-

instellingen (4)) en (2) het aantal nummers waarop die vorderingen betrekking hadden (in één vordering worden soms tientallen nummers hernomen).

	Identificaties i.v.m. telecommunicatie			Identificatie i.v.m. telecommunicatie via rechtstreekse toegang (3)	Identificatie i.v.m. pre-paid kaart (4)
	Aantal methoden	**Aantal vorderingen (1)**	**Aantal nummers (2)**		
2013	66	niet gekend	niet gekend	niet van toepassing	niet van toepassing
2014	67	niet gekend	niet gekend	niet van toepassing	niet van toepassing
2015	55	niet gekend	niet gekend	niet van toepassing	niet van toepassing
2016	niet gekend	2203	niet gekend	0	niet van toepassing
2017	niet gekend	4327	21566	0	niet van toepassing

Los van het feit dat het *quasi* onmogelijk is om de cijfers inzake identificaties over de jaren heen te vergelijken, kan het Comité niet om de vaststelling heen dat er sinds de invoering van de versoepelde procedure *ex* artikel 16/2 W.I&V veel meer identificaties worden verricht. Vanuit zijn algemene toezichtsbevoegdheid, zal het Comité de VSSE vragen intern te onderzoeken in welke mate dit hoge aantal vorderingen (mede) wordt veroorzaakt door het versoepelen van de procedure. Daarbij moet o.m. aandacht worden besteed aan de aard van dreigingen die de vorderingen rechtvaardigden en aan de vraag of en in welke mate dergelijke vorderingen gebeuren op verzoek van buitenlandse overheden/partnerdiensten.

III.1.2.2. De specifieke methoden

Specifieke methoden (VSSE)	**Aantal toelatingen**
Observatie	121
Doorzoeking	0
Identificatie postverkeer	0
Vervoers- en reisgegevens	54
Identificatie abonnee of communicatie- of betaalmiddel	49
Opsporen verkeersgegevens	708
Kennisname lokalisatiegegevens	680
TOTAAL	**1612**

Alhoewel het door de tussengekomen wetswijziging niet evident is om bovenstaande cijfers te vergelijken met vorige jaren, kan toch gesteld worden dat de stijging van het aantal specifieke methoden voornamelijk het gevolg is van het sterk gestegen aantal 'lokalisaties' (680 tegenover 596 vorig jaar).

III.1.2.3. De uitzonderlijke methoden

Uitzonderlijke methoden (VSSE)	Aantal toelatingen
Observatie	9
Doorzoeking	22
Fictieve rechtspersoon	0
Openen post	15
Verzamelen bankgegevens	10
Binnendringen informaticasystemen	35
Afluisteren communicatie	119
TOTAAL	**210**

De talrijke aanslagen in binnen- en buitenland hadden de daling in het aantal toegepaste uitzonderlijke methoden dat in 2015 te noteren viel, in 2016 omgezet in een sterke stijging. Die trend zette zich in 2017 door. Het aantal tapmaatregelen stagneerde.

III.1.2.4. 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). Sinds 8 mei 2017 mogen de uitzonderlijke methoden ook ingezet worden in het kader van het extremisme en de inmenging; voordien was dit niet toegelaten. De wet hanteert volgende definities:

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.

Sinds de inwerkingtreding van de Wet van 30 maart 2017 mogen de bijzondere methoden ook worden ingezet '*vanaf het grondgebied van het Rijk*' en dus niet alleen meer '*op*' het grondgebied (art. 18/1, 1° W.I&V).

In acht genomen dat per toelating verschillende dreigingen aan de orde kunnen zijn, kunnen volgende cijfers worden opgetekend:

AARD DREIGING	AANTAL 2017
1. Spionage	308
2. Terrorisme (en radicaliseringsproces)	678
3. Extremisme	63
4. Proliferatie	4
5. Schadelijke sektarische organisaties	0
6. Inmenging	9
7. Criminele organisaties	0
8. Activiteiten buitenlandse diensten in België opvolgen[44]	308

43 Deze bevoegdheid werd pas ingevoegd bij Wet van 29 januari 2016.

Bovenstaande cijfers tonen aan dat 'terrorisme', wat betreft de inzet van BIM-methoden, de absolute prioriteit blijft voor van de VSSE.

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:

1. 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 continuiteit 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
2. 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;
3. De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

AARD BELANG	AANTAL 2017
De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde	1053
De uitwendige veiligheid van de Staat en de internationale betrekkingen	1024
De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel	17

III.2. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS JURDISCTIONEEL 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 hier uitsluitend aandacht besteed worden aan de ter zake genomen jurisdictionele beslissingen en niet aan de operationele gegevens. 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. Tevens woont een lid van de Dienst Enquêtes sinds 2017 de tweewekelijkse vergaderingen bij waarop de VSSE de BIM-Commissie inlicht over de uitvoering van de uitzonderlijke methoden. Hierover wordt een verslag op gemaakt ten behoeve van het Vast Comité I, dat op deze wijze een beter zicht heeft op deze methoden.[44]

Artikel 43/4 W.I&V stelt dat het Vast Comité I op vijf manieren kan worden gevat:

1. Op eigen initiatief;
2. Op verzoek van de Commissie voor de bescherming van de persoonlijke levenssfeer;
3. Op klacht van een burger;
4. Van rechtswege als de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden;
5. 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 de specifieke of uitzonderlijke methoden die inlichtingen hebben opgeleverd die in een strafzaak worden gebruikt. De beslissing om een advies te vragen berust bij de onderzoeksgerechten of de strafrechters. Strikt genomen treedt het Comité alsdan niet op als jurisdictioneel orgaan.

WIJZE VAN VATTING	2013	2014	2015	2016	2017
1. Op eigen initiatief	16	12	16	3	1
2. Privacycommissie	0	0	0	0	0
3. Klacht	0	0	0	1	0
4. Schorsing door BIM-Commissie	5	5	11	19	15
5. Toelating minister	2	1	0	0	0
6. Prejudicieel adviesverlener	0	0	0	0	0
TOTAAL	**23**	**18**	**27**	**23**	**16**

Het aantal door het Comité genomen beslissingen daalde in 2017, ondanks de stijging van het aantal methoden en het feit dat er medio 2017 een nieuwe, com-

[44] Het Comité beval ook de ADIV aan dergelijke tweewekelijkse vergaderingen te organiseren. Het betreft immers een wettelijke verplichting (art. 18/10 § 1, derde lid W.I&V en art. 9 KB 12 oktober 2010).

plexe wetswijziging in werking trad. Op één na zijn alle vattingen het gevolg van een schorsing door de BIM-Commissie.

Eens gevat, kan het Comité verschillende soorten (tussen)beslissingen nemen (de tussenbeslissingen staan vermeld onder de punten 3 tot 10; de eindbeslissingen onder 11 tot 16). In drie gevallen (1, 2 en – soms – 6) wordt 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);
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). Deze termijn werd in alle dossiers gerespecteerd.

AARD VAN DE BESLISSING	2013	2014	2015	2016	2017
Beslissingen voorafgaand aan de vatting					
1. Nietige klacht	0	0	0	0	0
2. Kennelijk ongegronde klacht	0	0	0	0	0
Tussenbeslissingen					
3. Schorsing methode	0	3	2	1	0
4. Bijkomende informatie van BIM-Commissie	0	0	0	0	0
5. Bijkomende informatie van inlichtingendienst	0	1	1	4	0
6. Onderzoeksopdracht Dienst Enquêtes	50	54	48	60	35
7. Horen BIM-Commissieleden	0	0	2	0	0
8. Horen leden inlichtingendiensten	0	0	2	0	0
9. Beslissing m.b.t. geheim van onderzoek	0	0	0	0	0
10. Gevoelige informatie tijdens verhoor	0	0	0	0	0
Eindbeslissingen					
11. Stopzetting methode	9	3	3	6	9
12. Gedeeltelijke stopzetting methode	5	10	13	4	6
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	2	0	4	11	0
14. Onbevoegd	0	0	0	0	0
15. Wettige toelating / Geen stopzetting methode / Ongegrond	7	4	6	2	1
Prejudicieel advies					
16. Prejudicieel advies	0	0	0	0	0

III.2.2. DE RECHTSPRAAK

Hieronder wordt de essentie weergegeven van de eindbeslissingen die het Vast Comité I in 2017 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 sommige beslissingen werden geclassificeerd.

De beslissingen werden gegroepeerd onder drie rubrieken:

- Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode;
- Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging;
- De gevolgen van een onwettig(e) (uitgevoerde) methode.

III.2.2.1. Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode: voorafgaande beslissing van het diensthoofd en kennisgeving BIM-Commissie

Een specifieke methode kan pas effectief worden aangewend na kennisgeving van de toelating van het diensthoofd aan de BIM-Commissie (art. 18/3 § 1, tweede lid, W.I&V). In dossier 2017/5650 was hierover twijfel gerezen. De BIM-Commissie had gemerkt dat een observatie met een camera via een specifieke methode door het diensthoofd was verlengd, maar dat er een aantal dagen verlopen was tussen het einde van de eerste periode en het begin van de tweede. Ze schorste dan ook de methode wat betreft de korte periode tussen de twee geldige toelatingen. Ook voor het Vast Comité I kon de betrokken dienst niet uitsluiten dat er tijdens die enkele dagen geen gegevens waren ingewonnen. Daarom besloot het Comité als volgt: *'que la mise en œuvre éventuelle de la méthode spécifique ne résulte en effet pas d'une décision [du chef de service] avec information concomitante à la Commission BIM; que dans cette mesure ces données éventuellement recueillies sont illégales et que la procédure légale prévue par la Loi R&S trouve à s'appliquer même si [le service] envisage la destruction des données éventuellement recueillies.*'[45]

In een ander geval had de BIM-Commissie vastgesteld dat een inlichtingendienst gedurende meerdere dagen met een technisch hulpmiddel een woning had geobserveerd (art. 18/4 W. I&V) zonder de vereiste toelating (dossier 2017/5807). De periode voordien en nadien was wel gedekt door een geldige machtiging. Naar alle waarschijnlijkheid betrof het een loutere vergetelheid. Toch oordeelde het

[45] '*dat de eventuele aanwending van de specifieke methode inderdaad niet resulteert uit een beslissing (van het diensthoofd) met kennisgeving aan de BIM-Commissie; dat in voorkomend geval de eventueel ingezamelde gegevens onwettig zijn en dat de wettelijke procedure voorzien in de W.I&V toepassing vindt, zelfs indien [de dienst] overweegt over te gaan tot de vernietiging van de eventueel ingezamelde gegevens*'. (vrije vertaling).

Comité dat het '*ontegensprekelijk vaststaat dat de vigerende wettelijke bepalingen voor het uitvoeren van een BIM niet werden nageleefd. Dat de verklaringen van de [dienst] – stellende dat de methode, bestaand uit het observeren van een woning, goede resultaten oplevert – hieraan geen afbreuk doen. Dat de zwaarwichtigheid van het dossier deze onwettige situatie evenmin kan rechtzetten*.' Het Comité gelastte dan ook de vernietiging van de onrechtmatig bekomen inlichtingen.

Het Comité diende identieke beslissingen te nemen in dossiers 2017/5832 en 2017/5843. Daarin was namelijk dezelfde problematiek van een 'niet-aansluitende verlenging' aan de orde: de dienst was vergeten een machtiging te verlenen voor een periode van respectievelijk drie en zes dagen tussen twee geldige machtigingen. Ook hier oordeelde het Comité dat '*de zwaarwichtigheid van het dossier de aangehaalde onwettige situatie niet kan rechtzetten*.'

Wanneer de BIM-Commissie van het diensthoofd van een inlichtingendienst verneemt dat er gedurende een maand een observatie plaatsvond zonder wettige toelating, beveelt zij '*d'interdire l'exploitation des données ainsi récoltées*'[46] (dossier 2017/5900). Het Comité kon deze beslissing alleen maar bevestigen.

Ook in dossier 2017/5998 merkte de dienst zelf op dat een specifieke methode verder was uitgevoerd na het verstrijken van de in de toelating vermelde termijn. De dienst stelde de BIM-Commisie hiervan in kennis en deze verbood de exploitatie van de aldus verzamelde gegevens. Het Comité, dat ambtshalve gevat was, bevestigde de beslissing van de Commissie aangezien '*des données ont été récoltées au-delà de la période prévue par la décision du chef de service; que ces données n'ont pas été récoltées conformément à la loi à défaut d'autorisation du chef de service.*'[47]

III.2.2.2. Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging

III.2.2.2.1. Het opvragen van telefoniegegevens

In drie identieke gevallen wenste een inlichtingendienst over te gaan tot de kennisname van oproepgegevens en de lokalisatie van een bepaald gsm-toestel (dossiers 2017/5573, 2017/5574 en 2017/5575). Uit bijkomende gegevens die door de BIM-Commissie waren opgevraagd, bleek dat de dienst aan dat nummer was geraakt door een beroep te doen op een gewone methode (art. 16/2 W.I&V) terwijl uit de vordering aan de operator bleek dat het niet om een eenvoudige identificatie van een nummer ging maar '*sur l'identification réalisée au moyen d'une opéra-*

46 '*de exploitatie van de op deze wijze verzamelde gegevens te verbieden.*' (vrije vertaling).

47 '*de gegevens werden verzameld buiten de periode voorzien door de beslissing van het diensthoofd; dat deze gegevens niet werden verzameld conform de wet bij gebreke van de toestemming van het diensthoofd.*' (vrije vertaling).

tion technique, telle que la consultation des informations passées par un mat'.[48] De gehanteerde methode vereiste de inzet van een specifieke methode (art. 18/8 § 1, 1° en 2° W.I&V) (zie hierover ook III.2.3.).

Op 3 april 2017 beslist een inlichtingendienst in twee gelieerde dossiers (2017/5776 en 2017/5777) om op basis van art. 18/8 W. I&V informatie te bekomen over de oproepgegevens van een telefoonnummer en dit voor de afgelopen negen maanden. De wet laat dit, gegeven de betrokken dreiging, toe voor maximaal '*negen maanden voorafgaand aan de beslissing*'. Nu bleek echter dat de dienst informatie wenste te bekomen vanaf 1 juli 2016. Het Comité oordeelde evenwel '*[d]at de uiterste datum om negen maanden terug te gaan in de tijd – rekening houdend met het moment van beslissing, zijnde 3 april 2017 – 2 juli 2016 is en niet 1 juli 2016*'. Het vergaren van telefoniegegevens op 1 juli 2016 was dan ook niet door een wettige methode gedekt.

Dossier 2017/5916 was in dit opzicht identiek. De dienst wou overgaan tot de kennisname van oproep- en lokalisatiegegevens (art. 18/8 § 1 W.I&V) voor een periode die zich uitstrekte van 19 mei 2016 tot 16 mei 2017. Echter, in uitvoering van artikel 18/8 § 2 W.I&V '*la récolte de telles données ne peut excéder une période de 12 mois précédant le jour de la décision*'.[49] Aangezien deze beslissing was genomen op 23 mei 2017 '*la période maximale de récolte rétroactive de données ne peut donc s'étendre que du 22 mai 2016 au 22 mai 2017*.'[50] De beslissing van het diensthoofd werd dan ook vernietigd wat betreft de gegevensverzameling van 19 tot en met 21 mei 2016.

Deze rechtspraak werd nadien nog in twee verschillende dossiers herhaald.

Artikel 18/8, § 2 W.I&V bepaalt dat '[v]*oor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met terrorisme of extremisme, […] het diensthoofd in zijn beslissing de [telefonie]gegevens [kan] vorderen voor een periode van 12 maanden voorafgaand aan de beslissing*.' *In casu* dateerde de beslissing van 27 december 2017. Daaruit volgt dat de methode kan betrekking hebben op de periode tussen 26 december 2016 en 26 december 2017. De dienst had evenwel gegevens opgevraagd vanaf 20 december 2016 tot 20 december 2017. Het Comité concludeerde dan ook dat '*deze methode […] wettelijk gezien 6 dagen te vroeg start, nu pas vanaf 26 december 2016 de methode mocht worden geactiveerd*' (dossier 2017/6611).

In dossier 2017/6612 was de dreiging 'spionage' zodat de telefoniegegevens slechts konden gevorderd worden '*voor een periode van 9 maanden voorafgaand aan de beslissing*' (art. 18/8 § 2, 2° W.I&V). De beslissing van het diensthoofd respecteerde die limiet niet en was dus gedeeltelijk onwettig.

---

48 *'op basis van de identificatie gerealiseerd door een technische operatie, zoals de raadpleging van informatie binnengekomen via een mast'.* (vrije vertaling).

49 *'het inzamelen van dergelijke gegevens mag een periode van 12 maanden voorafgaand aan de dag van de beslissing, niet overschrijden.'* (vrije vertaling).

50 '*de maximale periode voor de retroactieve inzameling van gegevens mag zich uitstrekken van 22 mei 2016 tot 22 mei 2017'.* (vrije vertaling).

Wanneer de BIM-Commissie bij de betrokken inlichtingendienst opvraagt welke vordering werd gezonden naar de telecom-operator in uitvoering van een perfect wettelijke toelating om kennis te nemen van oproepgegevens, stelt zij vast dat ook lokalisatiegegevens werden opgevraagd (dossier 2017/5994). Aangezien het opvragen van deze gegevens niet vervat was in de toelating, besloot het Comité dat '*les données de localisation éventuellement obtenues de l'opérateur l'ont été illégalement*.'[51]

III.2.2.2.2. Het opvragen van reisgegevens

Een inlichtingendienst wenste de vliegtuigreizen in beeld te brengen van een target die in contact stond met een persoon die in het buitenland een terroristische cel zou hebben opgericht (dossier 2017/6208). De methode had betrekking op een periode van meer dan tweeëneenhalf jaar. Het Comité stelde vast dat '*la méthode est prévue par l'article 18/6/1 de la L.R&S qui ne fixe pas de limite de temps*.'[52] Het Comité merkte evenwel op dat de wetgever wel tijdslimieten had gesteld in het kader van de methode voorzien in artikel 18/8 W.I&V. Zo werd de mogelijkheid om telefoniegegevens op te vragen beperkt tot zes, negen of twaalf maanden voorafgaand aan de beslissing van het diensthoofd en dit in functie van de aard van de dreiging. Het Comité voegde hier echter aan toe '*que ce serait ajouter une condition non prévue par l'article 18/6/1 que de limiter dans le temps les demandes de données de voyage par référence à l'article 18/8*.'[53] Dit betekent evenwel niet dat dergelijke methode ongelimiteerd kan ingezet worden: '*toutes les méthodes de recueil de données, qu'elles soient spécifiques ou exceptionnelles, doivent respecter les principes de subsidiarité et de proportionnalité; que le Comité permanent R a déjà fait application de ce principe pour limiter dans le temps une observation spécifique visée à l'article 18/4 (cf. Rapport d'activité 2010, 68) […]; Attendu que, dans le cas d'espèce, la nature et la gravité de la menace décrites dans la décision […] sont telles qu'une réquisition de données de transport pour une période de 32 mois […] n'enfreint pas le principe de proportionnalité*.'[54]

---

51 '*de lokalisatiegegevens mogelijks ontvangen van de operator, onwettig werden verkregen*'. (vrije vertaling).

52 '*de methode wordt vastgesteld door artikel 18/6/1 W.I&V dewelke geen tijdslimiet bepaalt*. (vrije vertaling).

53 '*dat de verzoeken om reisgegevens op te vragen, onder verwijzing naar artikel 18/8 in tijd te beperken, zou betekenen dat een niet voorziene voorwaarde aan artikel 18/6/1 zou toegevoegd worden.*' (vrije vertaling).

54 '*alle inlichtingenmethoden, ongeacht of ze specifiek of uitzonderlijk zijn, moeten de principes van subsidiariteit en proportionaliteit respecteren; Dat het Vast Comité I reeds eerder dit principe heeft toegepast om een specifieke observatie voorzien in artikel 18/4 (cf. Activiteitenverslag 2010, pag. 68) in tijd te beperken; Overwegende dat, in het onderhavig geval, de aard en de ernst van de dreiging zoals beschreven in de beslissing […] van die aard zijn dat een vordering van de reisgegevens voor een periode van 32 maanden […] geen inbreuk vormt op het proportionaliteitsprincipe.*' (vrije vertaling).

III.2.2.3. De gevolgen van een onwettig(e) (uitgevoerde) methode

Een inlichtingendienst wenste over te gaan tot de kennisname van oproepgegevens en de lokalisatie van een bepaald gsm-toestel (dossiers 2017/5573, 2017/5574 en 2017/5575). Uit bijkomende gegevens die door de BIM-Commissie waren opgevraagd, bleek dat de dienst aan dat nummer was geraakt door een beroep te doen op een gewone methode (art. 16/2 W.I&V) terwijl uit de vordering aan de operator bleek dat het niet om een eenvoudige identificatie van een nummer ging. De gehanteerde methode vereiste de inzet van een specifieke methode (art. 18/8 § 1, 1° en 2° W.I&V). *'Attendu en conséquence que les numéros de GSM obtenus l'ont été d'une manière non conforme à la loi; Attendu que cette illégalité à l'origine ne peut qu'entraîner l'illégalité des méthodes qui se fondent sur cette méthode jugée illégale; Attendu en conséquence que la présente méthode ne peut qu'être illégale'.*[55]

III.3. CONCLUSIES EN AANBEVELINGEN

Het Vast Comité I formuleert volgende algemene conclusies en aanbevelingen:

- Het aantal door de VSSE ingezette bijzondere methoden blijft sterk stijgen. Dit was, wat betreft 2017, te verklaren door de toegenomen inlichtingen-activiteiten ingevolge de aanhoudende terreurdreiging. De stijging was grotendeels toe te schrijven aan het fors toegenomen aantal 'lokalisaties'.
- Ondanks de aanhoudende terreurdreiging daalde het (reeds lage) aantal bijzondere methoden die door de ADIV worden ingezet opnieuw.
- Wat betreft de ADIV benadrukt het Comité de naleving van de wettelijke verplichting om de BIM-Commissie tweewekelijks in te lichten over de uitvoering van de uitzonderlijke methoden (art. 18/10 § 1, derde lid W.I&V en art. 9 KB 12 oktober 2010).
- ADIV richtte zich bij de inzet van BIM-methoden zoals steeds meer op de dreiging van 'spionage' terwijl dit voor de VSSE 'terrorisme' was.
- Los van het feit dat het *quasi* onmogelijk is om de cijfers inzage identificaties over de jaren heen te vergelijken, kan het Comité niet om de vaststelling heen dat er sinds de invoering van de versoepelde procedure *ex* artikel 16/2 W.I&V veel meer identificaties worden verricht. Vanuit zijn algemene toezichtsbevoegdheid zal het Comité aan de VSSE vragen om intern te onderzoeken in welke mate dit hoge aantal vorderingen (mede) wordt veroorzaakt door het versoepelen van de procedure. Daarbij moet o.m. aandacht worden besteed

[55] *'Overwegende dat bijgevolg de GSM-nummers werden verkregen op een manier die niet conform is aan de wet; Overwegende dat deze onrechtmatigheid aan de basis slechts kan leiden tot de onwettigheid van de methoden die zich baseren op een als onwettig bestempelde methode; Overwegende dat bijgevolg de hier beschreven methode alleen maar onwettig kan zijn'.* (vrije vertaling).

aan de aard van dreigingen die de vorderingen rechtvaardigden en aan de vraag of en in welke mate dergelijke vorderingen gebeuren op verzoek van buitenlandse overheden/ partnerdiensten.

- Anders dan voor de inzet van bijzondere methoden beschikt het Comité niet over de cijfers met betrekking tot de geviseerde dreiging en de te verdedigen belangen wat betreft de gewone methoden *ex* artikel 16/2 W.I&V. Het Comité beveelt de diensten aan ook deze gegevens te registreren en ter beschikking te stellen van het Vast Comité I.
- Bij Wet van 25 december 2016 (*BS* 25 januari 2017) werd de mogelijkheid ingebouwd voor de VSSE en de ADIV om toegang te krijgen tot informatie die berust bij de Passagiersinformatie-eenheid (art. 16/3 W.I&V). Het Comité wordt in kennis gesteld van deze methode en kan ze desgevallend verbieden. Anders dan voor artikel 16/2 W.I&V werd niet voorzien in een verplichte verslaggeving aan het Parlement; artikel 35 § 2 W.Toezicht werd immers niet aangepast. Het Vast Comité I beveelt aan om dit alsnog te doen, temeer over het opvragen van vervoers- en reisgegevens op basis van artikel 18/6/1 W.I&V wél moet gerapporteerd worden omdat dit een specifieke methode vormt. Het Comité is overigens van oordeel dat dergelijke rapportage ook aangewezen is voor de bij Wet van 21 maart 2018 (*BS* 16 april 2018*)* ingevoerde mogelijkheid tot het gebruik van in databestanden opgeslagen camerabeelden (art. 16/4 W.I&V).
- Het Comité diende slechts in 15 dossiers een onwettigheid vast te stellen. Zoals uit de analyse van de rechtspraak blijkt, betreft het voornamelijk dossiers waarin de betrokken inlichtingendienst nagelaten had een toelating tot het uitvoeren van een methode te verlenen voor de (soms korte) periode tussen twee geldige methoden.

HOOFDSTUK IV
DE CONTROLE OP BUITENLANDSE INTERCEPTIES, BEELDOPNAMEN EN IT-INTRUSIES

Bij Wet van 30 november 1998 kreeg de ADIV een beperkte interceptiebevoegdheid: 'het onderscheppen, het afluisteren, de kennisname of de opname, […] om redenen van militaire aard, van militaire radioverbindingen uitgezonden in het buitenland.'

In 2003 werd die mogelijkheid aanzienlijk uitgebreid, zowel wat betreft de aard van de communicatie als wat betreft de dreiging. Sindsdien mag de ADIV zijn intercepties richten op '*elke vorm van communicatie uitgezonden in het buitenland zowel om redenen van militaire aard in het kader van de opdrachten gedefinieerd in artikel 11, § 2, 1° en 2° van deze wet als om redenen van veiligheid en bescherming van onze troepen en van deze van onze geallieerden tijdens operaties in het buitenland en van onze onderdanen die in het buitenland gevestigd zijn, zoals gedefinieerd in hetzelfde artikel 11, § 2, 3° et 4°.*' Gelet op deze verruimde bevoegdheid, werd een specifieke controletaak toevertrouwd aan het Vast Comité I (zie verder).

In 2010 werd de Wet opnieuw gewijzigd[56]: naast het '*het onderscheppen, het afluisteren, het kennisnemen of het opnemen*' kon de ADIV voortaan ook communicatie '*zoeken*'. Voorafgaand aan het onderscheppen, het afluisteren, het kennisnemen of het opnemen moet de ADIV immers in staat zijn het ganse elektromagnetische spectrum en de *cyberspace* te bewaken, bijvoorbeeld om nieuwe (exploitatie)mogelijkheden te zoeken en te identificeren of om over voldoende informatie te beschikken om met zekerheid vast te stellen dat bepaalde intercepties toegestaan zijn.

In 2017 werden de bevoegdheden van de ADIV opnieuw verruimd, net zoals de controletaak van het Vast Comité I. In een eerste onderdeel wordt die wetswijziging kort besproken. In een tweede onderdeel wordt de wijze waarop het Comité in 2017 zijn specifieke controletaak in deze heeft waargenomen, samengevat.

---

56 Deze mogelijkheid werd ingevoerd door de zgn. BIM-Wet. Deze wet maakte het voor de VSSE en de ADIV ook mogelijk om binnenlandse communicaties af te luisteren en op te nemen (art. 18/17, § 1 W.I&V en Hoofdstuk III). Er moet een duidelijk onderscheid worden gemaakt tussen 'intercepties als bijzondere inlichtingenmethode' en de 'veiligheidsintercepties' beschreven in dit hoofdstuk, zowel wat betreft het toepassingsgebied als wat betreft de controle.

IV.1. DE WETSWIJZIGING: NIEUWE BEVOEGDHEDEN VOOR DE ADIV EN EEN VERSTERKTE CONTROLE[57]

Op 30 maart 2017 werd de Wet houdende regeling van de inlichtingen- en veiligheidsdiensten gewijzigd. Als gevolg van deze wetswijziging, die in voege trad op 8 mei 2017, breidde de bevoegdheid van de ADIV in het kader van de veiligheidsintercepties uit. De intercepties kunnen voortaan voor communicaties '*uitgezonden of ontvangen in het buitenland*'. Vóór de wetswijziging was dit beperkt tot communicaties die waren *'uitgezonden in het buitenland'*. Daarenboven geldt deze mogelijkheid vanaf mei 2017 voor *quasi* alle opdrachten van de ADIV.[58] Daarbij is het niet onbelangrijk te vermelden dat de opdrachtomschrijvingen zelf, ook werden verruimd door dezelfde wetswijziging (zie ook Hoofdstuk III.2.1).[59]

Daarnaast voert de wet twee andere methoden in, te weten de intrusie in een informaticasysteem[60] en de opname van bewegende beelden.[61]

De wijze waarop het Comité deze methoden kan controleren, wijzigde ook op sommige vlakken.

De controle *voorafgaand* aan de intercepties, intrusies of beeldopnames gebeurt op basis van jaarlijks opgestelde lijsten.[62] Dit betekent dat er naast een jaarlijks interceptieplan, nu ook een intrusie- en beeldplan dient te worden opgesteld door de ADIV. In deze plannen stelt de ADIV een lijst op van '*organisaties of instellingen die het voorwerp zullen uitmaken van interceptie van hun communicaties, intrusies in hun informaticasystemen of opnames van vaste of bewegende beelden tijdens het komende jaar. Deze lijsten verantwoorden voor iedere organisatie of instelling de reden waarom zij het voorwerp is van een interceptie, intrusie of opname van vaste of bewegende beelden in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3 en 5°, en vermelden de voorziene duur*' (art. 44/3 W.I&V). De ADIV moet die lijsten in de maand december voor toelating aan de minister van Defensie zenden. Deze heeft tien werkdagen om zijn beslissing mee te delen aan

---

57 Zie artt. 44 t.e.m. 44/5 W.I&V.

58 '*[I]n het kader van de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5 W.I&V'.*

59 Indien een ingreep op een communicatienetwerk noodzakelijk is om de interceptie van in het buitenland uitgezonden of ontvangen communicatie mogelijk te maken, kan de ADIV de medewerking van een netwerkoperator of de verstrekker van een elektronische communicatiedienst vorderen (art. 44/5 W.I&V). Ook dit is nieuw.

60 In dit kader kan de ADIV '*overgaan tot de intrusie in een informaticasysteem dat zich in het buitenland bevindt, er de beveiliging van opheffen, er technische voorzieningen in aanbrengen teneinde de door het informaticasysteem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen, te decoderen, op te slaan en te manipuleren en het informaticasysteem te verstoren en te neutraliseren*' (art. 44/1 W.I&V).

61 In dit kader kan de ADIV '*in het buitenland middelen gebruiken voor de opname van vaste of bewegende beelden*' (art. 44/2 W.I&V).

62 Dit impliceert niet dat het Vast Comité I de bevoegdheid heeft om de door de minister goedgekeurde lijst al dan niet goed te keuren.

de ADIV[63] die op zijn beurt de lijsten, voorzien van de toelating van de minister, overzendt aan het Vast Comité I.[64, 65]

Het toezicht *tijdens* de interceptie, intrusie of opname gebeurt '*op elk ogenblik door middel van bezoeken aan de installaties waar de Algemene Dienst Inlichting en Veiligheid deze intercepties, intrusies en opnames van vaste of bewegende beelden uitvoert*'.

Het toezicht *na* de uitvoering van de methode werd aanzienlijk verscherpt. Het gebeurt '*aan de hand van maandelijkse lijsten van landen of van organisaties of instellingen die effectief het onderwerp hebben uitgemaakt van een afluistering, intrusie of opname van beelden gedurende de voorafgaande maand*' en die '*de reden verantwoorden waarom de interceptie, intrusie of opname van beelden werd uitgevoerd in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°*'. Deze lijsten moeten ter kennis van het Vast Comité I worden gebracht. De *ex post*-controle gebeurt ook aan de hand van '*het nazicht van logboeken die permanent op de plaats van de interceptie, de intrusie of de opname van vaste of bewegende beelden door de Algemene Dienst Inlichting en Veiligheid worden bijgehouden*'. Deze logboeken moeten steeds toegankelijk zijn voor het Vast Comité I.

Wat kan het Vast Comité I nu ondernemen indien het een onregelmatigheid vaststelt? Artikel 44/4 W.I&V bepaalt dat het Comité, *'[o]ngeacht de andere bevoegdheden aan dit Comité toegekend op basis van de wet van 18 juli 1991, het recht [heeft] de aan de gang zijnde intercepties, intrusies of beeldopnames te doen stopzetten wanneer blijkt dat ze de wettelijke bepalingen of de [ministeriële] toelating niet respecteren. Het beveelt dat de gegevens die onwettig werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd, volgens de door de Koning te bepalen nadere regels.*'[66] Het Comité moet zijn beslissing omstandig motiveren en meedelen aan de minister en aan de ADIV.

IV.2. DE IN 2017 VERRICHTE CONTROLES

IV.2.1. HET AFLUISTERPLAN

Het Vast Comité I kreeg het door de minister gevalideerde interceptieplan pas in juli 2017.[67] Het Comité formuleerde daarbij een aantal opmerkingen. De belang-

63 Indien de minister geen beslissing heeft genomen of deze niet heeft meegedeeld aan de ADIV vóór 1 januari, mogen de voorziene intercepties, intrusies en opnames aanvangen, onverminderd iedere latere beslissing van de minister.

64 Voor intercepties, intrusies of opnames die niet opgenomen zijn in de jaarlijkse lijsten, maar die '*onontbeerlijk en dringend blijken te zijn*', wordt de minister zo spoedig mogelijk en uiterlijk op de eerste werkdag die volgt op de aanvang van de methode ingelicht. Indien de minister niet akkoord gaat, kan hij deze methode laten stopzetten. Deze beslissing wordt door de ADIV zo spoedig mogelijk meegedeeld aan het Vast Comité I.

65 Het eerste beeld- en intrusieplan werd pas in de loop van 2018 aan het Comité bezorgd.

66 Er werd nog geen dergelijk KB getroffen.

67 Ook de voorgaande jaren werd de lijst met vertraging aan het Comité bezorgd.

rijkste betroffen de verschillen in prioriteit tussen enerzijds het Inlichtingenstuurplan[68] en anderzijds de voorgenomen SIGINT-intercepties en het feit dat de omschrijving van de organisaties en instellingen die het voorwerp zullen uitmaken van intercepties, te algemeen was.

IV.2.2. JAARLIJKSE INSPECTIE

Eind 2017 bracht het Vast Comité I een werkbezoek aan de SIGINT-installaties van de ADIV om, ondermeer, de overeenstemming van het logboek met de wet en de betreffende richtlijnen aan een toezicht te onderwerpen. Het Comité nam daarbij deel aan een coördinatievergadering van de SIGINT-afdeling.

Het Vast Comité I kon vaststellen dat de ADIV ten gevolge de in 2016 geformuleerde opmerkingen een nieuw logboek hanteerde. Er werden geen onregelmatigheden vastgesteld in dit nieuwe logboek, dat conform was met de ter zake geldende voorschriften.

IV.2.3. MOU MET EEN BUITENLANDSE PARTNER

Het Vast Comité I werd op de hoogte gebracht van de ondertekening van een *Memorandum of Understanding* (MoU) met een buitenlandse partner over een gemeenschappelijke interceptiecapaciteit.

Het Comité vond in verband met de werking van de MoU geen aanwijzingen van elementen die indruisen tegen de wet. Wel moest er worden vastgesteld dat, omwille van personeelsgebrek, de exploitatie van de geïntercepteerde gegevens nog niet kon worden uitgevoerd.

IV.2.4. RESULTATEN EN EVOLUTIES

Naar aanleiding van de jaarlijkse inspectie van de SIGINT-installaties van de ADIV, kon het Vast Comité I zich een beeld vormen van de realisaties van de betrokken afdeling. Het Comité werd eveneens geïnformeerd over de lopende projecten op technisch vlak[69], in verband met de aanwerving van vertalers[70],

---

68 Een plan opgesteld door de Directie I met daarin de op te volgen landen en de prioritisering.

69 Naar aanleiding van het verhoogde aantal terrorismedossiers en de noodzaak om sneller ruwe informatie uit te kunnen wisselen met de VSSE, bracht de ADIV bijvoorbeeld een beveiligde lijn tot stand met de VSSE.

70 De SIGINT-afdeling kampt nog steeds met vertaalcapaciteitsproblemen. Het Comité uitte reeds in het *Activiteitenverslag 2016* zijn bezorgdheid omtrent het gebrek aan gekwalificeerde vertalers. Het diende vast te stellen dat het aantal vertalers opnieuw was afgenomen. De SIGINT-afdeling werkt hard aan de rekrutering van nieuwe medewerkers, maar botst op de weigering van DG Human Resources om kandidaten vrij te geven. Het gebrek aan vertalers in

op vlak van procedures[71] en in verband met de aanwending van de middelen.[72]

Het Vast Comité I nam zich voor om in 2018 nog meer te investeren in de opvolging van deze wijze van collecte, die een steeds belangrijkere plaats inneemt in de internationale informatieuitwisseling is. Bijzondere aandacht zal worden besteed aan de nieuwe bevoegdheden van de ADIV (de opname van beelden en intrusies in IT-systemen) en de uitbreiding van de interceptiedoeleinden, aan de structurele samenwerking met de partners en aan de nadere omschrijving in de diverse plannen van de 'targets'.

---

de schoot van deze afdeling maakt het SIGINT-proces veel minder rendabel aangezien de intercepties niet kunnen worden vertaald en dus ook inhoudelijk niet kunnen worden gebruikt. Hoewel het niet steeds noodzakelijk is om over een vertaler te kunnen beschikken bij de exploitatie van een interceptie, wordt het risico om een informatie te 'missen' hoog ingeschat.

71 Zo werkt de afdeling SIGINT verder aan de inwerkingstelling van de 'projectfiches' waarmee twee jaar geleden een aanvang werd genomen. Het Comité kon vaststellen dat de leiding van de afdeling van deze fiches gebruik maakt in zijn besluitvormingsproces. Dat proces was al geëvolueerd in de zin dat er sprake was van een symbiose tussen de collecte en de analyse. Het is evenwel noodzakelijk om nog verder te gaan in de richting van een *analyse driven collection*. In deze fiches worden de te intercepteren organisaties en instellingen veel nader omschreven dan in het interceptieplan, bijvoorbeeld aan de hand van selectoren. Op die wijze sluiten de fiches beter aan bij de wettelijke vereiste om een gemotiveerde lijst van instellingen en organisaties op te stellen. Naar het oordeel van het Comité moeten de actuele lijsten meer gedetailleerd worden. De ADIV-SIGINT beloofde vooruitgang te boeken op dat vlak, maar ze stelde dat ze niet in staat is om exhaustieve lijsten van targets aan te leveren.

72 Opdat bijvoorbeeld personen die in het kader van hun functie zouden kunnen beschikken over SIGINT-data, wordt gewerkt aan de implementatie van een nieuwe technologie die een ruimere toegang moet verlenen tot bepaalde gegevensbanken.

HOOFDSTUK V
OPDRACHTEN VOOR PARLEMENTAIRE ONDERZOEKSCOMMISSIES

Sinds 1996[73] kan een parlementaire onderzoekscommissie het Vast Comité I inschakelen in haar onderzoeken. Dit gebeurde in het kader van een globale hervorming (lees: uitbreiding[74]) van de mogelijkheden van parlementaire onderzoeken. Van de mogelijkheid om het Comité in te schakelen, werd voor het eerst in 2016 gebruik gemaakt: zowel de parlementaire onderzoekscommissie belast met het onderzoek naar de terroristische aanslagen als deze naar de minnelijke schikking in strafzaken, belastten het Comité met diverse opdrachten. Ook in 2017 kreeg het Comité diverse onderzoeksopdrachten toegewezen door deze twee commissies.

V.1. DE PARLEMENTAIRE ONDERZOEKSCOMMISSIE NAAR DE AANSLAGEN

In maart 2016 werd België opgeschrikt door zware terroristische aanslagen. Half april 2016 volgde de oprichting van de parlementaire onderzoekscommissie 'belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging'.[75] Deze commis-

73 Wet van 30 juni 1996 tot wijziging van de Wet van 3 mei 1880 op het parlementair onderzoek en van artikel 458 van het Strafwetboek, *BS* 16 juli 1996 (*in casu* art. 4 § 3 dat stelt '*De commissie kan eveneens, overeenkomstig de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten, aan de Vaste Comités P en I opdracht geven om de nodige onderzoeken te doen*'). Zie W. VAN LAETHEM, 'De Wetsgeschiedenis van 1991 tot 2013' in VAN LAETHEM, W. en VANDERBORGHT, J. (eds.), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, Antwerpen, Intersentia, 2013, 55.

74 Het luidt thans dat de commissie '*alle in het Wetboek van strafvordering omschreven onderzoeksmaatregelen kan nemen*'. Een parlementaire onderzoekscommissie kan dus een onderzoek ter plaatse verrichten, getuigen verhoren, confrontaties organiseren, deskundigen aanstellen of telefonische mededelingen (laten) opsporen. Ook kan zij laten overgaan tot huiszoekingen en inbeslagnames, en kan ze dus onderzoeksopdrachten geven aan de Vaste Comités I en P.

75 *Parl. St.* Kamer 2016-17, 54K1752/001.

sie werd ingesteld '*om na te gaan of België zich middelen heeft verschaft om radicalisme en terrorisme doeltreffend te bestrijden, om te onderzoeken of het land beschikt over diensten die in staat zijn de veiligheid van de burgers te waarborgen en om aanbevelingen te formuleren waarmee die diensten kunnen worden verbeterd*'. Halfweg juni 2017 legde de Commissie haar omvangrijke 'Derde tussentijds verslag over het onderdeel veiligheidsarchitectuur' neer.[76]

Voor de realisatie van haar verslag schakelde de commissie in 2016 het Vast Comité I diverse malen in.[77] In 2017 concentreerde de onderzoeksopdrachten voor het Comité zich rond drie thema's: de informatiepositie van de inlichtingendiensten over één van de protagonisten van de aanslagen, Oussama Atar[78]; de financiering van de Grote Moskee in Brussel; en ten slotte, de stand van zaken in het kader van het 'Actieplan radicalisering in gevangenissen'.

Midden december 2016 wenste de Commissievoorzitter van de VSSE[79] informatie betreffende Oussama Atar: er werd opgevraagd over welke informatie de inlichtingendienst beschikte na diens eerste reis naar Syrië, welke contacten hij onderhield en of er hieromtrent informatie werd gedeeld met de FOD Buitenlandse Zaken. Gezien het lopende gerechtelijk onderzoek en het feit dat aspecten van de bekomen informatie afkomstig waren van menselijke bronnen en/of partnerdiensten, verwerkte het Comité de informatie in een geclassificeerd rapport. De nota lag ter inzage voor de expert van de onderzoekscommissie die over een veiligheidsmachtiging beschikte. Ten behoeve van de Commissieleden werd een gedeclassificeerd rapport opgesteld.

Na hoorzittingen met de imam van de Grote Moskee in Brussel en de directeur van het Islamitisch Cultureel Centrum van België (ICCB), verzocht de voorzitter van de parlementaire onderzoekscommissie in maart 2017 het Vast Comité I tevens om enkele andere verduidelijkingen: de commissie wenste te weten of er *foreign terrorist fighters* (FTF) opleidingen volgden die werden georganiseerd door de Grote Moskee en of de Veiligheid van de Staat over informatie beschikte met betrekking tot de financiële stromen tussen het ICCB en Saoedi-Arabië. Het Comité bevroeg hiertoe zowel de VSSE als het OCAD.[80] De VSSE concludeerde dat het onderzoek van de rekeningen van het ICCB geen enkel bewijs leverde van rechtstreekse financiering van een terroristische organisatie door het centrum. Daarentegen speelde het ICCB een belangrijke rol in de financiering van individuen en entiteiten, actief in de propaganda van de salafistische-wahhabistische

76 *Parl. St.* Kamer 2016-17, 54K1752/008, 567 p.

77 Hierover: VAST COMITÉ I, *Activiteitenverslag 2016* ('Hoofdstuk V. Opdrachten voor parlementaire onderzoekscommissies'), 113-124.

78 In de marge werd ook onderzoek verricht naar de aanwezigheid van informatie bij de VSSE over een voormalig Mechels politie-inspecteur.

79 Het Comité bevroeg hierover ook de ADIV. Uit een eerste reactie bleek dat de militaire inlichtingendienst over geen informatie omtrent betrokkene beschikte. Het Comité kon achteraf aantonen dat er wel informatie over Atar aanwezig was binnen de ADIV.

80 Voor een antwoord op deze vraag werd door de voorzitter van de onderzoekscommissie tevens gesuggereerd een beroep te doen op de Cel voor Financiële Informatieverwerking (CFI).

ideologie op Belgisch grondgebied. Het antwoord op de vraag of er FTF'ers opleiding volgden in de Grote Moskee van Brussel, was voorwerp van een geclassificeerd verslag.

In juli 2017 ten slotte, werd de minister van Justitie door de onderzoekscommissie gevraagd een stand van zaken te geven over de uitvoering van het Actieplan inzake de aanpak van radicalisering in de gevangenissen (maart 2015).[81] Immers, het is bekend dat gevangenissen een voedingsbodem vormen voor radicaal gedachtengoed omwille van de setting, het gemis aan perspectief, de mentale toestand van de gevangenen, verveling… In de Belgische gevangenissen worden bijna uitsluitend gevallen van religieuze (islam-)radicalisering en extremisme waargenomen. Sinds midden 2014 schenkt de VSSE specifieke aandacht aan dit fenomeen. De dienst richtte een omstandig, geclassificeerd antwoord over de uitvoering van het Actieplan aan het Vast Comité I, dat op zijn beurt de informatie ter inzage voorlegde aan de expert van de commissie.

De parlementaire onderzoekscommissie finaliseerde haar eindverslag in oktober 2017.[82] De oprichting van een zogenaamde 'opvolgingscommissie' die de uitvoering van de aanbevelingen controleert, werd hierin aanbevolen.

V.2. DE PARLEMENTAIRE ONDERZOEKS-COMMISSIE NAAR DE WET MINNELIJKE SCHIKKING

V.2.1. VOORAFGAAND

Begin december 2016 werd in de plenaire vergadering van de Kamer de tekst aangenomen met daarin het voorstel tot instelling van een tweede parlementaire onderzoekscommissie.[83] De totstandkoming van de verruimde minnelijke schikking in strafzaken bij Wet van 14 april 2011 stond daarbij centraal. Immers, na berichten in de media rezen grote vragen bij de snelheid waarmee een wetsvoorstel hierover in 2011 groen licht kreeg in het Parlement. Daarbij zou intensief lobbywerk verricht zijn om spoed achter de behandeling te zetten. Het Franse weekblad *Le Canard Enchaîné* beweerde dat Kazachse autoriteiten als voorwaarde voor de bestelling van Franse helikopters geëist zouden hebben dat de Franse

81 De finaliteit van het plan is tweeledig: enerzijds vermijden dat gedetineerden geradicaliseerd worden tijdens hun verblijf in de gevangenis en anderzijds het uitwerken van een gespecialiseerde omkadering van geradicaliseerde personen tijdens hun detentie.

82 *Parl. St.* Kamer 2017-18, 54K1752/010.

83 Voorstel tot instelling van een parlementaire onderzoekscommissie die ermee wordt belast onderzoek te voeren naar de omstandigheden die hebben geleid tot de aanneming en de toepassing van de wet van 14 april 2011 houdende diverse bepalingen, voor wat de minnelijke schikking in strafzaken betreft (*Parl. St.* Kamer 2016-17, 54K2179/006). De Commissie finaliseerde haar eindrapport op 16 april 2018 (*Parl. St.* Kamer 2017-18, 54K2179/007).

overheid het nodige zou doen om de vervolging in België tegen een zogenaamd 'Kazachs trio'[84], te beëindigen. Daarvoor zou de hulp zijn ingeroepen van een op dat ogenblik Belgische Senator en lid van de Parlementaire Assemblée van de Raad van Europa.

De zaak kwam al aan het licht in 2012 en leidde tot het openen van een onderzoek door de Franse gerechtelijke instanties. In februari 2015 volgden opnieuw onthullingen waardoor een grondig onderzoek naar de politieke en financiële, individuele en diplomatieke, nationale en buitenlandse interventies, druk en beïnvloeding die hebben geleid tot de totstandkoming van deze 'afkoopwet', zich opdrong.

De onderzoekscommissie verdeelde haar werkzaamheden in drie luiken: 'Luik I. Naturalisatie en nationaliteitsverwerking'; 'Luik II. Totstandkoming van de Wet van 14 april 2011 houdende diverse bepalingen, voor wat de minnelijke schikking in strafzaken betreft'[85]; en ten slotte 'Luik III. Toepassing van de Wet verruimde minnelijke schikking in strafzaken tot de inwerkingtreding van de Reparatiewet van 11 juli 2011'.[86]

Half december 2016 richtte de Voorzitter van het Vast Comité I een schrijven aan de Commissievoorzitter waarin hij meldde dat het Comité over documenten beschikte met betrekking tot de naturalisatie van in het dossier vernoemde personen. Deze documenten waren in hoofdzaak afkomstig van de Veiligheid van de Staat (VSSE) – dewelke een adviesbevoegdheid heeft in het kader van naturalisaties – en afkomstig uit eerder afgesloten toezichtonderzoek (Tractebel, zie verder).

In 2017 werd het Vast Comité I[87] intensief ingeschakeld en kreeg het verschillende onderzoeksopdrachten van de parlementaire onderzoekscommissie. De werkzaamheden van het Vast Comité I voor de commissie waren divers: het toezenden van onderzoeksverslagen, het opstellen van diverse rapporten, het fungeren als doorgeefluik voor geclassificeerde informatie door ze te 'zuiveren' van de meeste gevoelige informatie en het horen als getuige.

V.2.2. TOEZENDEN VAN EERDERE ONDERZOEKSVERSLAGEN

Het Vast Comité I had in het verleden toezichtonderzoeken gevoerd die rechtstreeks of onrechtstreeks van belang konden zijn voor de parlementaire onderzoekscommissie. Het betrof het onderzoek naar 'De werking van de inlichtingen-

84 Het betreft drie uit Centraal-Azië afkomstige zakenpartners die zich begin jaren '90 in België vestigden om vennootschappen op te richten.

85 Hieraan werd een Luik II(bis) toegevoegd: 'Ontstaan van het advocatenteam […] in opdracht van het Elysée'.

86 Artikel 1 § 1, derde lid van het oprichtingsbesluit (*Parl. St.* Kamer 2016-17, nr. 54K2179/006).

87 Ook het Vast Comité P kreeg in het kader van Luik I een onderzoeksopdracht toevertrouwd (verslag 30875/2017).

diensten bij het beheer van eventuele gegevens in de context voorafgaand aan het afsluiten van een internationale commerciële overeenkomst' (2000)[88], een rapport over de wijze waarop de VSSE zich van haar nieuwe opdracht tot bescherming van het wetenschappelijk en economisch potentieel kwijt[89] alsook het onderzoek naar 'De rol van de VSSE in het kader van procedures tot het verkrijgen van de Belgische nationaliteit.'[90]

V.2.3. 'FILTER' VOOR DE RAADPLEGING VAN GECLASSIFICEERDE DOCUMENTEN

Op grond van haar taak en de omvang van haar bevoegdheden, oordeelde de parlementaire onderzoekscommissie het nuttig om inzage te krijgen in documenten met geclassificeerde inlichtingen, ongeacht of het ging om dossiers over gerechtelijke onderzoeken dan wel informatie in handen van instanties waarvan het werk in essentie geheim is (zoals de Veiligheid van de Staat, de ADIV).

Wat de inzage in geclassificeerde informatie van de Veiligheid van de Staat betrof[91], diende een *modus vivendi* te worden gezocht aangezien de Commissieleden niet over de vereiste veiligheidsmachtiging beschikten.[92] Er werd besloten dat de geclassificeerde informatie door het Vast Comité I zou worden bestudeerd en dat het – in samenspraak met de inlichtingendiensten – zou beslissen welke informatie kon doorgegeven worden. Immers, in tegenstelling tot de parlementaire onderzoekscommissie naar de terroristische aanslagen, kon de Commissie daarvoor niet rekenen op de hulp van haar deskundigen; deze waren geen houder van een veiligheidsmachtiging.

Dit resulteerde in tien rapporten, verspreid over de periode van januari tot september 2017.[93] Diverse thema's kwamen daarbij aan bod. Zo kon onder meer een toelichting worden gegeven bij de rol van de VSSE in het kader van de naturalisatie- en nationaliteitsverwerving van het Kazaakse trio en de (toenmalige) aandacht van de inlichtingendienst voor de toekenning van arbeidsvergunningen. Ook wer-

88 Over het toezichtonderzoek werd tweemaal kort gerapporteerd (VAST COMITÉ I, *Activiteitenverslag 2001*, 6-8 en *Activiteitenverslag 2000*, 116-155). Het werd omwille van andere prioriteiten nooit afgerond.

89 VAST COMITÉ I, *Activiteitenverslag 2003*, 24-124.

90 Hierover: VAST COMITÉ I, *Activiteitenverslag 2012*, 5-14.

91 Het Comité kreeg hiertoe van de VSSE meerdere, bijzonder uitvoerige (geclassificeerde) documentatiebundels ter beschikking alsook punctuele antwoorden op de door het Comité geformuleerde onderzoeksvragen.

92 De Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen stelt immers dat *'niemand toegang heeft tot geclassificeerde informatie, documenten […] tenzij hij houder is van een overeenstemmende veiligheidsmachtiging en voor zover de kennisname en de toegang noodzakelijk zijn voor de uitoefening van zijn functie of zijn opdracht […]*' (art. 8 W.C&VM).

93 De rapporten – in versie 'Beperkte verspreiding – werden telkenmale voorgelegd aan de VSSE met verzoek tot maximale declassificatie van de erin opgenomen stukken.

den de werkzaamheden van de VSSE in de periode voor, tijdens en na de totstandkoming van de Wet verruimde minnelijke schikking beschreven, waaronder onder meer de aandacht van de dienst voor de toenemende aanwezigheid van zakenlui en politici vanuit Kazachstan. Er werd stilgestaan bij het bezoek van een toenmalig ondervoorzitter van de Senaat, in Parijs voor een ontmoeting met een van de adjuncten van de nationaal coördinator van de Franse inlichtingendiensten en waarbij een geclassificeerd document (de zgn 'fiche V', *infra*) zou zijn overhandigd.[94] Tevens werd de zaak onderzocht waarbij voornoemde Senator zich, bij zijn zoektocht naar zijn gsm-toestel, veroorloofde de voormalige Administrateur-generaal van de VSSE te benaderen met het verzoek bevel te geven een bijzondere inlichtingenmethode in te zetten. In een ander rapport werd ook de uitvoerig in de documentatiebestanden van de VSSE opgenomen Eric V. – een zakenman met een gerechtelijke verleden die in contact kwam met het Kazachse trio – beschreven. Waar nuttig, werd de Commissie door het Vast Comité I geïnformeerd over wat in de pers verscheen naar aanleiding van de diverse getuigenissen.[95]

Ook de ADIV werd – zij het in de marge – betrokken in de onderzoek. Het Comité ging na of de ADIV voorafgaand aan het afsluiten in oktober 2010 van een Memorandum of Understanding (MoU) tussen het Belgisch Studiecentrum voor Kernenergie, het Nationale Centrum voor Kernenergie van Kazachstan en Kazatomprom op de hoogte was van de ontwikkelingen in deze en of de namen van het Kazachse trio hierin werden genoemd.

V.2.4. GETUIGENIS(SEN) VOOR DE ONDERZOEKSCOMMISSIE

De Voorzitter van het Vast Comité I werd vijfmaal gehoord.[96] Bij de bespreking van de onderzoeksrapporten werd in openbare zitting vergaderd, tenzij de Voorzitter – omwille van het zeer gevoelige karakter ervan, niet alleen wat betreft de feiten en de weergegeven gebeurtenissen, maar ook wat betreft de geciteerde personen – de onderzoekscommissie verzocht achter gesloten deuren te vergaderen.[97]

---

94 In dat kader werd gereflecteerd over de toepassing door de VSSE van art. 29 Sv. dan wel art. 19 W.I&V en wat met de beschikbare informatie aangaande het parlementslid diende te gebeuren.

95 Bijvoorbeeld over een donatie van de Orde van Malta aan het liefdadigheidsfonds (Fonds d'Entraide Prince et Princesse Alexandre de Belgique) en 'la Compagnie des Mousquetaires d'Armagnac' of het optreden van een advocate in de naturalisatiedossiers en met betrekking tot de contacten van het Kazachse trio met het management van Tractebel.

96 Op 25 januari 2017, 15 februari 2017 (deels achter gesloten deuren), 29 maart 2017 (deels achter gesloten deuren), 24 april 2017 (achter gesloten deuren) en op 7 juni 2017 (achter gesloten deuren). Ook gewezen voorzitter Jean-Claude Delepière en gewezen raadsheer Walter De Smedt van het Vast Comité I werden door de commissie gehoord.

97 De Voorzitter diende herhaaldelijk de vigerende wetgeving inzake classificatie toe te lichten. De onderzoekscommissie op haar beurt overwoog klacht in te dienen bij het Parket van Brussel nadat herhaaldelijk informatie was gelekt naar de media.

De Voorzitter bracht verslag uit over de naturalisatie van de protagonisten en aanverwante dossiers, waarbij werd stilgestaan bij het optreden van de VSSE in deze naturalisatiedossiers. In tweede instantie werd het verslag over de nationaliteitsverwerving van deze protagonisten besproken, alsook de interne werking van het Vast Comité I en werd het dossier Tractebel aangekaart. De bespreking over de informatie van de VSSE over de activiteiten en contacten in de periode 2010-2011 van personen die het voorwerp uitmaakten van het onderzoek van de commissie en de mogelijke beïnvloeding vanuit Frankrijk op het totstandkomen van de Wet verruimde minnelijke schikking in strafzaken (Luik II), vond plaats achter gesloten deuren. Tijdens een vierde hoorzitting werden enkele gedclassificeerde inlichtingen van de VSSE toegelicht over de protagonisten voor de periode februari-maart 2011. Ten slotte werd toelichting gegeven over een onderzoek dat op verzoek van de commissie werd uitgevoerd met betrekking tot een gewezen Administrateur-generaal van de VSSE. In het verlengde hiervan werd deze laatste, op diens verzoek in openbare vergadering, gehoord over de bevindingen van het Vast Comité I over zijn contacten met voornoemde Senator en over zijn contacten met een Franse inlichtingendienst.

V.2.5. HET UITVOEREN VAN BIJKOMENDE ONDERZOEKSOPDRACHTEN

Op verzoek van de Voorzitter van de parlementaire onderzoekscommissie boog het Vast Comité I zich over een anonieme klacht gericht aan een Volksvertegenwoordiger.[98] De niet-gedateerde brief behandelde twee thema's: de neutralisatie en intimidatie van sommige medewerkers van de inlichtingendienst alsook de inmenging in de schoot van de VSSE van prominenten van een politieke partij. Het Comité vond – buiten het bestaan van een interpersoonlijk conflict tussen twee leden van de Veiligheid van de Staat – geen elementen die de aangehaalde feiten in de brief konden staven.

Ten slotte was ook de informatiedoorstroming tussen de Vaste Comités I en P, de relatie tussen toezichtonderzoeken en lopende gerechtelijke onderzoeken en de wijze van afsluiten van toezichtonderzoeken, aan de orde.

98 De anonieme klacht was getiteld '*Kazakhgate: ce que la Sûreté ne veut pas dire à la commission parlementaire*'.

HOOFDSTUK VI

DE CONTROLE VAN GEMEENSCHAPPELIJKE GEGEVENSBANKEN

in de nadagen van de aanslagen in Brussel, wijzigde de Wet van 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme[99] de Wet van 5 augustus 1992 op het politieambt (WPA). Daarmee werd een wettelijke basis gecreëerd voor de oprichting van gemeenschappelijke gegevensbanken.

Artikel 44/6 WPA vertrouwt de controle op de verwerking van de informatie en van de in de gemeenschappelijke gegevensbank vervatte persoonsgegevens gezamenlijk toe aan het Controleorgaan op de politionele informatie (COC) en aan het Vast Comité I. Tevens dienen beide instanties voorafgaand aan de oprichting van een gemeenschappelijke databank gezamenlijk advies te verlenen op basis van een 'voorafgaandelijke aangifte' die wordt ingediend verantwoordelijken voor de verwerking (de ministers van Binnenlandse Zaken en Justitie). Met het oog op een gecoördineerde uitoefening van deze twee bevoegdheden sloten beide instellingen in december 2017 een protocolakkoord.

VI.1. DE GEGEVENSBANK *FOREIGN TERRORIST FIGHTERS* KORT SAMENGEVAT[100]

Zich baserend op deze nieuwe mogelijkheid die de wetgever aanbood, hebben de ministers van Binnenlandse Zaken en Justitie de gemeenschappelijke gegevensbank *foreign terrorist fighters* opgericht.[101]

De gegevensbank bestaat uit inlichtingenfiches van personen gelieerd aan het fenomeen van strijders die afreizen naar jihadistische strijdzones. Deze fiches moeten het mogelijk maken om de potentiële dreiging te beoordelen die deze personen

99 *BS* 9 mei 2016.

100 Voor een gedetailleerde bespreking, zie VAST COMITÉ I, *Activiteitenrapport 2016*, 127-139 (www.comiteri.be).

101 KB van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'het informatiebeheer' van hoofdstuk IV van de wet op het politieambt, *BS* 22 september 2016.

vertonen, maar voornamelijk er een opvolging van te verzekeren met het oog op het anticiperen en het verhinderen van mogelijke terroristische acties door hen.[102]

De fiches worden *up-to-date* gehouden door de 'basisdiensten' (het OCAD, de geïntegreerde politie, de inlichtingen- en veiligheidsdiensten) en de 'partnerdiensten'.[103] De verschillende diensten die rechtstreeks toegang hebben tot de gegevensbank, hebben de verplichting deze permanent te voeden; in die zin wordt de gegevensbank dan ook bestempeld als zijnde 'dynamisch'.

De inlichtingenfiches bevatten alle niet-geclassificeerde persoonsgegevens en informatie[104] over de betrokkenen.

Er worden alleen inlichtingenfiches opgesteld van personen die in België verblijven of verbleven hebben, die al dan niet de Belgische nationaliteit bezitten en die zich, met het oog om zich bij terroristische groeperingen aan te sluiten of deze actief of passief steun te verlenen, in een van de volgende situaties (categorieën) bevinden (art. 6 § 1, 1° KB FTF):

- ze zijn naar een jihadistische conflictzone afgereisd (categorie 1);
- ze hebben België verlaten om naar een jihadistische conflictzone af te reizen (categorie 2);
- ze zijn naar België onderweg of naar België teruggekeerd na afgereisd te zijn naar een jihadistische conflictzone (categorie 3);
- ze werden (gewild of ongewild) verhinderd om naar een jihadistische conflictzone af te reizen (categorie 4);
- ze hebben de intentie om naar een jihadistische conflictzone af te reizen (op voorwaarde dat deze intentie aangetoond wordt door ernstige aanwijzingen) (categorie 5);

OF

- er bestaan ernstige aanwijzingen dat zij een van bovenstaande criteria kunnen vervullen (art. 6 § 1, 2° KB FTF).

Naast de inlichtingenfiches worden ook 'informatiekaarten' aangemaakt die bedoeld zijn voor instanties die geen toegang hebben tot de fiches. De kaart vormt een uittreksel van de inlichtingenfiche en bevat persoonsgegevens en informatie die strikt beperkt zijn tot informatie die de bestemmeling nodig heeft. Alleen de basisdiensten zijn bevoegd om de informatiekaarten door te zenden.

---

102 Uittreksel uit het Verslag aan de Koning (*BS* 22 september 2016, 63970).

103 Sommige partnerdiensten (het Directoraat-generaal penitentiaire instellingen en de penitentiaire instellingen, het Openbaar Ministerie, de Cel voor Financiële Informatieverwerking en de Dienst Vreemdelingenzaken) beschikken, net als de basisdiensten, over een rechtstreekse toegang. Andere partnerdiensten (de Algemene Directie Crisiscentrum, de Algemene Directie Veiligheid en Preventie, de Directie-generaal Consulaire zaken van de FOD Buitenlandse Zaken en de onderzoeks- en opsporingsdiensten van de Algemene Administratie der douane en accijnzen), kunnen toegang verkrijgen op basis van rechtstreekse bevraging (een soort *hit/no hit* principe).

104 Identificatiegegevens, gerechtelijke of administratieve gegevens, gegevens van bestuurlijke politie en niet-geclassificeerde toereikende, ter zake dienend en niet-overmatige inlichtingengegevens.

VI.2. DE TOEZICHTSOPDRACHT

VI.2.1. HET VOORWERP VAN TOEZICHT

In het kader van hun gemeenschappelijke controleopdracht beslisten het COC en het Vast Comité I in 2017 onderstaande elementen te onderzoeken:
- de inhoud van de inlichtingenfiche en de informatiekaart van elke FTF op basis van wettelijke en reglementaire parameters;
- de controle van de acties van het OCAD voor wat betreft de initiële validering als FTF alsook de verdere verwerkingen;
- de controle van de raadplegingen van de inlichtingenfiches en de informatiekaarten door de basisdiensten en de partnerdiensten;
- de controle van de manier waarop de burgemeesters worden ingelicht over de informatiekaart (dit kan meerdere burgemeesters per entiteit betreffen);
- de identificatie van gebruikers van de gemeenschappelijke gegevensbank FTF, hun aantal keer rechtstreekse toegangen/rechtstreekse bevragingen, de uitoefening (of niet) van een controle naar de rechtmatigheid van de rechtstreekse toegangen/rechtstreekse bevragingen, het (al dan niet) bestaan van een validatiesysteem en het bestaan van eventuele veiligheidsincidenten;
- het bestaan van een actualisering van de gebruiksaanwijzing van de gegevensbank;
- een onderzoek van de verwerkingen van twee geselecteerde dagen;
- de aanstelling van een consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer.

VI.2.2. UITGEVOERDE CONTROLES EN VASTSTELLINGEN

VI.2.2.1. Wat betreft het Coördinatieorgaan voor de dreigingsanalyse

Gelet op de centrale rol die het OCAD vervult als verantwoordelijke voor de verwerking van de gegevensbank FTF[105], drong zich wat betreft het OCAD een prioritaire controle op.[106]

---

105 Art. 44/11/3*bis* WPA kent het OCAD volgende opdrachten toe: het controleren van de kwaliteit en het zich verzekeren van de relevantie van de verwerkte gegevens, het organiseren van de passende samenwerking en het respect voor de vooropgestelde doeleinden. Art. 4 KB FTF kent het OCAD daarnaast enkele speficieke opdrachten toe: de beoordeling van de gegevens van de inlichtingenfiche, de validering van de registratie van personen als FTF, als contactpunt fungeren voor de ministers van Binnenlandse Zaken en Justitie en het informeren van de dienst die de gegevensbank voedt wanneer het OCAD oordeelt dat de doorgezonden gegevens niet langer toereikend, ter zake dienend en niet overmatig zijn.

106 Er werden verschillende vergaderingen georganiseerd met het OCAD. Het COC en het Vast Comité I kregen van het OCAD alle gevraagde documenten (fiches en kaarten) toegestuurd. Ook werd de dienst schriftelijke vragenlijsten bezorgd.

VI.2.2.1.1. Een soms moeilijk operationeel beheer

Op het moment van de controle voerde het OCAD een dubbele registratie uit.

De eerste registratie gebeurde in de (geclassificeerde) gegevensbank van het OCAD zelf. Alle (al dan niet geclassificeerde) informatie over een entiteit werd daarin opgenomen en diende om deze te evalueren. Daarvoor werden de elementen '*à charge*' en '*à decharge*' in aanmerking genomen in een voorbereidende werkfiche. Vervolgens vond een tweede registratie plaats van de niet-geclassificeerde en niet aan embargo onderworpen informatie (te weten het belangrijkste deel van de ontvangen informatie) in de gegevensbank FTF. Het is aangaande deze tweede registratie dat het OCAD kloeg over tijdverlies.

Ondertussen kwam een technische oplossing tot stand, dewelke in de loop van 2018 zou worden gerealiseerd.

VI.2.2.1.2. De kwaliteitscontrole door OCAD

Het COC en het Vast Comité I konden vaststellen dat het OCAD toeziet op de kwaliteit van de gegevens die opgenomen zijn in de geanalyseerde dossierfiches en ook op de relevantie ervan ten aanzien van de wettelijke doeleinden. Zo heeft OCAD al herhaalde keren een bepaalde dienst erover ingelicht dat de geleverde informatie met het oog op een registratie in de gemeenschappelijke gegevensbank FTF niet ter zake dienend was.

Het OCAD stelde een nota op over de kwaliteitscontrole op de gegevensverwerking in de gemeenschappelijke gegevensbank. Er werd begin 2017 een 'kwaliteitsteam' ('*team Q*') binnen het OCAD opgericht. Dit team is belast met de kwaliteitscontrole en het uitwerken van richtlijnen voor de verwerking van gegevens. De analyse richt zich op de kwaliteit van de registratie van de basisgegevens, de verificatie van de codering van het dreigingsniveau, de controle op het bestaan van een gegevensbeoordeling en de motivatie van deze beoordeling. Ook de juistheid van de codering van bepaalde data maken het voorwerp uit van controle. De redactie van de fiche (en de motivatie) werden eveneens geanalyseerd voor wat betreft de naleving van de verschillende classificatiegraden.

Het COC en het Vast Comité I werden op de hoogte gebracht van de resultaten van de maanden mei, juni en oktober (2017). Uit de overhandigde documenten bleek dat de vastgestelde tekortkomingen een gepaste opvolging kregen (bijkomende briefing, ondervraging van de houder van de fiche, communicaties via e-mail naar de titularissen…).[107]

Het COC en het Vast Comité I waren van oordeel dat de uitvoering (en de documentatie) van de 'kwaliteitscontroles' aantoonden dat het OCAD zijn rol van operationeel verantwoordelijke van de gegevensbank FTF uiterst nauwkeurig

[107] De in sommige fiches vastgestelde tekortkomingen betroffen de evaluatie van de gegevens of de motivatie ervan. Ook bleken sommige data van de (laatste) bijwerkingen niet ingevuld.

vervulde. Het COC en het Vast Comité I moedigden het OCAD aan om deze controles verder te zetten, ze te documenteren en, vanzelfsprekend, op het gepaste niveau de nodige conclusies te trekken.

VI.2.2.1.3. Een willekeurige controle door het COC en het Vast Comité I

Op de op dat ogenblik 619 in de databank FTF opgenomen entiteiten werd een willekeurige steekproef getrokken. Het COC en het Vast Comité I konden vaststellen dat de inhoud van de inlichtingenfiches en de informatiekaarten van de betrokken dossiers overeenkwam met de wettelijke en reglementaire bepalingen.

De informatie die in deze inlichtingenfiches voorkwam werd gevoed en verrijkt door verschillende diensten (niet enkel de politie en VSSE, maar bijvoorbeeld ook het Directoraat-generaal Penitentiaire Instellingen), wat een meerwaarde betekende en op die manier beantwoordde aan de finaliteit van de gemeenschappelijke gegevensbank.

Het COC en het Vast Comité I konden op basis van de voorgelegde en geanalyseerde FTF-inlichtingenfiches en -informatiekaarten vaststellen dat het OCAD blijk gaf van een professionele en ernstige aanpak bij het beoordelen van de informatie die zij ontvingen.

Het onderzoek leverde overigens geen enkel spoor op informatie die overeenkomstig een embargo of wettelijke classificatie niet opgenomen had mogen worden.

Er stond uit informatierapporten (RIR) afkomstige politionele informatie met de code 00 of 01 in de gegevensbank.[108] Het OCAD had nochtans aangegeven deze, net omwille van de gevoeligheid van de erin opgenomen informatie, nooit op te nemen in de gegevensbank FTF.

Uit de analyse van het COC en het Vast Comité I bleek dat de praktijk van het OCAD om de RIR's 00 en 01 systematisch uit te sluiten, niet werd opgenomen in de regelgeving. *De lege lata*, zijn de enige uitzonderingen op de verplichting om de gemeenschappelijke databank te voeden met informatie:

– ofwel de classificatie[109]: geclassificeerde informatie mag niet worden opgenomen in de inlichtingenfiches noch in de informatiekaarten[110];
– ofwel een embargo door de bevoegde magistraat, met instemming van de federale procureurl[111]: in dat geval is de verplichting tot voeden uitgesteld (en

108 De codes worden toegekend door de (politie-)dienst die de nota opstelt. Een 'RIR 01' betreft politie-informatie die enkel mits akkoord van de opsteller kan worden gebruikt. Een 'RIR 00' op zijn beurt betreft politie-informatie die in geen enkel geval mag worden gebruikt. Het gaat om uiterst gevoelige informatie die bijvoorbeeld kan leiden tot de identificatie van een bron. Deze codes vloeien voort uit de Gemeenschappelijke richtlijn MFO3 van de ministers van Binnenlandse Zaken en Justitie betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie.

109 Op basis van de Wet van 11 december 1998 inzake de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

110 Art. 1, 11° et 12°; art. 6 § 1, 3° KB FTF.

111 Art. 44/11/3*ter* § 5 WPA.

niet uitgesloten) zolang deze meent dat de voeding de uitoefening van de strafvordering of de veiligheid van een persoon in het gedrang kan brengen;
– ofwel een embargo door de leidinggevende van een inlichtingen- en veiligheidsdienst wanneer en zolang hij oordeelt dat deze voeding de veiligheid van een persoon in het gevaar kan brengen of wanneer de informatie afkomstig is van een buitenlandse dienst die uitdrukkelijk gevraagd heeft deze niet aan andere diensten toe te zenden.[112]

Dit betekent dat behoudens classificatie of embargo, alle informatierapporten moeten worden opgenomen in de gemeenschappelijke FTF-gegevensbank.

VI.2.2.1.4. De personen in 'vooronderzoek'

De personen waarover er enkel 'ernstige aanwijzingen' bestaan (en waarover dus geen zekerheid is) dat ze behoren tot een van de vijf categorieën, mogen worden opgenomen in de gegevensbank, maar slechts voor een maximumduur van zes maanden (artt. 6 § 1, 2° en 13 KB FTF). Wanneer er tijdens deze termijn geen enkele informatie binnenkomt die de registratie bij een van de vijf categorieën kan rechtvaardigen, moeten de namen van deze personen 'in vooronderzoek' worden gewist.

Een onderzoek van de lijsten van deze personen in maart 2017 (bijna driehonderd personen) en in december 2017 (een twintigtal personen), toonde aan dat vijf entiteiten die op de eerste lijst stonden, nog steeds voorkwamen op de tweede lijst. Gelet op de maximale bewaartermijn van zes maanden, zou dat niet gemogen hebben. Er werd blijkbaar niets gewist en er was geen automatisch 'knipperlicht' als het OCAD naliet om actie te ondernemen. Dit punt was voor verbetering vatbaar.

VI.2.2.1.5. De bewaring van gegevens

Voor de personen die opgenomen zijn in de databank, stelt de WPA dat tenminste elke drie jaar na de laatste verwerking moet worden onderzocht of de gegevens nog steeds rechtstreeks verband houden met het doeleinde. In voorkomend geval, worden de gegevens bewaard.

Blijkens de vaststellingen van het COC en het Vast Comité I, beschikt het OCAD niet over een informatica-tool waarmee deze specifieke verplichting kan worden opgevolgd. Hierover meldde het OCAD dat deze technische oplossing (vooralsnog) geen prioriteit had (in 2017), aangezien de evaluatie pas ten laatste moet plaatsvinden na drie jaar en dat de gemeenschappelijke gegevensbank FTF in werking is sedert 1 januari 2016.

Het COC en het Vast Comité I bevalen de ontwikkeling van een informatica-tool aan in de loop van 2018; deze moet het OCAD in staat stellen om vanaf januari 2019 de bewaringstermijnen op te volgen.

---

[112] Art. 44/11/3*ter* § 5 WPA.

VI.2.2.2. De controle van de loggings bij de beheerder van de gegevensbank

Het COC en het Vast Comité I verzochten de Federale Politie om de mededeling van de uitgevoerde loggings door de verschillende diensten van twee willekeurig gekozen dagen. Uit deze informatie, aangevuld met een analyse van een steekproef van de inlichtingenfiches (*supra*), kon worden vastgesteld dat de gemeenschappelijke FTF-gegevensbank door de verschillende diensten geraadpleegd en gevoed werd.

Een dermate grote toegang houdt onvermijdelijk veiligheidsrisico's in. De betrokken consulenten inzake veiligheid en bescherming van de persoonlijke levenssfeer en deze van de gemeenschappelijke gegevensbank FTF hebben hier een belangrijke rol omdat zij waken over de rechtmatigheid van de diverse toegangen door de verschillende diensten. De loggings vormen daartoe een uitgelezen controle-instrument. Het COC en het Vast Comité I hebben moeten vaststellen dat er op het ogenblik van de inspectie maar weinig (of zelfs helemaal geen controles worden uitgevoerd) van de loggings (cf. *infra*).

Bijgevolg waren het COC en het Vast Comité I van mening dat de consulenten inzake veiligheid en bescherming van de persoonlijke levenssfeer systematische controles moeten verrichten of op zijn minst regelmatig steekproeven moeten nemen van de loggings van hun diensten.

VI.2.2.3. De informatie aan de burgemeesters

Het KB FTF bepaalt dat de korpsoverste van de betrokken politiezone de informatiekaarten betreffende de *foreign fighters* die in zijn gemeente verblijven, (systematisch) bezorgen aan de burgemeester. De burgemeester kan deze vervolgens gebruiken in het kader van zijn bevoegdheden en onder zijn verantwoordelijkheid. Het OCAD had geen enkel zicht over de manier waarop deze verplichting wordt nageleefd.[113]

VI.2.2.4. Mededeling van uittrekels van de informatiekaart aan derden

Het OCAD bezorgt elke maand aan verschillende bestemmelingen een lijst waarin de namen zijn opgenomen van alle FTF.[114] Volgens het OCAD gaat het om diensten die deze informatie nodig hebben in de uitoefening van hun bevoegdheden.

---

113 Daarom moet de naleving van die verplichting op een andere manier worden onderzocht. Het COC en het Vast Comité I zullen hierop terugkomen in een later onderzoek. Ze vestigden evenwel de aandacht op het nut van een opvolgingsinstrument op niveau van het OCAD om erover te waken dat deze verplichting daadwerkelijk wordt nageleefd.

114 Te noteren dat deze doorzending via e-mail gebeurt. Ook al zijn deze gegevens niet geclassificeerd en voorziet artikel 11 KB FTF dat deze kunnen worden doorgezonden '*met welk middel ook*', zijn het COC en het Comité van oordeel dat er gelet op de gevoeligheid van de informatie, aandacht moet worden besteed aan de beveiliging van deze doorzending.

Sommige van die diensten hebben een rechtstreekse toegang tot de gegevensbank. Voor hen stelt er zich geen probleem. Voor wat de andere diensten betreft, herinneren het COC en het Vast Comité I eraan dat een gezamenlijke lezing van de artikelen 44/11/6*quater* WPA en 11 § 2 KB FTF vereist dat deze communicaties aan derden voorafgaandelijk het voorwerp uitmaken van een beoordeling door het OCAD of de door politie- en inlichtingendiensten.

Voor het COC en het Vast Comité I hoort bij een dergelijke beoordeling een analyse van alle informatieveiligheidsaspecten met betrekking tot de FTF; op grond van die analyse moeten aangepaste beveiligingsmaatregelen opgelegd worden aan de verschillende bestemmelingen.

VI.2.2.5. Controle van andere diensten die toegang hebben tot de gegevensbank FTF

VI.2.2.5.1. Verificatie bij andere diensten

De uitgevoerde controle in 2017 beperkte zich niet louter tot het OCAD. Ingevolge verificaties die werden uitgevoerd bij verschillende diensten, konden het COC en het Comité vaststellen dat:

- alle diensten beschikten over een lijst waarin de identiteit wordt vermeld van personen die toegang hebben tot de gegevensbank. Er werd verklaard dat al deze personen in het bezit waren van een veiligheidsmachtiging van het niveau 'geheim';
- de diensten hadden geen rechtstreekse toegang tot de 'loggings' (deze zijn beschikbaar bij de Federale Politie), wat maakt dat de meeste diensten niet in staat waren een rechtmatigheidscontrole uit te voeren van de toegang tot of bevraging van de gegevensbank (*supra*);
- met uitzondering van het openbaar ministerie[115], beschikte het merendeel van de diensten over een validatiesysteem. Sommige diensten hebben dit systeem verder ontwikkeld op verzoek van het COC en het Vast Comité I. Toch moet voorbehoud worden geformuleerd bij het systeem van één van de diensten die slechts een controle in de FTF-gegevensbank uitvoert als de persoon reeds gekend is in de Algemene Nationale Gegevensbank (ANG) van de politie. Een persoon kan immers worden opgenomen in de FTF-gegevensbank

115 Het is nuttig om daarbij te verwijzen naar de Memorie van toelichting van de Wet van 27 april 2016 (*Parl. St.* Kamer 2015-16, 54K1727/1, 30) en naar het Verslag aan Koning bij het KB FTF: *'De wetgever heeft rekening gehouden met het specifieke onafhankelijke statuut van het openbaar ministerie en heeft geoordeeld dat de gerechtelijke gegevens voornamelijk afkomstig zijn van de politiediensten. Bijgevolg is de verplichting van de politiediensten om de gemeenschappelijke databank te voeden voldoende opdat de pertinente gerechtelijke gegevens worden geregistreerd. Om zich ervan te vergewissen dat de voeding van de gegevensbank FTF in dit kader goed wordt uitgevoerd, wordt voorzien dat de gerechtelijke overheden de gepaste instructies versturen onder andere via omzendbrieven'*. De COL 22/2016 kondigt richtlijnen in die zin aan voor de politiediensten.

(bijvoorbeeld op initiatief van een inlichtingendienst) zonder daarom noodzakelijk te zijn opgenomen in de ANG.

– geen enkele dienst had kennis van een veiligheidsincident.[116] Als de diensten hierover later opnieuw worden bevraagd, brengt de Federale Politie het COC en het Vast Comité I op de hoogte van een veiligheidsincident in de loop van oktober 2017. Het COC en het Comité oordelen dat zij, in hun hoedanigheid van controleorgaan van de gemeenschapppelijke gegevensbank FTF, systematisch en spontaan van ieder veiligheidsincident op de hoogte moeten worden gebracht.

VI.2.2.5.2. Verificaties bij de beheerder van de gegevensbank

Naar aanleiding van diverse verificaties die werden uitgevoerd bij de Federale Politie als beheerder van de FTF-gegevensbank[117], konden het COC en het Vast Comité I met voldoening vaststellen dat de gebruiksaanwijzing van de gegevensbank FTF werd bijgewerkt. Het COC en het Comité benadrukken dat er, naast dit noodzakelijk instrument, opleidingen op het niveau van de gebruikers moeten georganiseerd worden op initiatief van de aangeduide consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer.

Het COC en het Vast Comité I kregen daarnaast de lijst van alle gebruikers die toegang hadden tot de database FTF (1506 personen op 14 april 2017) alsook de loggings (historiek van de toegangen) voor de gekozen data (*supra*).

Ten slotte gaf de Federale Politie toelichting bij het veiligheidsincident dat het resultaat was van verkeerdelijk in de gegevensbank geregistreerde informatie.

VI.2.2.6. De niet-aanstelling van een consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer voor de gegevensbank FTF

Elke dienst/gebruiker heeft een consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer aangesteld (wiens bevoegdheid beperkt is tot de betrokken dienst).

Echter, eind 2017 hadden de verantwoordelijken voor de verwerking (de ministers van Justitie en Binnenlandse Zaken) nog steeds geen veiligheidsconsulent voor de gegevensbank FTF aangewezen. De aanstelling van deze functie is nochtans cruciaal.[118]

Het COC en het Vast Comité I richtten in die zin twee brieven aan de de ministers van Justitie en Binnenlandse Zaken in hun hoedanigheid van verant-

---

116 De Dienst Vreemdelingenzaken meldde dat ze initiatieven nam op vlak van informatieveiligheid: er werd een specifieke opleiding uitgewerkt alsook werd een applicatie ontwikkeld die de toegang moet toelaten via authentificatie van de e-ID. Het COC en het Vast Comité I ondersteunen en moedigen dergelijke initiatieven aan.

117 Art. 3 KB FTF.

118 Zie art. 44/3 § 1/1 WPA en art. 5 KB FTF.

woordelijken voor de verwerking. Eerder werden ze hierover geïnterpelleerd in de gemeenschappelijke adviezen.[119]

VI.2.2.7. Twee nieuwe verwerkingen: home-grown terrorist fighters en haatpredikers

In de marge van hun onderzoek naar de gemeenschappelijke gegevensbank FTF, hebben het COC en het Vast Comité I de verwerking vastgesteld van entiteiten die waren opgenomen in de zgn. Joint Information Box[120] (JIB), met name de lijst (beheerd door het OCAD) van personen en organisaties die een sleutelrol spelen in het radicaliseringsproces.[121]

Daarnaast werd een andere, nieuwe verwerking ingevoerd, onder de noemer *home-grown terrorist fighters* (HTF).[122] Deze verwerking beoogt de oplijsting van personen met terroristische neigingen in België en die, anders dan bij de *foreign terrorist fighters* niet de intentie hebben (in het verleden of toekomst) om af te reizen naar een jihadistische conflictzone.

Deze nieuwe verwerkingen kwamen er op uitdrukkelijke vraag van de ministers van Justitie en Binnenlandse Zaken. Zonder de opportuniteit of het operationeel nut van dergelijke bijkomende verwerkingen in twijfel te willen trekken[123], vestigden het COC en het Vast Comité I er de aandacht op dat met deze verwerkingen werd gestart zonder KB en zonder voorafgaandelijk advies van het Vast Comité I en het COC.

Het COC en het Vast Comité I hebben de ministers van Justitie en Binnenlandse Zaken hierover bevraagd.

VI.3. DE ADVIESFUNCTIE

VI.3.1. EEN 'BIJKOMENDE VOORAFGAANDELIJKE AANGIFTE'

Op 22 juni 2017 hebben de ministers van Binnenlandse Zaken en Justitie een 'aanvullende voorafgaandelijke aangifte' betreffende de FTF-gegevensbank overgezonden aan het COC en het Vast Comité I.

Deze aangifte had tot doel om de oorspronkelijke aangifte inzake de mogelijkheid tot rechtstreekse toegang voor de Justitiehuizen (meer in het bijzonder het

---

119 Cf. het gemeenschappelijk advies 1/2016 van 20 juni 2016 (punt 10) en het gemeenschappelijk advies 2/2016 van 1 december 2016 (punt 10), in VAST COMITÉ I, *Activiteitenrapport 2016*, 219-230.

120 Zie VAST COMITÉ I, *Activiteitenverslag 2015*, 7-11.

121 Het betrof 72 entiteiten op 13 november 2017.

122 Het betrof 30 entiteiten au 13 november 2017.

123 Zie hierover het gemeenschappelijk advies nr. 01/2016 van 20 juni 2016, als bijlage bij het Activiteitenverslag 2016 van het Vast Comité I (216 e.v.).

Directoraat-generaal Justitiehuizen van de Federatie Wallonië-Brussel, de Dienst Justitiehuis van het ministerie van de Duitstalige Gemeenschap en de Afdeling Justitiehuizen van de administratieve diensten van de Vlaamse overheid, beleidsdomein Welzijn, Volksgezondheid en Gezin) te vervolledigen.

Voor deze diensten is de rechtstreekse toegang beperkt tot de persoonsgegevens van de *foreign terrorist fighters* voor wie de dienst zijn opdracht van justitiële begeleiding en toezicht moet uitoefenen (art. 7 § 1, lid 6 KB FTF). Samenhangend met hun (beperkte) rechtstreekse toegang, hebben deze diensten de verplichting om de FTF-gegevensbank te voeden (artt. 44/11/3*ter* §§ 4 en 5 WPA en 7 § 1, lid 5 KB FTF).

Deze aanvullende aangifte bevatte een aantal toelichtingen en preciseringen aangaande de identiteit van de veiligheidsconsulenten, de identificatie van de personen die recht hebben op een directe toegang en een beschrijving van het valideringssyteem.

VI.3.2. EEN GEZAMENLIJK ADVIES

Conform artikel 44/11/3*bis* § 3 WPA brachten het COC en het Vast Comité I op 20 juli 2017 een gemeenschappelijk advies uit.[124]

Samenvattend stelden het COC en het Vast Comité I het volgende:

- de aanvullende voorafgaandelijke aangifte maakte (nog steeds) geen melding van de consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer die moet worden aangesteld door de ministers van Binnenlandse Zaken en Justitie, en dit niettegenstaande de eerder geformuleerde opmerkingen hieromtrent. In hun schrijven van 22 juni 2017 kondigden de ministers de 'spoedige aanstelling' van deze persoon aan;
- ze benadrukten aangaande het type van toegang, dat het beginsel van de *need to share* – zoals terecht onderstreept door de parlementaire onderzoekscommssie 'aanslagen'[125] – geen enkele afbreuk doet aan het principe van de *need to know*. Met andere woorden, de toegang dient in die zin te worden georganiseerd dat de noodzakelijke *need to share de facto* niet evolueert naar een *nice to know*.
- ze herhaalden dat het in het kader van hun controleopdracht absoluut noodzakelijk is om te kunnen beschikken over de historiek van de inlichtingenfiches en dit om na te kunnen gaan wat de toestand en de inhoud ervan op een uitgekozen moment is. In hun begeleidend schrijven stelden de ministers dat er hieraangaande een technische oplossing wordt uitgewerkt door de Federale Politie (belast met het technisch en functioneel beheer van de FTF-gegevensbank).

124 Dit advies kan worden geconsulteerd op www.comiteri.be.
125 *Parl. St.*, Kamer 2016-17, 54K1752/008, 166.

– ze verzochten de betrokken diensten dat deze er bij het opstellen van hun intern valideringssysteem rekening mee zouden houden dat ze (middels een document) konden aantonen dat de persoonsgegevens en informatie die ze in het systeem inbrengen passend, ter zake dienen en niet overmatig zou zijn in het licht van de doeleinden en de finaliteiten van de FTF-gegevensbank.

HOOFDSTUK VII
ADVIEZEN

Artikel 33, zevende lid, W.Toezicht bepaalt dat het Comité '*enkel op verzoek van de Kamer van volksvertegenwoordigers of van de bevoegde minister advies [mag] uitbrengen over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin de beleidslijnen van de bevoegde ministers worden geformuleerd*.' Daarnaast dient het Comité ook advies te verlenen bij de wettelijke regeling in verband met gemeenschappelijke databanken, maar dan samen met het COC. Deze adviesbevoegdheid wordt behandeld in Hoofdstuk VI.

In 2017 werd het Comité driemaal door het Parlement en tweemaal door de minister van Justitie om advies verzocht. Een advies – met name het advies op verzoek van de Commissie Binnenlandse Zaken bij het Wetsontwerp houdende wijziging van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen – wordt onder hoofdstuk X.2.3 besproken omdat het aansluit bij de werking van het Beroepsorgaan.

VII.1. ADVIES BIJ HET ONTWERP VAN WET TOT WIJZIGING VAN DE WET VAN 30 NOVEMBER 1998

In februari 2016 vroeg de minister van Justitie het advies van het Vast Comité I aangaande het voorontwerp van wet tot wijziging van de Inlichtingenwet van 30 november 1998.[126, 127] In het kader van de bespreking van het ontwerp in de Kamer van Volksvertegenwoordigers, werd begin 2017 een gelijkaardig advies[128] bezorgd aan de Kamercommissie Justitie.

Daarin beval het Vast Comité I in algemene zin aan dat de wjzigingsvoorstellen beter geduid moesten worden naar finaliteit en in bepaalde gevallen meer in detail moesten geregeld worden in het ontwerp. Ook diende grondiger gereflecteerd te worden over sommige fundamentele opties. Daarnaast beval het Comité

126 Dit advies werd eerder integraal opgenomen in het *Activiteitenverslag 2016*, 210-218.

127 Ondertussen is de Wet van 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek (*BS* 8 mei 2017) van kracht.

128 Het advies kan worden geconsulteerd op www.comiteri.be.

aan dat het toezicht en de controle op een adequaat niveau zouden gebracht worden om de mogelijkheden van de diensten en van de toezichthouders in balans te houden. De bedenkingen moesten worden gekaderd in de bekommernis om te voldoen aan de fundamentele eisen zoals die voortvloeien uit nationale en internationale rechtsnormen. Het Comité benadrukte dat het uitgebreide ontwerp tal van positieve elementen bevatte en dit zowel op legistiek vlak als vanuit het oogpunt van de operationele noden van beide inlichtingendiensten.

VII.2. ADVIES BIJ HET WETSONTWERP BETREFFENDE DE CLASSIFICATIE EN DE VEILIGHEIDSMACHTIGINGEN, VEILIGHEIDSATTESTEN EN VEILIGHEIDSADVIEZEN

Op 1 december 2017 werd het Vast Comité I door de Voorzitter van de Commissie voor de Binnenlandse Zaken, de Algemene Zaken en het Openbaar Ambt gevraagd advies te verlenen aangaande het wetsontwerp houdende wijziging van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.[129]

Vooraf benadrukte het Comité dat nergens gewag werd gemaakt van de mogelijke/onvermijdelijke implicaties van het op de werklast van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en-adviezen.

Het Comité formuleerde tal van opmerkingen en bedenkingen. Een gepast antwoord van de wetgever drong zich op om te vermijden dat er rechtsonzekerheid zou ontstaan in een dergelijke belangrijke materie die zich situeert in het spanningsveld van veiligheid en rechten van de burger.

Het Comité benadrukte dat het ontwerp geen antwoord bood op de vele problemen die de toepassing van de toen geldende regeling met zich bracht (complex, veel te korte beroepstermijnen…), zowel op het vlak van de betrokken administraties, van de betrokken burgers als van het Beroepsorgaan. Eerder werden voorstellen geformuleerd om bepaalde van die problemen te remediëren. Het ontwerp van wet ging daar niet alleen niet op in, het creëerde onvermijdelijk bijkomende problemen voor alle actoren. Het Comité achtte het dan ook aangewezen dat zowel de Wet van 11 december 1998 houdende veiligheidsmachtigingen, -attesten en -adviezen als de Wet van 11 december 1998 tot oprichting van het beroepsorgaan op een coherente wijze zouden worden hervormd.

---

129 Gelet op het uiterst korte tijdsbestek – hat advies werd ingewacht voor 15 december 2017 – om te antwoorden enerzijds en op de uitgebreidheid en de complexiteit van de voorgestelde wijzigingen anderzijds, kon het Comité niet in detail ingaan op elk aspect van het ontwerp, laat staan een legistieke controle uitvoeren of alternatieve tekstvoorstellen uitwerken. Het advies kan worden geconsulteerd op www.comiteri.be.

VII.3. ADVIES BIJ HET VOORONTWERP VAN WET INZAKE HET GEBRUIK VAN CAMERA'S

In 2017 formuleerde het Vast Comité I ook een advies aan de minister van Justitie omtrent het '*Voorontwerp van wet tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiediensten te regelen en tot wijziging van wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's en van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten*'.[130]

Het Comité stelde zich vooreerst vragen bij de noodzaak van bepaalde aspecten van het ontwerp en wees op de complexiteit van de voorgestelde regeling. Verder ging het Comité in detail in op het voorgestelde artikel 16/4 § 1 W.I&V (de mogelijkheid tot rechtstreekse toegang tot informatie en persoonsgegevens die verzameld worden door camera's gebruikt door de politiediensten), artikel 16/4 § 2 W.I&V (de mogelijkheid tot toegang *a posteriori* tot verzamelde gegevens waarbij het Comité van oordeel was dat de voorziene controle niet in verhouding was met het potentieel intrusief karakter van de voorgestelde methode), artikel 16/4 § 4 W.I&V (dat een nieuwe, verregaande mogelijkheid onder de vorm van datamining vooropstelde waarbij de/alle (gekende of mogelijke) targets van de inlichtingendiensten automatisch kunnen afgetoetst worden aan de gegevens beschikbaar in de technische databanken) en artikel 16/4 § 6 W.I&V (waarbij het Comité zich afvroeg of het geheim van het onderzoek niet meer zou kunnen ingeroepen worden tegenover de inlichtingendiensten die camerabeelden wensen te consulteren).

VII.4. ADVIES OMTRENT EEN REGELING VOOR EEN INLICHTINGENMETHODE VOOR HET MACHTIGEN VAN MENSELIJKE BRONNEN TOT HET PLEGEN VAN MISDRIJVEN

Halverwege december 2017 bracht het Vast Comité I op verzoek van de minister van Justitie zijn advies[131] uit omtrent '*een wettelijke regeling voor een inlichtingenmethode voor het machtigen van menselijke bronnen tot het plegen van misdrijven in de Wet van 30 november 1998 houdende de inlichtingen- en veiligheidsdiensten*'.

In dat advies merkte het Comité op dat – vooraleer de mogelijkheid te creëren voor informanten om misdrijven te plegen – de wettelijke verplichting die rust op de Nationale Veiligheidsraad om een richtlijn uit te vaardigen omtrent alle aspec-

130 Het advies kan worden geconsulteerd op www.comiteri.be.
131 Het advies kan worden geconsulteerd op www.comiteri.be.

ten van de werking met menselijke bronnen[132], prioritair uitvoering moest krijgen.

Wat betreft de mogelijkheid om misdrijven te plegen, was het Comité van oordeel dat in deze geen rol is weggelegd voor het Federaal Parket, maar wel voor de BIM-Commissie en – gezien het belang van de materie – ook voor het Vast Comité I.

Wat betreft de verdere uitwerking van de regeling, dient eerst uitgemaakt te worden welke finaliteit(en) het plegen van misdrijven moet(en) dienen. Indien de voornaamste reden is dat het de diensten moet toelaten 'hun informatiepositie te behouden', kon gedacht worden aan een uitbreiding van de mogelijkheid voorzien in artikel 13/1 W.I&V. In dat geval is de toelating immers eerder een 'beschermings- of ondersteuningsmaatregel'. Wel moet dan bijkomend voorzien worden in een tussenkomst van het Vast Comité I. Indien het echter (ook) de bedoeling zou zijn dat informanten misdrijven kunnen plegen om bepaalde inlichtingen te bekomen (bijvoorbeeld wegmaking van documenten), dan was het Comité van oordeel dat dit als een specifieke methode zou moeten beschouwd worden, hetgeen inhoudt dat zowel de BIM-Commissie als het Vast Comité I kunnen interveniëren.

Het Comité was verder van oordeel dat er moest nagedacht worden over de mogelijkheid om expliciet in de wet te bepalen dat BIM-methoden kunnen gebruikt worden om de betrouwbaarheid na te gaan van informanten die op verzoek van de inlichtingendiensten infiltreren, en die desgevallend misdrijven mogen plegen.

132 Sinds 2010 werd die verplichting ingeschreven in art. 18 W.I&V.

HOOFDSTUK VIII
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.[133] 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*

133 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 2017 voerde de Dienst Enquêtes I onderzoeksdaden uit in het kader van opsporingsonderzoeken. Een eerste dossier betrof een onderzoek in opdracht van de gerechtelijke overheden te Brussel naar het mogelijks frauduleus gebruik van een dienstkaart door een lid van een inlichtingendienst. Een tweede opsporingsonderzoek werd gevoerd op vordering van het Federaal Parket en betrof de mogelijke betrokkenheid van een lid van een inlichtingendienst aan een misdaad of wanbedrijf tegen de inwendige en uitwendige veiligheid van de Staat.

Verder stelt artikel 50 W.Toezicht dat '*[e]lk lid van een politiedienst dat een misdaad of een wanbedrijf gepleegd door een lid van een inlichtingendienst vaststelt, maakt daarover een informatief verslag op en bezorgt dat binnen de vijftien dagen aan het hoofd van de Dienst Enquêtes I*'. De enquêtedienst ontving in 2017 twee meldingen in die zin.

HOOFDSTUK IX
EXPERTISE EN EXTERNE CONTACTEN

IX.1. EXPERT OP DIVERSE FORA

Leden van het Vast Comité I en van zijn personeel werden in 2017 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. In de loop van 2017 organiseerde het BISC twee studiedagen over 'Managing uncertainties. De bescherming van kritische infrastructuren en de inlichtingendiensten' en 'Counter insurgency – Terrorisme and the role of intelligence services'. De voorzitter van het Comité nam de opening van deze studiedagen voor zijn rekening;
- De griffier nam eind januari 2017 op uitnodiging van de *European Union Agency for Fundamental Rights* (FRA) deel aan het panelgesprek 'Enforcing the right to remedy in cases of surveillance: a human right challenge' tijdens de '10th International Conference on Computers, Privacy and Data Protection' in Brussel;
- In februari 2017 nam het Vast Comité I deel aan de derde 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).[134] De resultaten van het expertenonderzoek werden er besproken en een ontwerprapport[135] werd voorgelegd;

---

134 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). De DRA 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.

135 Dit resulteerde in oktober 2017 in de publicatie: FRA, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update*, Luxemburg, 2017, 164 p.

- De griffier van het Vast Comité I werd uitgenodigd in het kader van het opleidingsonderdeel 'Intelligence' van de Master in de internationale betrekkingen en de diplomatie (Universiteit Antwerpen) om er de werking van het Comité toe te lichten;
- Het Vast Comité I vormde in maart de gesprekspartner van de *Stiftung Neue Verantwortung* tijdens een gedachtewisseling omtrent 'New challenges and changes to democratic control of intelligence in Belgium and Germany';
- Tijdens de RightsCon conference in Brussel eind maart 2017 nam de griffier deel aan het panelgesprek 'Surveying Surveillance in the EU';
- Op uitnodiging van het *Geneva Centre for the Democratic Control of Armed Forces* (DCAF) namen zowel de voorzitter als de griffier van het Comité in Tunesië eind april 2017 deel aan rondetafelgesprekken over *'Les lois qui régissent le renseignement – Droit comparés'*. In een zelfde context intervenieerde de voorzitter van het Comité in november 2017 eveneens in Tunis in de sessie 'Redevabilité et protection des données personnelles' tijdens de rondetafel 'Cybersécurité – Expériences internationales et Droits comparés';
- Er werd een beroep gedaan op de expertise van het Comité in een praktijkseminarie bestemd voor politie, magistratuur en advocatuur rond het thema 'claassificatie en veiligheidsmachtigingen';
- In oktober 2017 werd het Vast Comité I ingeschakeld in het kader van een DCAF-training over 'Monitoring Law Enforcement and Intelligence Services in Georgia – Status, Needs and International Best Practices' (Tbilisi, Georgië);
- Het Vast Comité I werkte in oktober 2017 mee aan een enquête uitgevoerd door *Privacy International* (UK) en *La Ligue des Droits de l'Homme* (B) aangaande 'Oversight of intelligence sharing between your government and foreign governements';
- De griffier van het Vast Comité I nam in november 2017 deel aan de 'Expert Roundtable on Intelligence Oversight in the framework of the DCAF Assistance Program for the Parliament of the Republic of Macedonia' over 'The Accountability of Electronic Interception of Communication'. Daar werd onder meer de kiem gelegd voor een 'Parliamentary Handbook on Inspection Visits';
- In 2017 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'* en *'Le contrôle parlementaire'*.

IX.2. SAMENWERKINGSPROTOCOL MENSENRECHTEN

België werkt al jaren aan de oprichting van een nationaal Mensenrechteninstituut, een engagement dat werd aangegaan bij het ondertekenen van het Protocol bij het VN-verdrag tegen foltering. De effectieve oprichting van een dergelijk

instituut kon pas na ratificatie van het protocol, waarmee – naast het federale Parlement – ook alle deelstaten moeten instemmen. Ondertussen verschenen de instemmingsaktes van de Vlaamse, Franstalige en Duitstalige Gemeenschap als van het Waals Gewest in het Staatsblad en werd ook de akte van de Verenigde Vergadering van de Gemeenschappelijke Gemeenschapscommissie gepubliceerd. Rest alleen nog de federale instemmingswet.

In afwachting van de oprichting van het instituut, resulteerde de vergaderingen met diverse instellingen met een mandaat op het gebied van mensenrechten[136] in januari 2015 in een samenwerkingsprotocol.[137] Daarin kwamen alle deelnemende instanties overeen om praktijken en methoden uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen.

De activiteiten van dit platform namen in 2017 de vorm aan van maandelijkse overlegvergaderingen waarin zowel algemene problematieken (bijv. 'België en de bevordering en bescherming van mensenrechten', 'The efforts to provide support to strengthen the human rights infrastructure', 'Het beroepsgeheim en de nieuwe vreemdelingenwet over buitenlanders die 'een gevaar vormen voor de samenleving'…) als de uitwisseling van werkwijzen en methodologieën over concrete individuele dossiers aan de orde waren. Na de Privacycommissie in 2016 nam Unia in 2017 het voorzitterschap waar.

IX.3. EEN MULTINATIONAAL INITIATIEF INZAKE INTERNATIONALE INFORMATIE-UITWISSELING

Sinds 2015 voeren onafhankelijke toezichthouders van vijf Europese landen gelijktijdig maar elk binnen het kader van zijn mandaat en bevoegdheden, een onderzoek naar de internationale uitwisseling van persoonsgegevens in het kader van de strijd tegen FTF. Het betreft België, Denemarken, Nederland, Noorwegen en Zwitserland.[138] Het is daarbij de bedoeling te komen tot een gemeenschappelijke rapport.

In 2017 werden diverse ontwerpteksten uitgewisseld en vond een tweedaagse *expert meeting* plaats op uitnodiging van het *Norwegian EOS Committee*. Dit resulteerde in een eerste ontwerp van een gemeenschappelijk document dat als basis diende voor verdere discussie.

---

136 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.

137 Samenwerkingsprotocol van 13 januari 2015 tussen de instellingen met een volledig of gedeeltelijk mandaat belast met de eerbiediging van de rechten van de mens.

138 Zie VAST COMITÉ I, *Activiteitenverslag 2015*, 80-81.

IX.4. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

Het Vast Comité I onderhield nauwe contacten met de Franse *Délégation parlementaire au renseignement* (DPR), met de *Commission nationale de contrôle des interceptions de sécurité* (CNCIS) en de recent opgerichte *Commission nationale de contrôle des techniques de renseignement* (CNCTR). Tijdens een colloquium dat plaatsvond in de Franse Assemblée nationale in maart 2017 en waarop een vertegenwoordiging van het Comité aanwezig was, konden de relaties verder worden uitgebouwd.

Het Comité nodigde op 27 en 28 november 2017 het nieuwe Zwitserse toezichtsorgaan *Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten* (Autorité de surveillance indépendente des activités de renseignement) uit voor een bezoek in Brussel. Een tegenbezoek is gepland voor eind 2018.

De nieuwe Canadese ambassadeur werd ontvangen door de voorzitter van het Vast Comité I voor een kennismakingsgesprek en ook met het Canadese toezichtsorgaan werd informatie uitgewisseld over de op til zijnde wijzgingen in het Canadese toezichtlandschap op de inlichtingendiensten, meer in het bijzonder over de oprichting van *l'Office de surveillance des activités en matière de sécurité nationale et de renseignement.*

In november 2017 werd in Brussel het *International Intelligence Oversight Forum*, georganiseerd door de *Special Rapporteur for Privacy* (SRP) van de Verenigde Naties. Hieraan namen zowel vertegenwoordigers van toezichthouders, inlichtingendiensten, universiteiten en NGO's deel. Het thema in 2017 was 'The Road Ahead – Dilemmas and Best Practices in Democratic Intelligence Oversight'. Een delegatie van het Vast Comité I onderhield informele contacten met toezichthouders uit Nederland, Frankrijk, het Verenigd Koninkrijk, Duitsland, Noorwegen… Het doel van dit forum bestond erin om in een vertrouwelijke omgeving een beter begrip te krijgen in de uitdagingen waarmee onder meer democratische toezichtorganen worden geconfronteerd in een digitale wereld.

Ten slotte vonden voorbereidende contacten plaats met het oog op de organisatie van een bezoek in Brussel in de loop van 2018 van de Georgische *Office of the Personal Data Protection Inspector* en vertegenwoordigers van het Georgische parlement.

IX.5. 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, de rechtmatigheid en de doelmatigheid 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. De controle van de speciale fondsen van de ADIV wordt uitgevoerd door een vertegenwoordiger van het kabinet van de minister van Defensie en dit viermaal per jaar. Op suggestie van het Rekenhof gebeurt dit sinds 2010 in aanwezigheid van de voorzitter van het Vast Comité I. Ook in 2017 was de voorzitter aanwezig bij deze controle.

IX.6. 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**
12 januari 2017	'Comité I bundelt aanwijzingen tegen Oussama Atar voor commissie aanslagen 22 maart'	De Morgen
25 januari 2017	'Kazachgate: Chodiev est devenu belge alors que la Sûreté connaissait ses liens avec la mafia, dit le Comité R'	La Libre Belgique
25 januari 2017	'La Sûreté ne s'est pas opposée à la naturalisation de Chodiev qu'elle savait mafieux'	Le Vif
29 maart 2017	'Kazachgate zorgt voor spanningen bij Staatsveiligheid'	Knack
29 maart 2017	'Kazachgate: Comité I ziet geen elementen die aantijgingen in anonieme brief ondersteunen'	nl.metrotime.be
12 juli 2017	'Geldgebrek belemmert waakhond Staatsveiligheid'	De Standaard
17 oktober 2017	'Attentats à Bruxelles: le service de renseignement militaire pointé du doigt dans le rapport du Comité R'	rtbf.be
18 oktober 2017	'Jaarverslag Comité I 'Inlichtingendiensten lieten steken vallen vóór 2017''	De Standaard

HOOFDSTUK X
DE GRIFFIE VAN HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN

De voorzitter van het Vast Comité I oefent het voorzitterschap van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen uit. 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 administratieve 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.[139]

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.

X.1. EEN BIJ WIJLEN ZWARE EN COMPLEXE PROCEDURE

Zowel de griffie als het Beroepsorgaan worden geconfronteerd met een toenemende werklast. De te behandelen dossiers worden immers steeds complexer op het vlak van administratief beheer, de terechtzittingen en de beslissingen.

139 Zie hierover uitgebreid VAST COMITÉ I, *Activiteitenverslag 2006*, 91-119.

Zo voldoen heel wat verzendingen niet aan de vereisten gesteld in de artikelen 2 en 3 van het KB Beroepsorg., waarin respectievelijk staat dat '*alle processtukken aan het beroepsorgaan worden toegezonden bij ter post aangetekende brief*' en dat '*de beroepsakte wordt ondertekend en gedagtekend door de eiser of door een advocaat*'. De griffier ziet zich dan ook genoodzaakt de eiser hierop te wijzen met het oog op de regularisatie van de situatie binnen de wettelijke termijn.[140] Hetzelfde geldt voor de administratieve dossiers die door de diverse veiligheidsoverheden worden toegezonden; deze blijken niet steeds volledig zodat de griffie ook hier bijkomende handelingen moet stellen om ze te doen vervolledigen. In dezelfde zin blijkt de toepassing van artikel 5 § 3 W.Beroepsorg. problematisch: het verzoek om bepaalde stukken niet ter inzage te geven van de verzoeker is zelden correct gemotiveerd of gaat uit van een overheid die hiertoe niet wettelijk bevoegd is, zodat de griffie ook hier soms bijkomende informatie moet inwinnen.[141]

Deze moeilijkheden brachten het Beroepsorgaan ertoe een schrijven te richten aan de verschillende veiligheidsoverheden aangaande de motivering van de beslissingen (en de kennisgeving ervan aan de betrokken personen), de samenstelling van de dossiers alsook (de motivering van) het verzoek om bepaalde stukken aan de inzage van de eisers te onttrekken. Het opzet van het Beroepsorgaan bestond erin om de wettelijke beginselen in herinnering te brengen aangaande de verschillende mogelijkheden (van verzoeken) tot embargo met betrekking tot gevoelige informatie, opdat de rechten van de verdediging zo goed als mogelijk kunnen worden gewaarborgd in deze complexe materie waarin soms belangen van nationale veiligheid op het spel staan. Desondanks had dit niet het gewenste effect bij alle veiligheidsoverheden. De inroeping van niet door de wet ingestelde motieven voor een inzage-embargo blijft problematisch. Ook houden een aantal veiligheidsoverheden er de visie op na dat geclassificeerde documenten enkel om deze reden niet kunnen worden ingezien door de eiser of zijn advocaat, hetgeen indruist tegen de geest en de letter van de wet. Verder moet worden vastgesteld dat de beslissingen van diverse veiligheidsoverheden niet getuigen van zorgvuldig-

140 Omwille van de zeer korte termijnen, is het beroep in deze gevallen dan ook vaak laattijdig en dus onontvankelijk.

141 Artikel 5 § 3 W.Beroepsorg. laat het Beroepsorgaan toe op verzoek van een inlichtingen- of politiedienst te beslissen om sommige stukken uit het onderzoeksdossier dat ter inzage van de eiser (of zijn advocaat), te halen. Dit is het geval indien de verspreiding ervan een gevaar zou inhouden voor de bescherming van de bronnen, de persoonlijke levenssfeer van derden of de vervulling van de wettelijke opdrachten van de inlichtingendiensten. Door middel van de Wet van 21 april 2016 (BS 29 april 2016) heeft de wetgever deze mogelijkheid uitgebreid door het Beroepsorgaan toe te laten, op verzoek van een betrokken dienst, stukken te verwijderen indien deze onder het geheim van een lopend opsporings- of gerechtelijk onderzoek vallen. Het Beroepsorgaan heeft de Voorzitter van het Vast Comité I, als Voorzitter van het Beroepsorgaan, gemandateerd om te oordelen over deze verzoeken. In uitzonderlijke gevallen, heeft de Voorzitter ambtshalve elementen die verband hielden met de persoonlijke levenssfeer van derden uit het dossier verwijderd. Het betrof gevallen waarin de betrokken dienst manifest nagelaten had zich te beroepen op art. 5 § 3 W.Beroepsorg.

heid en respect voor de beginselen van het administratief recht; zo zijn er beslissingen zonder enige motivering, ontbreken data en identiteit van de functionaris die de beslissing neemt…

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 (of twee) advoca(a)t(en) die ter zitting het standpunt van zijn/hun cliënt toelicht(en). 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.

De stijgende complexiteit van de dossiers en hun groeiend aantal (*infra*), hebben het Vast Comité I ertoe gebracht om begin 2017 zijn administratie te versterken. Er werd een jurist en een administratieve kracht aangeworven wat een belangrijke impact had op de middelen van het Comité.

X.2. EEN WETSONTWERP EN EEN ADVIES

X.2.1. HET WETSONTWERP

Diverse elementen leiden ertoe aan te mogen nemen dat de werklast van het Beroepsorgaan in de toekomst nog (gevoelig) zal toenemen. Na de aanslagen van Parijs en Brussel had de regering aangekondigd om de moraliteitsonderzoeken ('screenings') op te drijven, in het bijzonder met het oog op de verhoging van de veiligheid van kritieke infrastructuren.

Dit voornemen concretiseerde zich eind 2017 door de neerlegging van een wetsontwerp[142] met het oog op de wijziging van de W.C&VM. De Voorzitter van de Commissie Binnenlandse Zaken, Algemene Zaken en Openbaar Ambt verzocht de Voorzitter van het Vast Comité I hierover een advies uit te brengen.[143] De drie belangrijkste pijlers van het ontwerp worden hieronder samengevat.

142 *Parl. St.* Kamer 2017-2018, nr. 54K2767/001.
143 Het advies kan worden geconsulteerd op www.comiteri.be.

X.2.2. DE HOOFDLIJNEN VAN HET WETSONTWERP[144]

X.2.2.1. De bevoegdheid en de rol van de veiligheidsofficier

Het ontwerp beoogt in de eerste plaats een uitbreiding van de taken van de veiligheidsofficier in het kader van de veiligheidsverificaties (attesten en veiligheidsadviezen) en de verankering van deze functie in de schoot van het Openbaar Ministerie.

De veiligheidsofficier krijgt als nieuwe bevoegdheid toegewezen om '*te zorgen voor de inachtneming van de veiligheidsregels in het kader van een veiligheidsadvies of veiligheidsattest*' op het niveau van de betrokken privaat- en publiekrechtelijke rechtspersonen.

X.2.2.2. De hervorming van de procedure inzake veiligheidsadviezen

Het ontwerp beoogt ondermeer om de procedure inzake veiligheidsadviezen zowel op niveau van de reglementaire beslissing van de administratieve overheid als op het niveau van de individuele beslissing te hervormen.

Wat de reglementaire beslissing betreft, bepaalt de nieuwe procedure dat het de Koning toekomt te bepalen welke 'activiteitensectoren' onderworpen zijn aan de toepassing van de veiligheidsadviezen alsook de bevoegde (sectoriële) administratieve overheden aan te duiden.[145] Zowel privaatrechtelijke als publiekrechtelijke rechtspersonen die deel uitmaken van een betrokken activiteitensector, voeren vervolgens op vraag van de bevoegde administratieve overheid of op eigen initiatief, een 'risicoanalyse' uit die ze toezenden aan deze laatste. De administratieve overheid vraagt vervolgens een specifieke 'dreigingsanalyse' aan bij 'de bevoegde diensten'. Van zodra ze in het bezit is van deze analyse, stelt de bevoegde aministratieve overheid op haar beurt een 'impactanalyse' op. Deze beoogt het in kaart brengen van de mogelijke schade aan fundamentele staatsbelangen. Op basis van bovenvernoemde analyses, zendt de administratieve overheid een aanvraagdossier inzake een veiligheidsverificatie aan de NVO. De NVO beslist uiteindelijk of er al dan niet veiligheidsverificaties mogen worden uitgevoerd.

Wat de regeling voor de individuele beslissingen betreft, bepaalt het ontwerp dat de rechtspersonen de betrokkene op de hoogte moeten brengen van de verplichting om een veiligheidsverificatie te ondergaan. De veiligheidsofficier van rechtspersonen vraagt voorafgaand aan de veiligheidsverificatie, de instemming van de betrokkene. De veiligheidsofficier van de bevoegde administratieve

144 Het ontwerp werd begin 2018 aangenomen: Wet van 23 februari 2018 houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheids-machtigingen, veiligheidsattesten en veiligheidsadviezen (*BS* 1 juni 2018). Gezien voorliggend rapport 2017 behelst, werd de voorkeur gegeven aan het gebruik van de term 'ontwerp'.

145 Het betreft in deze een belangrijk verschil met de initiële regeling inzake veiligheidsadviezen waarbij 'een' (eender welke) administratieve overheid de procedure kon initiëren.

overheid waakt onder meer over de conformiteit van de verificatieverzoeken. Hij bezorgt deze op zijn beurt aan de NVO. De NVO doet binnen de opgelegde termijn (maximum één maand) uitspraak over de individuele aanvraag. Indien de NVO nalaat binnen deze termijn een veiligheidsadvies te formuleren, kan ze worden aangemaand om alsnog uitspraak te doen binnen een termijn die minstens even langs is dan de initieel voorgeschreven termijn. Gebeurt dit niet, wordt het advies geacht positief te zijn. Het ontwerp bepaalt dat het advies wordt toegekend voor een duur van maximaal vijf jaar[146], en dit onder voorbehoud van een ambtshalve herevaluatie door de NVO (op basis van nieuwe elementen). De administratieve overheid informeert de veiligheidsofficier van de werkgever over het veiligheidsadvies. Indien er een negatief veiligheidsadvies wordt verleend, wordt de betrokken persoon daarvan per aangetekende zending op de hoogte gebracht, met uitzondering van de motieven waarvan de verspreiding mogelijks schade zou kunnen toebrengen aan één van de fundamentele belangen zoals opgesomd in de wet, aan de bescherming van de bronnen, aan het geheim van een opsporings- of gerechtelijk onderzoek of aan de bescherming van de persoonlijke levenssfeer van derden.[147]

X.2.2.3. De inhoud van de veiligheidsverificatie

De laatste belangrijke pijler van het wetsontwerp bestaat erin om de bepalingen inzake de inhoud van de veiligheidsverificatie te wijzigen (art. 22*sexies* W.C&VM). Daarbij worden drie doelstellingen voor ogen gehouden.

Vooreerst is het de bedoeling om ook veiligheidsverificaties mogelijk te maken ten aanzien van minderjarigen. Verder wordt beoogd om, in het kader van veiligheidsverificaties van meerderjarigen, de tijdens hun minderjarigheid gepleegde feiten mee in rekening te nemen.

Daarnaast laat het ontwerp de politie- en inlichtingendiensten toe[148] gegevens op te vragen bij hun buitenlandse homologen wanneer de persoon voor wie de veiligheidsverificatie vereist is in het buitenland woont (of heeft gewoond), er op doorreis is geweest of er verbleven heeft.

Ten slotte breidt het ontwerp het aantal te bevragen gegevensbanken uit. Artikel 22*sexies* W.C&VM voorziet reeds in de consultatie en evaluatie van gerechtelijke gegevens[149], van informatie afkomstig van inlichitngendiensten, het centraal strafregister, het strafregister en de bevolkings- en vreemdelingregisters bijgehou-

---

146 Ook dit vormt een verschil met de actuele regeling die niet voorzag in een 'maximale' geldigheidstermijn. Verder moet tot op heden de uitvoering van de veiligheidsverificatie plaatsvinden 'voorafgaand' aan de toelating om een beroep, functie, opdracht of mandaat uit te oefenen. Het ontwerp introduceert de mogelijkheid om personen die reeds in functie zijn, aan een veiligheidsverificatie te onderwerpen.

147 Cf. art. 22, lid 5 W.C&VM (ongewijzigd).

148 De NVO beschikt momenteel reeds over deze bevoegdheid.

149 Overgezonden mits toelating van de bevoegde gerechtelijke overheden.

den op de gemeenten, het Rijksregister, het wachtregister van de vreemdelingen alsook de politiegegevens ter beschikking van politiefunctionarissen tijdens de uitvoering van identiteitscontroles. Het ontwerp voegt hieraan volgende gegevens toe: de gegevens en informatie uit de internationale politionele databanken voortvloeiend uit verdragen die België binden, de gegevens van administratieve politie, de gegevens uit gemeenschappelijke gegevensbanken en *'andere gegevens en informatie'*. Het ontwerp bepaalt dat het toereikend, ter zake en niet overmatig karakter van deze gegevens evenals de lijst ervan moeten worden bepaald bij Koninklijk besluit.[150]

X.2.3. HET ADVIES VAN HET VAST COMITÉ I[151]

In zijn advies onderlijnt het Comité het feit dat het ontwerp geen antwoord biedt op diverse problemen die het gevolg zijn van de toepassing van de actuele regelgeving (complexiteit, veel te korte beroepstermijnen…), en dit zowel voor de overheden, de betrokken burgers als het voor het Beroepsorgaan.

Eerder formuleerde het Comité voorstellen om sommige van deze problemen te verhelpen. Het Vast Comité I merkt dat het ontwerp deze problemen niet alleen onbehandeld liet, meer nog, het ontwerp creëerde bijkomende problemen voor alle actoren. Het Comité achtte het aangewezen om de twee wetten van 11 december 1998 (W.V&VM en W.Beroepsorg.) op een coherente wijze te hervormen.

X.3. GEDETAILLEERDE CIJFERS

In dit onderdeel 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 vijf jaar eveneens opgenomen.

In 2017 wordt de eerder vastgestelde verhoging bevestigd. Het aantal beroepen stijgt van 169 naar 192, het hoogste aantal ooit. De vastgestelde verhoging wordt in het bijzonder opgemerkt wat betreft het aantal beroepen ingediend tegen negatieve veiligheidsadviezen (van 101 naar 122). Dit werd ook in 2016 vastgesteld. Deze trend is eveneens merkbaar wat betreft het aantal beroepen ingediend tegen beslissingen waarbij een veiligheidsattest werd geweigerd of ingetrokken (van 18

150 Dit Koninklijk besluit verscheen in de loop van 2018: KB van 8 mei 2018 tot bepaling van de lijst van de gegevens en informatie die geraadpleegd kunnen worden in het kader van de uitvoering van een veiligheidsverificatie (*BS* 1 juni 2018).

151 Het advies kan worden geconsulteerd op www.comiteri.be.

naar 30), terwijl het aantal beroepen in het kader van een veiligheidsmachtiging, een tegenovergestelde beweging kent (van 50 naar 40).

Tabel 1. Betrokken veiligheidsoverheid

	2013	2014	2015	2016	2017
Nationale Veiligheidsoverheid	98	99	68	92	129
Veiligheid van de Staat	1	0	1	0	0
Algemene Dienst Inlichting en Veiligheid	78	60	47	68	53
Federaal Agentschap voor Nucleaire Controle	9	8	10	8	7
Federale Politie	1	3	3	1	3
Lokale Politie	2	1	1	0	0
Lokale Luchthavencommissie	–	–	–	–	–
TOTAAL	**189**	**171**	**130**	**169**	**192**

Tabel 2. Aard van de bestreden beslissing

	2013	2014	2015	2016	2017
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)					
Vertrouwelijk	5	5	9	5	1
Geheim	56	43	35	38	33
Zeer geheim	5	4	4	7	6
Weigering	41	25	36	28	30
Intrekking	5	9	7	9	7
Weigering en intrekking	4	0	0	0	0
Machtiging voor beperkte duur	1	2	3	4	1
Machtiging voor lager niveau	0	1	0	1	0
Geen beslissing binnen termijn	15	15	2	7	2
Geen beslissing binnen verlengde termijn	0	0	0	1	0

	2013	2014	2015	2016	2017
SUBTOTAAL VEILIGHEIDS-MACHTIGINGEN	**66**	**52**	**48**	**50**	**40**
Veiligheidsattesten toegang geclassificeerde zones (art. 22bis, al.1 W.C&VM)					
Weigering	0	4	6	1	3
Intrekkig	0	0	0	0	0
Geen beslissing binnen termijn	0	0	0	0	0
Veiligheidsattesten plaats of gebeurtenis (art. 22bis, al. 2 W.C&VM)					
Weigering	15	16	12	9	20
Intrekking	0	0	1	0	0
Geen beslissing binnen termijn	0	0	0	0	0
Veiligheidsattesten voor de nucleaire sector (art. 8bis, § 2 W.C&VM)					
Weigering	–	–	–	7	7
Intrekking	–	–	–	1	0
Geen beslissing binnen termijn	–	–	–	0	0
Veiligheidsadviezen (art. 22quinquies W.C&VM)					
Negatief advies	106	99	63	101	122
Geen advies	2	0	0	0	0
Herroeping van een positief advies	0	0	0	0	0
Normatieve rechtshandelingen (art. 12 W. Beroepsorg.)					
Beslissing van publieke overheid om attesten te eisen	0	0	0	0	0
Weigering NVO om verificaties voor attesten te verrichten	0	0	0	0	0
Beslissing van een administratieve overheid om adviezen te eisen	0	0	0	0	0
Weigering NVO om verificaties voor adviezen te verrichten	0	0	0	0	0
SUBTOTAAL ATTESTEN EN ADVIEZEN	**123**	**119**	**82**	**119**	**152**
TOTAAL BESTREDEN BESLISSINGEN	**189**	**171**	**130**	**169**	**192**

Tabel 3. Hoedanigheid van de verzoeker

	2013	2014	2015	2016	2017
Ambtenaar	4	0	4	2	4
Militair	26	17	29	23	20
Particulier	159	145	93	139	164
Rechtspersoon	0	6	4	5	4

Tabel 4. Taal van de verzoeker

	2013	2014	2015	2016	2017
Franstalig	92	92	75	99	115
Nederlandstalig	97	76	54	70	77
Duitstalig	0	0	0	0	0
Anderstalig	0	0	1	0	0

Tabel 5. Aard van de door het Beroepsorgaan genomen voorbereidende beslissingen[152]

	2013	2014	2015	2016	2017
Volledig dossier opvragen (1)	187	168	130	167	191
Aanvullende informatie opvragen (2)	12	16	7	23	36
Horen lid overheid (3)	3	11	7	10	0
Beslissing voorzitter (4)	0	0	0	0	0
Informatie uit dossier halen door Beroepsorgaan (5)	68	78	50	54	80[156]
Informatie uit dossier halen door inlichtingendienst (6)	0	0	0	0	0

(1) Het Beroepsorgaan beschikt over de mogelijkheid het gehele dossier bij de veiligheidsoverheden op te vragen. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan.

152 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 2017, terwijl de beslissing pas viel in 2018.

153 Zie hoger wat betreft art. 5 § 3 W.Beroepsorg. Het dient opgemerkt dat in vele gevallen het verzoek tot niet-inzage slechts gedeeltelijk werd ingewilligd (soms omwille van een gebrekkige motivering door de betrokken dienst).

(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 inlichtingen- of politiedienst hierom verzoekt, kan de voorzitter van het Beroepsorgaan beslissen dat bepaalde informatie uit het dossier dat aan de verzoeker ter inzage zal worden voorgelegd, wordt gehaald.[154]
(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	2016	2017
Dossierinzage door klager / advocaat	103	84	84	87	105
Horen van de klager / advocaat[158]	138	115	107	127	158

Tabel 7. Aard van de beslissingen van het Beroepsorgaan

	2013	2014	2015	2016	2017
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)					
Beroep onontvankelijk	2	0	4	0	3
Beroep zonder voorwerp	3	3	3	7	0
Beroep ongegrond	20	12	19	18	13
Beroep gegrond (volledige of gedeeltelijke toekenning)	35	14	24	24	24
Bijkomende onderzoeksdaden door overheid	0	0	0	2	0
Bijkomende termijn voor overheid	14	12	1	2	1
Zonder gevolg	0	0	1	0	0

154 Zie *supra* in verband met art. 5 § 3 W.Beroepsorg.
155 De W.Beroepsorg. regelt de bijstand door een advocaat tijdens de zitting, maar niet de vertegenwoordiging door deze laatste. In bepaalde dossiers wordt de klager (al dan niet bijgestaan door zijn advocaat) meermaals gehoord.

	2013	2014	2015	2016	2017
Veiligheidsattesten toegang geclassificeerde zones (art. 22bis, al. 1 W.C&VM)					
Beroep onontvankelijk	0	0	0	0	1
Beroep zonder voorwerp	0	0	0	0	1
Beroep ongegrond	0	2	4	1	0
Beroep gegrond (toekenning)	0	0	2	1	1
Veiligheidsattesten plaats of gebeurtenis (art. 22bis, al. 2 W.C&VM)					
Beroep onontvankelijk	1	0	0	0	1
Beroep zonder voorwerp	0	0	0	0	1
Beroep ongegrond	6	6	8	2	12
Beroep gegrond (toekenning)	11	8	10	4	7
Verleent akte van afstand van beroep	0	0	2	0	1
Veiligheidsattesten voor de nucleaire sector (art. 8bis § 2 W.C&VM)					
Beroep onontvankelijk	–	–	–	1	1
Beroep zonder voorwerp	–	–	–	1	0
Beroep ongegrond	–	–	–	0	1
Beroep gegrond (toekenning)	–	–	–	7	5
Veiligheidsadviezen (art. 22quinquies W.C&VM)					
Beroep onbevoegd	0	4	0	0	20[159]
Beroep onontvankelijk	4	4	6	15	10
Beroep zonder voorwerp	1	4	0	0	1
Bevestiging negatief advies	25	53	28	42	49
Omvorming in positief advies	65	41	23	46	41
Verleent akte van afstand van beroep	0	0	2	0	1
Beroep tegen normatieve rechtshandelingen (art. 12 W.Beroepsorg.)	0	0	0	0	0
TOTAAL	**187**	**163**	**137**	**173**	**195**

156 Het betreft in casu de beroepen ingediend tegen (negatieve) veiligheidsadviezen van de Nationale Veiligheidsoverheid met betrekking tot personeel van onderaannemers actief bij in België gevestigde Europese instellingen. Het Beroepsorgaan had beslist dat het ontbrak aan een wettelijke basis van de door de Nationale Veiligheidsoverheid geformuleerde adviezen. Bijgevolg verklaarde het Beroepsorgaan zich zonder rechtsmacht om te oordelen over de al dan niet gegrondheid van het veiligheidsadvies afgeleverd door de Nationale Veiligheidsoverheid.

HOOFDSTUK XI
DE INTERNE WERKING VAN HET VAST COMITÉ I

XI.1. SAMENSTELLING VAN HET VAST COMITÉ I

De samenstelling van het Comité bleef in 2017 ongewijzigd: Voorzitter Guy Rapaille (F), advocaat-generaal bij het hof van beroep te Luik en raadsheren Gérald Vande Walle (F)[157] en Pieter-Alexander De Brock (N).

Bij de Dienst Enquêtes I namen twee commissarissen-auditoren ontslag en werden respectievelijk in september en oktober 2017 vervangen. De dienst blijft daarmee bestaan 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), werd uitgebreid met een administratieve kracht voor het secretariaat en een jurist en kwam daardoor op een totaal van 18 administratieve personeelsleden.

XI.2. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE

In de loop van 2017 vonden twee 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. De dertien stemgerechtigde leden[158] van de commissie waren: Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Peter De Roover (N-VA), Laurette Onkelinx (PS), André Frédéric (PS), Denis Ducarme (MR), Phi-

157 Raadsheer Gérald Vande Walle bereikte op 31 december 2017 de pensioengerechtigde leeftijd en werd begin 2018 vervangen door Laurent Van Doren, hoofdcommissaris van politie.

158 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'*).

lippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld), Hans Bonte (sp.a), Gilles Vanden Burre (Ecolo-Groen) en Georges Dallemagne (cdH). De Commissie vergaderde onder het voorzitterschap van Kamervoorzitter Siegfried Bracke (N-VA). Negen van deze Volksvertegenwoordigers werden in april 2016 tevens benoemd als vast lid van de Parlementaire begeleidingscommissie 'Aanslagen'. Het accent van de parlementaire werkzaamheden lag bij de onderzoekscommissie (cf. Hoofdstuk V.1).

Tijdens de twee commissievergaderingen werden – achter gesloten deuren – de gemeenschappelijke toezichtonderzoeken van het Vast Comité I en het Vast Comité P, besproken. Ook was de bespreking van de door het Vast Comité I afgesloten onderzoeken aan de orde. In november 2017 werd het *Activiteitenverslag 2016* van het Vast Comité I besproken. De Commissie nam '*akte van het activiteitenverslag 2016 van het Comité I en verleent haar goedkeuring aan de aanbevelingen van het Comité*'.[159] Ten slotte werd tijd uitgetrokken voor de bespreking van het jaarlijkse verslag over de toepassing van de specifieke en uitzonderlijke methoden door de inlichtingendiensten en de controle door het Vast Comité I (art. 35 W.Toezicht).

XI.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 opstarten en bespreken van lopende gemeenschappelijke toezichtonderzoeken.

In 2017 waren twee gemeenschappelijke toezichtonderzoeken aan de orde: het naar aanleiding van de aanslagen in Parijs opgestarte onderzoek over de '*informatiepositie van het OCAD, voorafgaand aan 13 november 2015 's avonds, over de individuen of groepen die de aanslagen te Parijs hebben uitgevoerd of hierbij betrokken waren*' (cf. II.5) en een nieuw opgestart onderzoek naar de ondersteunende diensten van het OCAD (cf. II.6.4).

Verder werden uiteenlopende punten geagendeerd: de (mogelijke) aanpassing van het administratief statuut, de aanpak van het structureel begrotingsprobleem van alle dotatiegerichte instellingen en de mogelijke synergiën, de rol van beide

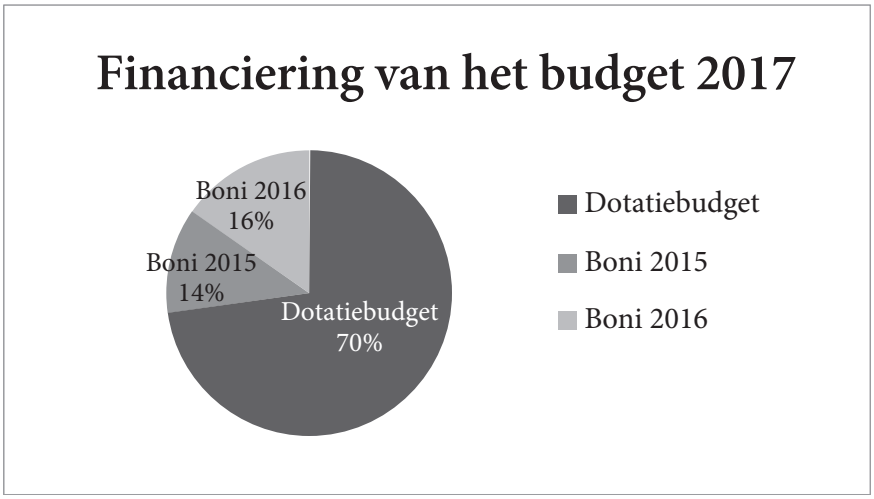
159 *Parl. St.* Kamer 2017-18, nr. 54K2734/001 (Activiteitenverslag 2016 van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, Verslag namens de Bijzondere commissie belat met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten).

Comités in relatie met de 'opvolgingscommissie' opgericht in het kader van de Onderzoekscommissie 'aanslagen', de opvolging van de ontwikkelingen in het kader van een nieuwe privacywetgeving… Ook was de voorbereiding van de organisatie van een viering naar aanleiding van het 25-jarig bestaan van beide Vaste Comités aan de orde en bleken beide comités het erover eens dat moet verder worden gewerkt aan een gemeenschappelijke methodologie, in de eerste plaats voor de gemeenschappelijke toezichtonderzoeken.

In 2017 vonden, naast informele contacten op de werkvloer, vier gemeenschappelijke vergaderingen plaats.

XI.4. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Het 'budget 2017' van het Vast Comité I werd vastgelegd op 3,635 miljoen euro, wat een vermindering inhield van 3,6% ten aanzien van het budget 2016. De financieringsbronnen van dit budget werden door de Kamer van Volksvertegenwoordigers[160] als volgt toegewezen:



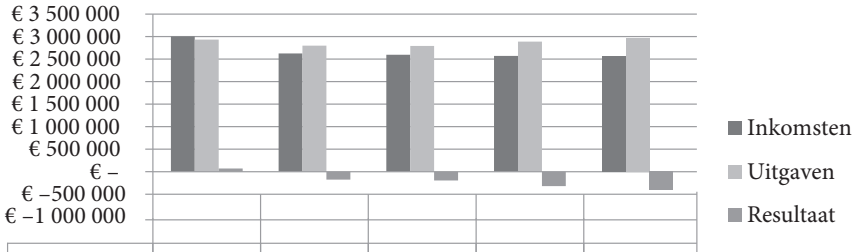
In het verlengde van de vorige begroting, is het Vast Comité I er opnieuw in geslaagd om zijn werkingsbudgetten in te perken, en dit niettegenstaande een moeilijke professionele context en het steeds in aantal toenemende wettelijke opdrachten. Desalniettemin kon het Comité in 2017 zijn administratieve staff met twee personeelsleden uitbreiden zonder daarbij de budgettaire enveloppe te overschrijden.

160 *Parl. St.* 2016-2017 Kamer, 54K2225/001, 20-22.

De uitvoering van het budget 2017 leverde een budgettaire bonus op van 0,698 miljoen euro, te weten het vastgestelde verschil tussen de inkomsten en de samengestelde uitgaven.

Zoals in 2016, leidt de financiële realiteit tot een veel minder gunstige vaststelling. Artikel 57, lid 1, W.Toezicht vermeldt dat de kredieten die noodzakelijk zijn voor de werking dienen te worden uitgetrokken op de begroting van de dotaties. Doch, zoals aangegeven door bovenstaande tabel, werd het 'budget 2017' gebaseerd op verschillende financieringsbronnen en staat de enige nieuwe bijdrage in termen van eigen beheer ingeschreven in de dotatie van de algemene uitgavenbegroting van de Staat.[161] Op het niveau van de bedrijfsresultaten vertaalt dit zich voor het Comité in een verlies van 0,372 miljoen euro (wat een stijging inhoudt van 16,87% tegenover de budgettaire oefening van 2016 (–0,318 miljoen euro)). Deze tendens wordt reeds enkele jaren vastgesteld en hypothekeert bij een ongewijzigd beleid op middellange termijn de kredietwaardigheid van het Comité.

Vast Comité I: Evolutie van de balans



	2013	2014	2015	2016	2017
Inkomsten	€ 3 005	€ 2 626	€ 2 597	€ 2 570	€ 2 565
Uitgaven	€ 2 935	€ 2 799	€ 2 792	€ 2 889	€ 2 937
Resultaat	€ 70.38	€ –173	€ –194	€ –318	€ –372

Nu de beslissing van de Ministerraad van 15 oktober 2014 bij aanvang van de legislatuur om het dotatiebudget jaarlijks lineair met 2% te verminderen van kracht blijft, wordt de belangrijkste determinant van de verhoging van de reële uitgaven zeer waarschijnlijk het aantal nieuwe wettelijke opdrachten die het Comité werd toegekend, en dit meer dan het fenomeen van de indexering. Zonder significante verhoging van de dotatie ingeschreven in de Staatsbegroting, zal de uitputting van de opgebouwde reserves de werking van het Comité – en dit zowel op operationeel als op financieel niveau – in gevaar brengen.[162]

---

161 Wet van 25 december 2016 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2017, *BS* 29 december 2016.

162 Ook andere dotatiegerechtige instellingen (het Vast Comité van Toezicht op de politiediensten, de Commissie voor de bescherming van de persoonlijke levenssfeer, het Controleorgaan

Evenwel werden, op initiatief van de Voorzitter van de Kamer van Volksvertegenwoordigers, synergieën tussen de verschillende dotatiegerechtigde instellingen bestudeerd die op sommige domeinen een effect resulteerden door een bundeling van de taken: deze aanpak laat toe om bijkomende beheerskosten voor sommige instellingen te vermijden, maar hebben een eerder marginale invloed in financieel opzicht. Wat ook het belang van dit voordeel mag zijn, is het van belang deze telkenmale aan te wenden als ook de voorbereidende studies de relevantie ervan hebben bewezen.

XI.5. EEN EXTERNE AUDIT BIJ ALLE DOTATIEGERECHTIGDE INSTELLINGEN

Op verzoek van de Commissie van de Comptabiliteit van de Kamer van Volksvertegenwoordigers startte het Rekenhof samen met Ernst and Young een onderzoek naar de dotatiegerechtigde instellingen, waaronder het Vast Comité I.

Het Rekenhof moest zich vooral richten op de budgettaire aspecten (een analyse van de inkomsten en uitgaven) en op de afbakening van de taken van de diverse instellingen. Ernst and Young kreeg als hoofdopdracht de processen, de systemen en de organisatie die in elk van deze instellingen aanwezig zijn, verder te analyseren.

Om deze werkzaamheden te kunnen uitvoeren, dienden de instellingen tal van documenten en informatie ter beschikking te stellen en een hele reeks van punctuele vragen te beantwoorden. Deze audit, die eind 2017 van start ging en waarvan de resultaten in het eerste trimester van 2018 bekend werden, bracht heel wat werk mee voor het Vast Comité I en dit bovenop de toegenomen werklast (*supra*).

XI.6. VORMING

Omwille van het belang voor de organisatie, moedigt het Vast Comité I zijn leden en medewerkers aan tot het volgen van algemene (informatica, management…) of sectoreigen opleidingen en conferenties.[163] Wat betreft deze laatste categorie werden onderstaande studiedagen door een of meerdere (personeels)leden van het Vast Comité I bijgewoond.

---

voor de politionele informatie, de Federale Ombudsman, de Hoge Raad voor de Justitie, de BIM-Commissie en de Verenigde benoemingscommissies voor het notariaat) kampen met hetzelfde probleem en delen dezelfde zienswsijze. Ze richtten in die zin in 2017 gezamenlijk een brief aan de Voorzitter van de Kamer van Volksvertegenwoordigers waarin ze hun bezorgdheid uitten over de verregaande gevolgen van de inperking van de financiële middelen (cf. Woord vooraf).

163 Er vonden ook interne opleidingen plaats, waaronder een aantal (door de medewerkers verplicht bij te wonen) veiligheidsbriefings alsook inlichtingengerelateerde opleidingen.

DATUM	TITEL	ORGANISATIE	PLAATS
25-27 januari 2017	The Age of Intelligence Machines	Computers, Privacy & Data Protection (CPDP)	Brussel
23 februari 2017	Third Expert Meeting – National Intelligence Authorities and Surveillance in the EU: Fundamental Rights and Surveillance	European Union Agency for Fundamental Rights (FRA)	Wenen
27 februari 2017	L'informateur de police: une production du renseignement entre fantasmes et réalités (La source)	Groupe de recherche METIS Renseignement	Parijs
22 maart 2017	Le contrôle et l'évaluation de la politique publique du renseignement	Délégation parlementaire au renseignement (DPR) et Commission nationale de contrôle des techniques de renseignement (CNCTR)	Parijs
31 maart 2017	Surveying Surveillance in the EU	RightsCon	Brussel
26-27 april 2017	Table ronde sur le cadre legal régissant les services de renseignement	Republiek Tunesië en Centre pour le contrôle démocratique des forces armées (DCAF)	Tunis
12 mei 2017	Managing uncertainties. De bescherming van kritische infrastructuren en de inlichtingendiensten	Belgian Intelligence Studies Centre (BISC)	Gent
12 mei 2017	Les métodes d'enquête pénale dans le domaine des nouvelles technologies	Centre de recherche information, droit et société (CRIDS)	Brussel
29 juni 2017	The Electromagnetic Attack	European Corporate Security Association (ECSA)	Brussel
12-13 september 2017	Information on Methods of Analysis Course	Belgian Intelligence Academy (BIA)	Heverlee
25 september 2017	Table ronde 'Que faire pour rendre le renseignement plus efficace encore dans la lutte contre le terrorisme'	Centre Com	Parijs
2 oktober 2017	Champs d'application des textes, principes de base et rôle de la CPVP	Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL)	Brussel
9 oktober 2017	Les obligations des responsables de traitements et des sous-traitants	Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL)	Brussel

DATUM	TITEL	ORGANISATIE	PLAATS
16 oktober 2017	Les obligations des responsables de traitements et des sous-traitants (suite); les flux transfrontalièrs et les droits des personnes concernées	Commissie voor de bescherming van de persoonlijke levenssfeer (CBPL)	Brussel
24 otober 2017	Cyberveiligheid en cyberdefensie: dreigingen, uitdagingen en strategische antwoorden	Royal Higher Institute for Defence and the Study Centre for Military Law and Law of War	Brussel
26-27 oktober 2017	Training on Monitoring Law Enforcement and Intelligence Services in Georgia – Status, Needs and International Best Practices	Democratic Centre for Armed Forces (DCAF) and the Public Defender of Georgia	Tbilissi
16-17 november 2017	Cybersécurité – Expériences internationales et Droits comparés	Republiek Tunesië en Centre pour le contrôle démocratique des forces armées (DCAF)	Tunis
30 november 2017	Cybersecurity framework in BEL Defence – Cyber Coalition 2017 – scenario overview and deployed CSOC visit	ADIV	Brussel
1 december 2017	Terrorisme Counter insurgency en de rol van de inlichtingendiensten	Belgian Intelligence Studies Centre (BISC)	Brussel
11 december 2017	Secret et publications: comment écrire sur les services de renseignement?	Groupe de recherche METIS Renseignement	Parijs

HOOFDSTUK XII
AANBEVELINGEN

Op basis van de in 2017 afgesloten toezichtonderzoeken, controles en inspecties 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 (XII.1), op de coördinatie en de efficiëntie van de inlichtingendiensten, het OCAD en de ondersteunende diensten (XII.2) en – ten slotte – op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I (XII.3).

XII.1. AANBEVELINGEN IN VERBAND MET DE BESCHERMING VAN DE RECHTEN DIE DE GRONDWET EN DE WET AAN PERSONEN WAARBORGEN

XII.1.1. ONDERZOEK NAAR HET STERK TOEGENOMEN AANTAL GEWONE IDENTIFICATIES[164]

Sinds de invoering van de versoepelde procedure ex artikel 16/2 W.I&V, waarbij bepaalde identificaties van communicaties niet langer als een specifieke methode worden beschouwd, is het aantal vorderingen tot identificaties aan operatoren zeer sterk gestegen. Vanuit zijn algemene toezichtsbevoegdheid beveelt het Comité de VSSE aan om intern te onderzoeken in welke mate dit hoge aantal vorderingen (mede) wordt veroorzaakt door het versoepelen van de procedure. Daarbij moet o.m. aandacht worden besteed aan de aard van dreigingen die de vorderingen rechtvaardigden en aan de vraag of en in welke mate dergelijke vorderingen gebeuren op verzoek van buitenlandse overheden/partnerdiensten.

164 Zie 'Hoofdstuk III. De controle op de bijzondere en bepaalde gewone inlichtingenmethoden'.

XII.1.2. GEDRAGSREGELS INZAKE CONTACTEN MET BURGERS[165]

Het Comité benadrukte dat inlichtingenagenten niet onterecht de indruk mogen wekken dat ze over bepaalde bevoegdheden of mogelijkheden beschikken. Verder moeten ze rekening houden met de wijze waarop personen die de werking van een inlichtingendienst niet kennen, een persoonlijke ontmoeting kunnen beleven. Het Comité beveelt aan dat de VSSE en de ADIV hiermee rekening houden in de opleiding, er in hun richtlijnen specifiek aandacht aan besteden en dat de inspecteurs bij het contact met externen zeer duidelijk uiteenzetten over welke bevoegdheden ze beschikken en wat de rechten en plichten van de aangesproken persoon zijn. De VSSE en de ADIV kunnen bepaalde instrumenten ontwerpen (bijv. een brochure over de dienst en haar bevoegdheden, een korte synopsis van de Inlichtingenwet) die – indien het geval zich daartoe leent – kunnen worden voorgelegd of afgegeven ter informatie van de betrokkene.

XII.1.3. HET BEROEPSGEHEIM IN RELATIE TOT INLICHTINGENDIENSTEN[166]

Artikel 16 W.I&V bepaalt sinds 2017 dat '*personen en organisaties die behoren tot de privésector […], onverminderd artikel 2, § 2, uit eigen beweging aan de inlichtingen- en veiligheidsdiensten de informatie en persoonsgegevens [kunnen] meedelen die nuttig zijn voor de uitvoering van hun opdrachten*.' Hierdoor zijn bepaalde beroepsbeoefenaars niet langer gehouden tot het op hen van toepassing zijnde beroepsgeheim in hun relatie tot de inlichtingendiensten. Het Comité beveelt echter aan dat de wetgever in deze bepaling expliciet zou vermelden in welke mate specifieke geheimhoudingsverplichtingen al dan niet gelden in relatie tot de VSSE en de ADIV.

XII.1.4. EEN MEER GEDETAILLEERD AFLUISTERPLAN[167]

Sinds enige tijd werkt de SIGINT-afdeling van de ADIV met 'projectfiches'. In deze fiches worden de te intercepteren organisaties en instellingen veel nader omschreven dan in het interceptieplan (bijv. aan de hand van selectoren). Op die wijze sluiten de fiches beter aan bij de wettelijke vereiste om een gemotiveerde lijst van instellingen en organisaties op te stellen. Naar het oordeel van het Comité

---

165 Zie 'Hoofdstuk II.2. Het mogelijks ongeoorloofd opvragen van bankverrichtingen en het beroepsgeheim'.

166 Zie 'Hoofdstuk II.2. Het mogelijks ongeoorloofd opvragen van bankverrichtingen en het beroepsgeheim'.

167 Zie 'Hoofdstuk IV. De controle op buitenlandse intercepties, beeldopnamen en IT-intrusies'.

moeten de actuele lijsten meer gedetailleerd worden. De ADIV beloofde vooruitgang te boeken op dat vlak, maar ze stelde dat ze niet in staat is om exhaustieve lijsten van targets aan te leveren.

XII.1.5. EEN WETTELIJKE BASIS VOOR DE NIEUWE GEMEENSCHAPPELIJKE GEGEVENSBANKEN[168]

Het Vast Comité I en het COC hadden in 2017 aanbevolen dat de nodige reglementaire besluiten zouden getroffen worden met betrekking tot de nieuwe gemeenschappelijke gegevensbanken in verband met haatpredikers en *homegrown terrorist fighters*. Bij Koninklijke besluiten van 23 april 2018[169] werd die verplichting nagekomen: de bestaande FTF-databank werd uitgebreid met *homegrown terrorist fighters* en er werd een tweede gegevensbank opgericht voor de haatpredikers. Echter, artikel 44/11/3*bis* van de Wet op het Politieambt bepaalt dat de bevoegde ministers voorafgaand aan de oprichting bij het COC en het Vast Comité I aangifte moeten doen van een gegevensbank en van de voorgenomen de verwerkingsmodaliteiten. Deze instellingen hebben vervolgens dertig dagen de tijd om hun advies te formuleren. Bij het afsluiten van voorliggend activiteitenverslag (midden 2018), vond echter nog geen aangifte plaats, ook al zijn beide gegevensbanken operationeel.

XII.1.6. DE AANSTELLING VAN EEN CONSULENT INZAKE VEILIGHEID EN BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER[170]

De gemeenschappelijke controle door het COC en het Vast Comité I van de FTF-databank bracht enkele problemen aan het licht zoals bijvoorbeeld het ontbreken van een controle van de wettelijkheid van de toegangen en van een mechanisme om veiligheidsincidenten te melden. Deze problemen konden mogelijks verklaard worden door het feit dat er in 2017 nog geen consulent inzake veiligheid en bescherming van de persoonlijke levenssfeer was aangesteld. Beide instellingen hadden daar nochtans regelmatig op aangedrongen. Het COC en het Comité

168 Zie 'Hoofdstuk VI. De controle van gemeenschappelijke gegevensbanken'.

169 K.B. 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1*bis* "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt; K.B. 23 april 2018 tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Foreign Terrorist Fighters en tot uitvoering van sommige bepalingen van de afdeling 1*bis* "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank Foreign Terrorist Fighters naar de gemeenschappelijke gegevensbank Terrorist Fighters.

170 Zie 'Hoofdstuk VI. De controle van gemeenschappelijke gegevensbanken'.

beveelden dan ook aan dat de bevoegde ministers zo spoedig mogelijk zouden overgaan tot de aanstelling van deze consulent.

XII.1.7. DE ROL VAN DE CONSULENTEN INZAKE VEILIGHEID EN BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER[171]

Het COC en het Vast Comité I bevelen aan dat de veiligheidsconsulenten van de diverse diensten die betrokken zijn bij de werking van de FTF-databank, op regelmatige basis en steekproefgewijs *loggings* opvragen bij de Federale Politie om zo een periodieke controle uit te oefenen op de wettigheid van de uitgevoerde raadplegingen. Tevens bevelen ze aan dat de validsatiesystemen periodiek zouden geëvalueerd worden, dat er initiatieven worden genomen inzake informatieveiligheid (controle van toegangen, vorming, sensibilisering…) en dat er een uitwisseling tot stand komt van *best practices*.

XII.2. AANBEVELINGEN IN VERBAND MET DE COÖRDINATIE EN DE EFFICIËNTIE VAN DE INLICHTINGENDIENSTEN, HET OCAD EN DE ONDERSTEUNENDE DIENSTEN

XII.2.1. RISICOANALYSE VOORAFGAAND AAN BUITENLANDSE MISSIES[172]

In het kader van het onderzoek naar de wijze waarop de ADIV een zending naar een conflictgebied had voorbereid waarbij contacten werden gelegd met een bepaalde organisatie, merkte het Vast Comité I op dat er geen geformaliseerde risicoanalyses (strategisch politiek-beleidsmatig noch operationeel) waren gemaakt. In de verschillende missiedocumenten kwamen wel risico-elementen aan bod, maar niet op gestructureerde en gesynthetiseerde wijze. Bij het opstarten van een operatie en vanzelfsprekend ook tijdens het verloop ervan, is het aangewezen dat er een gestructureerde, formele risicoanalyse wordt uitgevoerd door de ADIV. Dit laat toe dat de dienst en de minister, elk binnen hun bevoegdheid, alle relevante risico's oplijsten (ook deze op het vlak van de Belgische militaire- en buitenlandpolitiek), deze al dan niet te aanvaarden en in voorkomend geval risico-beperkende maatregelen te nemen (inclusief het voorbereiden van communicatie ingeval tijdens een operatie een voorzien risico zou bewaarheid worden).

171 Zie 'Hoofdstuk VI. De controle van gemeenschappelijke gegevensbanken'.
172 Zie Hoofdstuk 'II.1. Een klacht over drie operaties van de ADIV'.

XII.2.2. POLITIEKE DEKKING VOOR SAMENWERKINGSVERBANDEN[173]

In het kader van de internationale samenwerkingsverbanden die door de ADIV (maar ook door de VSSE) worden aangegaan, kunnen engagementen worden genomen of keuzes worden gemaakt die een politieke aftoetsing en dekking behoeven. Bij wijze van algemeen principe beval het Comité vroeger reeds aan dat de bevoegde ministers afdoende zouden worden geïnformeerd opdat zij in de mogelijkheid zouden zijn om ten aanzien van het Parlement hun politieke verantwoordelijkheid op te nemen.[174] Het Comité herhaalt deze aanbeveling en maakt deze concreter, door elementen mee te geven die criteria kunnen vormen om al dan niet te kunnen beoordelen of en wanneer de minister door de dienst moet worden geïnformeerd. Daarbij horen onder andere de vragen welk bureau de operatie uitvoert; waar een operatie zich voordoet (een conflictgebied of niet, Belgisch militair operatiegebied of niet); hoe groot de strategisch-beleidsmatige risico's (die op een structurele en formele manier zijn opgelijst) zijn; de internationale context; de vraag of er al dan niet een verband is met een gerechtelijk onderzoek; het gevaar op compromittering van de operatie… Deze opsomming is niet limitatief. Het komt de dienst en de minister toe om deze criteria zo nodig aan te vullen en verder uit te werken.

XII.2.3. INLICHTINGENBELEID TUSSEN DE ADIV EN DE VSSE AFSTEMMEN[175]

Het Comité beveelt aan dat, wanneer de twee Belgische inlichtingendiensten contacten onderhouden met buitenlandse diensten of *non-state actors*, ze met elkaar zouden overleggen om hun inlichtingenbeleid af te stemmen om op die wijze tot een coherent resultaat te komen. Het 'Nationaal Inlichtingenstuurplan' dat onder de verantwoordelijkheid van de Nationale Veiligheidsraad wordt opgesteld, kan hiertoe een nuttig kader bieden.

XII.2.4. HET BEHEER, DE OPSLAG EN DE MEDEDELING VAN INFORMATIE UIT DE FTF-DATABANK[176]

Er dient onderzocht te worden of het wenselijk is gevoelige politie-informatie (rapporten die de code 00 of 01 kregen) al dan niet in de FTF-databank op te

173 Zie Hoofdstuk 'II.1. Een klacht over drie operaties van de ADIV'.
174 VAST COMITÉ I, *Activiteitenverslag 2014*, 113-114.
175 Zie 'Hoofdstuk 'II.1. Een klacht over drie operaties van de ADIV'.
176 Zie 'Hoofdstuk VI. De controle van gemeenschappelijke gegevensbanken'.

nemen. Indien het antwoord negatief is, dient het wettelijk kader te worden aangepast.

Verder pleiten het COC en het Comité voor de ontwikkeling van informaticatoepassingen die de opvolging van de termijnen die gelden voor de bewaring van gegevens alsook de opvolging van de overzending van informatiekaarten naar de burgemeester, moeten vergemakkelijken.

Ten slotte wordt aanbevolen om de mededeling van (uittreksels van) informatiekaarten aan derden te beveiligen en aan een voorafgaande evaluatie te onderwerpen, waarbij aandacht moet besteed worden aan de beveiligingsmaatregelen die door die derden werden genomen.

XII.3. AANBEVELING IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

XII.3.1. TER BESCHIKKING STELLEN VAN INFORMATIE AAN HET VAST COMITÉ I[177]

Anders dan voor de inzet van bijzondere methoden, beschikt het Comité niet over de cijfers met betrekking tot de geviseerde dreiging en de te verdedigen belangen wat betreft de gewone methoden *ex* artikel 16/2 W.I&V. Het Comité beveelt de diensten aan ook deze gegevens te registreren en ter beschikking te stellen van het Vast Comité I.

XII.3.2. UITBREIDING VERSLAGGEVING PARLEMENT[178]

Bij Wet van 25 december 2016 (*BS* 25 januari 2017) werd de mogelijkheid ingebouwd voor de VSSE en de ADIV om toegang te krijgen tot informatie die berust bij de Passagiersinformatie-eenheid (art. 16/3 W.I&V). Het Comité wordt in kennis gesteld van deze methode en kan ze desgevallend verbieden. Anders dan voor artikel 16/2 W.I&V werd niet voorzien in een verplichte verslaggeving aan het Parlement; artikel 35 § 2 W.Toezicht werd immers niet aangepast.

Het Vast Comité I beveelt aan om dit alsnog te doen, temeer daar over het opvragen van vervoers- en reisgegevens op basis van artikel 18/6/1 W.I&V wél moet gerapporteerd worden omdat dit een specifieke methode vormt. Het Comité is overigens van oordeel dat dergelijke rapportage ook aangewezen is voor de bij Wet van 21 maart 2018 (*BS* 16 april 2018*)* ingevoerde mogelijkheid tot het gebruik van in databestanden opgeslagen camerabeelden (art. 16/4 W.I&V).

---

177 Zie 'Hoofdstuk III. De controle op de bijzondere en bepaalde gewone inlichtingen-methoden'.

178 Zie 'Hoofdstuk III. De controle op de bijzondere en bepaalde gewone inlichtingen-methoden'.

XII.3.3. INFORMATIEPLICHT IN HET KADER VAN UITZONDERLIJKE METHODEN[179]

Wat betreft de ADIV, benadrukt het Comité de naleving van de wettelijke verplichting om de BIM-Commissie tweewekelijks in te lichten over de uitvoering van de uitzonderlijke methoden (art. 18/10 § 1, derde lid W.I&V en art. 9 KB 12 oktober 2010).

XII.3.4. EEN INSTRUMENT VOOR DE CONTROLE VAN DE EVOLUTIE VAN DE INLICHTINGENFICHES IN DE FTF-DATABANK[180]

Met het oog op een adequate controle van de inlichtingenfiches in de FTF-databank, dringen het COC en het Vast Comité I aan op de ontwikkeling van een instrument dat moet toelaten kennis te nemen van alle verwerkingen uitgevoerd in een inlichtingenfiche. Ze verzoeken de Federale Politie om hiertoe, in zijn hoedanigheid van beheerder van de gegevensbank, de nodige stappen te zetten.

179 Zie 'Hoofdstuk III. De controle op de bijzondere en bepaalde gewone inlichtingen-methoden'.
180 Zie 'Hoofdstuk VI. De controle van gemeenschappelijke gegevensbanken'.

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 2017 TOT 31 DECEMBER 2017)

Wet 25 december 2016 betreffende de verwerking van passagiersgegevens, *BS* 25 januari 2017

Wet 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek, *BS* 28 april 2017

Wet 19 april 2017 tot wijziging van het Wetboek van Strafvordering, het Gerechtelijk Wetboek en de wet van 10 april 2014 tot wijziging van verschillende bepalingen met het oog op de oprichting van een nationaal register voor gerechtsdeskundigen en tot oprichting van een nationaal register van beëdigd vertalers, tolken en vertalers-tolken, welk ik u overmaak voor de bekendmaking ervan, *BS* 31 mei 2017

Wet 19 april 2017 tot wijziging van het Wetboek van Strafvordering, het Gerechtelijk Wetboek en de wet van 10 april 2014 tot wijziging van verschillende bepalingen met het oog op de oprichting van een nationaal register voor gerechtsdeskundigen en tot oprichting van een nationaal register van beëdigd vertalers, tolken en vertalers-tolken- Erratum, *BS* 12 juni 2017

Wet 31 juli 2017 houdende diverse bepalingen inzake elektronische communicatie, *BS* 12 september 2017

Wet 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, *BS* 31 oktober 2017

Wet 21 november 2017 houdende tweede aanpassing van de algemene uitgavenbegroting voor het begrotingsjaar 2017, *BS* 27 november 2017

Wet 9 december 2015 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, *BS* 30 november 2017

Wet 22 december 2017 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2018, *BS* 28 december 2017

K.B. 12 december 2016 houdende gedeeltelijke verdeling, betreffende de strijd tegen het terrorisme en het radicalisme van het provisioneel krediet ingeschreven in het programma 03-41-1 van de algemene uitgavenbegroting voor het begrotingsjaar 2016 bestemd tot het dekken van de uitgaven betreffende de versterking van de genomen

maatregelen alsook de nieuwe initiatieven inzake de strijd tegen het terrorisme en het radicalisme, *BS* 9 januari 2017

K.B. 14 december 2016 houdende gedeeltelijke verdeling, betreffende de strijd tegen het terrorisme en het radicalisme van het provisioneel krediet ingeschreven in het programma 03-41-1 van de algemene uitgavenbegroting voor het begrotingsjaar 2016 bestemd tot het dekken van de uitgaven betreffende de versterking van de genomen maatregelen alsook de nieuwe initiatieven inzake de strijd tegen het terrorisme en het radicalisme, *BS* 9 januari 2017

K.B. 20 december 2016 houdende gedeeltelijke verdeling, betreffende de strijd tegen het terrorisme en het radicalisme van het provisioneel krediet ingeschreven in het programma 03-41-1 van de algemene uitgavenbegroting voor het begrotingsjaar 2016 bestemd tot het dekken van de uitgaven betreffende de versterking van de genomen maatregelen alsook de nieuwe initiatieven inzake de strijd tegen het terrorisme en het radicalisme, *BS* 12 januari 2017

K.B. 16 februari 2017 houdende de procedure volgens dewelke de Koning kan overgaan tot erkenning van een daad van terrorisme in de zin van artikel 42*bis* van de wet van 1 augustus 1985, *BS* 3 maart 2017

K.B. 6 maart 2017 tot wijziging van het koninklijk besluit van 23 mei 2016 tot regeling van de overplaatsing van de beschermingsassistenten van de Veiligheid van de Staat naar de federale politie, *BS* 9 maart 2017

K.B. 19 maart 2017 tot vaststelling van de datum van inwerkingtreding van de artikelen 5 en 17 tot 23 van de wet van 21 april 2016 houdende diverse bepalingen Binnenlandse zaken – geïntegreerde politie, *BS 23* maart 2017

K.B. 12 maart 2017 tot vaststelling van de taalkaders voor de centrale diensten van de Veiligheid van de Staat, *BS 5* april 2017

K.B. 9 april 2017 tot wijziging van het koninklijk besluit van 3 juni 2007 betreffende de bewapening van de geïntegreerde politie, gestructureerd op twee niveaus alsook de bewapening van de leden van de diensten enquêtes bij de vaste comités P en I en van het personeel van de Algemene Inspectie van de federale politie en van de lokale politie, *BS 5* mei 2017

K.B. 21 december 2017 ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, houdende diverse bepalingen betreffende de Passagiersinformatie-eenheid en de functionaris voor de gegevensbescherming, *BS* 29 december 2017

M.B. 22 februari 2017 betreffende de bekwaamheidsproeven van bepaalde burgerlijke ambtenaren van het stafdepartement inlichtingen en veiligheid van de krijgsmacht, *BS* 16 maart 2017

M.B. 28 februari 2017 betreffende de vereisten inzake voortgezette vorming van bepaalde burgerlijke ambtenaren van het stafdepartement inlichtingen en veiligheid van de krijgsmacht, *BS* 17 maart 2017

M.B. 16 mei 2017 tot wijziging, wat betreft de Veiligheid van de Staat, van het ministerieel besluit van 25 oktober 2013 houdende interne organisatie, overdracht van bevoegdheid en machtigingen tot handtekening in de Federale Overheidsdienst Justitie inzake de gunning en de uitvoering van overheidsopdrachten voor aanneming van werken, leveringen en diensten, inzake toelagen en inzake diverse uitgaven, *BS* 14 juli 2017

Vergelijkende selectie van Nederlandstalige Cyber Security Experts (m/v/x) (niveau A2) voor het Ministerie van Landsverdediging, *BS* 15 maart 2017

Vergelijkende selectie van Nederlandstalige Cyber Risk Prevention Experts (m/v/x) (niveau A2) voor het Ministerie van Landsverdediging, *BS* 15 maart 2017

Resultaat van de vergelijkende Nederlandstalige selectie voor bevordering naar niveau A (reeks 3) voor het Ministerie van Landsverdediging attaché analist, *BS* 21 maart 2017

Vergelijkende selectie van Nederlandstalige Cyber Security Expert (m/v/x) (niveau A2) voor het Ministerie van Landsverdediging – erratum, *BS* 22 maart 2017

Vergelijkende selectie van Nederlandstalige Cyber Risk Prevention Expert (m/v/x) (niveau A2) voor het Ministerie van Landsverdediging – erratum, *BS* 22 maart 2017

Vergelijkende selectie van Nederlandstalige inspecteurs (m/v/x) (niveau B) voor het Ministerie van Landsverdediging, *BS* 24 maart 2017

Resultaat van de vergelijkende selectie van Nederlandstalige ICT – consultants (m/v/x) (niveau B), voor OCAD – FOD Binnenlandse Zaken, *BS* 9 juni 2017

Oproep tot kandidaten voor het mandaat van Franstalig lid van het Vast Comité van Toezicht op de inlichtingendiensten, *BS* 4 juli 2017

Nieuwe oproep tot kandidaten voor het mandaat van mannelijk Nederlandstalig lid van de lokale politie voor het Controleorgaan op de politionele informatie, *BS* 26 september 2017

Vergelijkende selectie van Franstalige Diensthoofd Budget en Boekhouding (m/v/x) (niveau A3) voor de Veiligheid van de Staat, *BS* 22 november 2017

Vergelijkende selectie van Nederlandstalige polyvalente medewerkers directiesecretariaat (m/v/x) (niveau B) (OCAD), voor de FOD Binnenlandse Zaken, *BS* 8 december 2017

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 2017 TOT 31 DECEMBER 2017)

Senaat

Voorstel van resolutie om opdracht te geven tot het instellen van een onderzoek naar wahabistische organisaties die actief zijn op ons grondgebied om te bepalen of ze schadelijke sektarische organisaties zijn, *Parl. St.* Senaat 2017-18, nr. 6-383/1

Kamer van Volksvertegenwoordigers

Parlementair onderzoek belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging, derde tussentijds verslag over het onderdeel 'veiligheidsarchitectuur', *Parl. St.* Kamer 2016-17, nrs. 54K1752/007 tot 54K1752/010

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, met het doel de bescherming van de openbare orde en de nationale veiligheid te versterken (2215/1-4), *Hand.* Kamer 2016-17, 9 februari 2017, CRIV54PLEN156, 49

Aangehouden amendementen en artikelen van het 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, met het doel de bescherming van de openbare orde en de nationale veiligheid te versterken (2215/1-5), *Hand.* Kamer 2016-17, 9 februari 2017, CRIV54PLEN157, 42

Wetsontwerp tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek, *Parl. St.* Kamer 2016-17, nrs. 54K2043/005 tot 54K2043/011 en *Hand.* Kamer 2016-17, 16 maart 2017, CRIV54PLEN161, 44

Voorstel van resolutie over de steun van België aan Tunesië (1427/1-6), *Hand.* Kamer 2016-17, 30 maart 2017, CRIV54PLEN163, 50

Wetsvoorstel betreffende de verwerking van persoonsgegevens door de Federale Overheidsdienst Justitie in het kader van de uitvoering van vrijheidsstraffen en vrijheidsbenemende maatregelen en van het beheer van de inrichtingen waar deze uitvoering plaatsvindt, *Parl. St.* Kamer 2016-17, nr. 54K2194/002

Wetsontwerp houdende vereenvoudiging, harmonisering, informatisering en modernisering van bepalingen van burgerlijk recht van burgerlijk procesrecht alsook van het notariaat, en houdende diverse bepalingen inzake justitie, *Parl. St.* Kamer 2016-17, nr. 54K2259/002

Wetsvoorstel betreffende de melding van veronderstelde integriteitsschending door leden van de geïntegreerde politie, *Parl. St.* Kamer 2016-17, nr. 54K2355/001

Voorstel van resolutie betreffende de schadelijke inmenging door bepaalde Golfstaten in de vrije uitoefening van de islamitische eredienst in België, *Parl. St.* Kamer 2016-17, nr. 54K2365/001

Wetsontwerp tot regeling van de private en bijzondere veiligheid, *Parl. St.* Kamer 2016-17, nrs. 54K2388/003, 54K2388/004, 54K2388/005 en 54K2388/007

Hoorzitting met Generaal Marc Compernol, Chef Defensie over de Strategische Visie voor Defensie — Horizon 2030, *Parl. St.* Kamer 2016-17, nr. 54K2392/001

Wetsontwerp tot wijziging van artikel 36*bis* van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *Parl. St.* Kamer 2016-17, nr. 54K2405/001

Wetsontwerp houdende eerste aanpassing van de algemene uitgavenbegroting voor het begrotingsjaar 2017, *Parl. St.* Kamer 2016-17, nr. 54K2411/001

Wetsvoorstel tot wijziging van het Wetboek van Strafvordering om de strijd tegen het terrorisme te bevorderen (2050/1-14) – Wetsvoorstel tot wijziging van de Organieke wet van 8 juli 1976 betreffende de openbare centra voor maatschappelijk welzijn om de strijd tegen terroristische misdrijven te bevorderen (1687/1-4), *Hand.* Kamer 2016-17, 4 mei 2017, CRIV54PLEN166, 66 en *Hand.* Kamer 2016-17, 4 mei 2017, CRIV54PLEN167, 24

Wetsvoorstel tot wijziging van artikel 134*quinquies* van de Nieuwe Gemeentewet, teneinde de burgemeester in de mogelijkheid te stellen inrichtingen te sluiten waarvan

vermoed wordt dat er terroristische activiteiten plaatsvinden (1473/1-12), *Hand.* Kamer 2016-17, 4 mei 2017, CRIV54PLEN167, 1

Wetsontwerp tot regeling van de private en bijzondere veiligheid (2388/1-6) – Wetsvoorstel tot wijziging van de wet van 10 april 1990 tot regeling van de private en bijzondere veiligheid wat de overname van politietaken betreft (675/1-3) – Wetsvoorstel tot wijziging van de wet van 10 april 1990 tot regeling van de private en bijzondere veiligheid wat betreft de uitoefeningsvoorwaarden voor functies binnen de private en bijzondere veiligheid (1829/1) – Wetsvoorstel tot wijziging van de wet van 10 april 1990 tot regeling van de private en bijzondere veiligheid wat de slotenmakerij betreft (2035/1), *Hand.* Kamer 2016-17, 8 juni 2017, CRIV54PLEN172, 95

De bestrijding van de illegale wapenhandel, hoorzittingen, *Parl. St.* Kamer 2016-17, nr. 54K2499/001

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – vervanging van een lid, *Hand.* Kamer 2016-17, 29 juni 2017, CRIV54PLEN177, 44

Wijzigingen van het statuut van de directeur-generaal en van de leden van de dienst enquêtes van het Vast Comité van Toezicht op de Politiediensten, *Parl. St.* Kamer 2016-17, nr. 54K2564/001 en *Hand.* Kamer 2016-17, 3 juli 2017, CRIV54PLEN178, 94

Wetsvoorstel betreffende het verbod op buitenlandse financiering van activiteiten die de vrije beleving van de eredienst in België belemmeren, *Parl. St.* Kamer 2016-17, nr. 54K2675/001

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – Vervanging van een lid – ingediende kandidaturen, *Hand.* Kamer 2016-17, 21 september 2017, CRIV54PLEN184, 64

Commentaar en opmerkingen bij de ontwerpen van Staatbegroting voor het begrotingsjaar 2018, *Parl. St.* Kamer 2017-18, nrs. 54K2689/003 tot 54K2689/005

Ontwerp van algemene uitgavenbegroting voor het begrotingsjaar 2018, *Parl. St.* Kamer 2017-18, nrs. 54K2690/001, 54K2690/005, 54K2690/011 en 54K2690/013

Verantwoording van de algemene uitgavenbegroting voor het begrotingsjaar 2018, *Parl. St.* Kamer 2017-18, nr. 54K2691/007

Algemene beleidsnota, *Parl. St.* Kamer 2017-18, nrs. 54K2708/005, 54K2708/008, 54K2708/009, 54K2708/017, 54K2708/2024 en 54K2708/2029

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – vervanging van een lid – hoorzitting van de kandidaten, *Hand.* Kamer 2017-18, 12 oktober 2017, CRIV54PLEN190, 11

Wetsontwerp tot wijziging van de wet van 8 juni 2006 houdende regeling van economische en individuele activiteiten met wapens, *Parl. St.* Kamer 2017-18, nr. 54K2709/001

Opvolgingscommissie, *Hand.* Kamer 2017-18, 9 november 2017, CRIV54PLEN195, 49

Activiteitenverslag 2016 van het vast comité van toezicht op de inlichtingen- en veiligheidsdiensten, *Parl. St.* Kamer 2017-18, nr. 54K2734/001

Wetsontwerp houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *Parl. St.* Kamer 2017-18, nrs. 54K2767/001 en 4K2767/002

Benoeming van een Franstalig effectief lid van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, *Parl. St.* Kamer 2017-18, nr. 54K2770/001

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – Benoeming van een Franstalig effectief lid, *Hand.* Kamer 2017-18, 16 november 2017, CRIV54PLEN197, 114

Rekenhof, Grondwettelijk hof, Hoge Raad voor de Justitie, Vast comité van toezicht op de politiediensten, Vast comité van toezicht op de inlichtingen- en veiligheidsdiensten, Federale ombudsmannen, Commissie voor de Bescherming van de persoonlijke levenssfeer, Benoemingscommissies voor het notariaat, Controleorgaan op de politionele informatie, BIM-Commissie, Federale Deontologische Commissie (rekeningen van het begrotingsjaar 2016, begrotingsaanpassingen van het begrotingsjaar 2017 en begrotingsvoorstellen voor het begrotingsjaar 2018), *Parl. St.* Kamer 2017-18, nrs. 54K2843/001 tot 54K2843/003

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 2017 TOT 31 DECEMBER 2017)

Senaat

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over de 'kinderen van Belgische Syriëstrijders – indoctrinatie door ISIS trauma's – risico's voor onze samenleving' (Senaat 2016-17, 8 mei 2017, Vr. nr. 6-1449)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over de 'minderjarige jihadisten – kindsoldaten – risico's voor onze samenleving – bevestigde gedetecteerde aanwezigheid tussen asielzoekers in ons land' (Senaat 2016-17, 12 september 2017, Vr. nr. 6-1541)

Schriftelijke vraag van M. Taelman aan de minister van Ontwikkelingssamenwerking over de 'cybercrime – e-mail spoofing – overheid – veiligheidsdiensten preventie' (Senaat 2017-18, 9 november 2017, Vr. nr. 6-1639)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Defensie over de 'Veiligheid van de Staat (VSSE) – Algemene Dienst Inlichting en Veiligheid (ADIV) – Social Media Intelligence (SOCMINT)' (Senaat 2017-18, 29 november 2017, Vr. nr. 6-1669)

Kamer van Volksvertegenwoordigers

Vraag van G. Gilkinet aan de minister van Justitie over de 'veiligheid van de ambtenaren van de FOD's' (*Vr. en Ant*. Kamer 2016-17, 10 januari 2017, QRVA 101, 199, Vr. nr. 980)

Vraag van B. Pas aan de minister van Justitie over 'de veiligheid van de ambtenaren van de FOD's' (*Vr. en Ant*. Kamer 2016-17, 10 januari 2017, QRVA 101, 204, Vr. nr. 1037)

Vraag van B. Pas aan de minister van Justitie over de 'maatregelen naar aanleiding van terrorisme – het opsluiten van jihadisten in de gevangenis' (*Vr. en Ant*. Kamer 2016-17, 10 januari 2017, QRVA 101, 210, Vr. nr. 1176)

Vraag van F. Dewinter aan de minister van Justitie over het 'personeel veiligheidsdiensten – Arabisch' (*Vr. en Ant*. Kamer 2016-17, 10 januari 2017, QRVA 101, 217, Vr. nr. 1211)

Vraag van D. Van der Maelen aan de minister van Justitie over 'de bevoegdheid van Britse inlichtingendiensten op Belgisch grondgebied' (*Vr. en Ant*. Kamer 2016-17, 10 januari 2017, QRVA 101, 224, Vr. nr. 1341)

Vraag van G. Dallemagne aan de minister van Justitie over de 'verdeling van de reeds vereffende provisie voor terreurbestrijding' (*Vr. en Ant.* Kamer 2016-17, 10 januari 2017, QRVA 101, 258, Vr. nr. 1521)

Vraag van B. Pas aan de minister van Mobiliteit over de 'luchthaven – veiligheidspersoneel – bagage- en onderhoudspersoneel' (*Vr. en Ant.* Kamer 2016-17, 10 januari 2017, QRVA 101, 322, Vr. nr. 1280)

Vraag van de F. Dewinter aan de minister van Justitie over 'de radicalisering in de gevangenissen (*Hand.* Kamer 2016-17, 12 januari 2017, CRIV54PLEN152, 20, Vr. nr. 1745)

Samengevoegde vragen van Ph. Blanchart en S. Lahaye-Battheu aan de minister van Binnenlandse Zaken over 'het eCallsysteem' (*Hand.* Kamer 2016-17, 18 januari 2017, CRIV54COM569, 7, Vr. nrs. 15733 en 15948)

Vraag van de R. Terwingen aan de minister van Justitie over 'de vraag van Vlaams minister Homans om adviezen van de Staatsveiligheid over de erkenning van moskeeën te kunnen inkijken' (*Hand.* Kamer 2016-17, 19 januari 2017, CRIV54PLEN153, 21, Vr. nr. 1761)

Vraag van H. Bonte aan de minister van Binnenlandse Zaken over de 'veiligheidsdiensten – de invulling van de kaders' (*Vr. en Ant.* Kamer 2016-17, 20 januari 2017, QRVA 102, 274, Vr. nr. 1537)

Vraag van F. Schepmans aan de minister van Binnenlandse Zaken over de 'Open Source and Social Media Collect and Analyse Tool – Federale Politie' (*Vr. en Ant.* Kamer 2016-17, 20 januari 2017, QRVA 102, 287, Vr. nr. 1645)

Vraag van D. Ducarme aan de minister van Buitenlandse Zaken over de 'intrekking van veiligheidsmachtigingen bij de Algemene Dienst Inlichting en Veiligheid (ADIV)' (*Vr. en Ant.* Kamer 2016-17, 20 januari 2017, QRVA 102, 374, Vr. nr. 750)

Vraag van K. Metsu aan de minister van Justitie over 'het bezoekrecht in de gevangenissen' (*Hand.* Kamer 2016-17, 25 januari 2017, CRIV54COM575, 1, Vr. nr. 15957)

Vraag van J.-M. Nollet aan de minister van Defensie over de 'Britse geheime diensten – verslagen van telefoontaps' (*Vr. en Ant.* Kamer 2016-17, 27 januari 2017, QRVA 103, 350, Vr. nr. 997)

Samengevoegde vragen van G. Grovonius en J.-J. Flahaux aan de eerste minister en de minister van Buitenlandse Zaken over 'Tunesië' (*Hand.* Kamer 2016-17, 8 februari 2017, CRIV54COM589, 15, Vr. nrs. 15837 en 16173)

Samengevoegde vragen van F. Dewinter, H. Bonte, G. Dallemagne, K. Metsu, Ph. Pivin, G. Vanden Burre, H. Vuye, A. Turtelboom en V. Yüksel aan de eerste minister over 'de antiterreurmaatregelen van de regering en het OCAD-verslag over het oprukkende wahabisme' (*Hand.* Kamer 2016-17, 9 februari 2017, CRIV54PLEN156, 16, Vr. nrs. 1828, 1822, 1823, 1829, 1830, 1831, 1824,1825 en 1826)

Vraag van B. Pas aan de minister van Justitie over de 'screening van haatpredikers' (*Vr. en Ant.* Kamer 2016-17, 17 februari 2017, QRVA 106, 177, Vr. nr. 1572)

Vraag van R. Hufkens aan de minister van Defensie over de 'pilootproject bewaking kazerne Heverlee' (*Vr. en Ant.* Kamer 2016-17, 17 februari 2017, QRVA 106, 363, Vr. nr. 1045)

Vraag van E. Kir aan de staatssecretaris voor Asiel en Migratie over 'de politiecontroles in het Noordstation in het kader van de strijd tegen het terrorisme' (*Hand.* Kamer 2016-17, 22 februari 2017, CRIV54COM604, 17, Vr. nr. 16450)

Vraag van F. Dewinter aan de minister van Justitie over 'Abdelhamid Abaoud – plannen Brussels Airport' (*Vr. en Ant.* Kamer 2016-17, 23 februari 2017, QRVA 107, 195, Vr. nr. 1206)

Vraag van S. Lahaye-Battheu aan de minister van Justitie over de 'Staatsveiligheid – opvolging sektes' (*Vr. en Ant.* Kamer 2016-17, 23 februari 2017, QRVA 107, 196, Vr. nr. 1350)

Vraag van B. Pas aan de minister van Justitie over 'databank "foreign terrorist fighters" – databank haatpredikers, ronselaars en eenzame wolven – toegang Vlaamse overheidsdiensten' (*Vr. en Ant.* Kamer 2016-17, 23 februari 2017, QRVA 107, 203, Vr. nr. 1389)

Vraag van B. Pas aan de minister van Justitie over 'het onder huisarrest plaatsen van haatpredikers' (*Vr. en Ant.* Kamer 2016-17, 23 februari 2017, QRVA 107, 209, Vr. nr. 1481)

Vraag van B. Hellings aan de minister van Justitie over 'VN-onderzoek – terbeschikkingstelling van de archieven van de Veiligheid van de Staat' (*Vr. en Ant.* Kamer 2016-17, 23 februari 2017, QRVA 107, 216, Vr. nr. 1548)

Vraag van N. Lijnen aan de minister van Defensie over de 'NAVO – Cyberaanvallen' (*Vr. en Ant.* Kamer 2016-17, 23 februari 2017, QRVA 107, 258, Vr. nr. 1031)

Vraag van S. Pirlot aan de minister van Defensie over de 'salafistische extremisten in het leger' (*Vr. en Ant.* Kamer 2016-17, 23 februari 2017, QRVA 107, 276, Vr. nr. 1056)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'visa voor bedienaars van de erediensten' (*Vr. en Ant.* Kamer 2016-17, 3 maart 2017, QRVA 108, 283, Vr. nr. 683)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over de 'asielzoekers – opvolging en screening' (*Vr. en Ant.* Kamer 2016-17, 3 maart 2017, QRVA 108, 296, Vr. nr. 618)

Vraag van G. Calomne aan de minister van Binnenlandse Zaken over 'de politiediensten die voor de veiligheid van de Brusselse stations en metro worden ingezet' (*Hand.* Kamer 2016-17, 8 maart 2017, CRIV54COM613, 1, Vr. nr. 17084)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over de 'duikers die met valse getuigschriften in de kerncentrale van Tihange werkten' (*Hand.* Kamer 2016-17, 8 maart 2017, CRIV54COM613, 29, Vr. nr. 17052)

Vraag van K. Jadin aan de minister van Mobiliteit over de 'afgedankte geradicaliseerde technicus' (*Vr. en Ant.* Kamer 2016-17, 10 maart 2017, QRVA 109, 317, Vr. nr. 2015)

Vraag van F. Demon aan de minister van Binnenlandse Zaken over 'de toenemende agressie tegen parkeerwachters' (*Hand.* Kamer 2016-17, 15 maart 2017, CRIV54COM621, 2, Vr. nr. 16957)

Vraag van E. Kir aan de minister van Binnenlandse Zaken over 'de repatriëring van een terreurverdachte naar Bagdad' (*Hand.* Kamer 2016-17, 15 maart 2017, CRIV54COM621, 6, Vr. nr. 17093)

Vraag van E. Kir aan de minister van Binnenlandse Zaken over 'de uitspraken van de minister in de pers in het kader van de strijd tegen terrorisme' (*Hand.* Kamer 2016-17, 15 maart 2017, CRIV54COM621, 31, Vr. nr. 17237)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over 'de situatie van de uit Irak en Syrië teruggekeerde Belgische strijders' (*Hand.* Kamer 2016-17, 16 maart 2017, CRIV54PLEN161, 13, Vr. nr. 1914)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over 'de aanslagen in Londen' (*Hand.* Kamer 2016-17, 23 maart 2017, CRIV54PLEN162, 40, Vr. nr. 1946)

Vraag van K. Metsu aan de minister van Justitie over de 'uitkeringen Syriëstrijders' (*Vr. en Ant.* Kamer 2016-17, 24 maart 2017, QRVA 111, 250, Vr. nr. 644)

Vraag van K. Metsu aan de minister van Justitie over de 'opvolging teruggekeerde Syriëstrijders en pogingen tot vertrek' (*Vr. en Ant.* Kamer 2016-17, 24 maart 2017, QRVA 111, 260, Vr. nr. 1226)

Vraag van A. Top aan de minister van Defensie over 'de kritiek van de Syrische president Bashar al-Assad' (*Hand.* Kamer 2016-17, 29 maart 2017, CRIV54COM632, 2, Vr. nr. 16561)

Samengevoegde vragen van G. Vanden Burre en W. Demeyer aan de minister van Justitie over 'de mogelijke aanslag die in Antwerpen werd verijdeld en de reactie van burgemeester Bart De Wever' (*Hand.* Kamer 2016-17, 29 maart 2017, CRIV54COM634, 24, Vr. nrs. 17514 en 17558)

Samengevoegde vragen van S. Van Hecke en A. Top aan de minister van Binnenlandse Zaken over 'de persconferentie van de Antwerpse burgemeester en korpschef tegen het advies van het federale parket in' (*Hand.* Kamer 2016-17, 30 maart 2017, CRIV54PLEN163, 16, Vr. nrs. 1957 tot 1959)

Vraag van Ph. Pivin aan de minister van Justitie over de 'inlichtingendiensten – informatie-uitwisseling met andere landen' (*Vr. en Ant.* Kamer 2016-17, 31 maart 2017, QRVA 112, 142, Vr. nr. 1051)

Vraag van C. Van Cauter aan de minister van Justitie over 'de adviezen van de Staatsveiligheid bij de erkenning van moskeeën' (*Vr. en Ant.* Kamer 2016-17, 31 maart 2017, QRVA 112, 169, Vr. nr. 1739)

Vraag van D. Ducarme aan de staatssecretaris voor Asiel en Migratie over de 'rekrutering van geradicaliseerden in Duitse asielcentra' (*Vr. en Ant.* Kamer 2016-17, 31 maart 2017, QRVA 112, 290, Vr. nr. 829)

Vraag van D. Ducarme aan de staatssecretaris voor Asiel en Migratie over de 'terrorismebestrijding – screening' (*Vr. en Ant.* Kamer 2016-17, 31 maart 2017, QRVA 112, 292, Vr. nr. 838)

Vraag van M. De Coninck aan de staatssecretaris voor Asiel en Migratie over 'de aanpak van Syriëstrijders' (*Vr. en Ant.* Kamer 2016-17, 31 maart 2017, QRVA 112, 319, Vr. nr. 913)

Vraag van W. De Vriendt aan de staatssecretaris voor Asiel en Migratie over de 'procedure medische regularisatie' (*Vr. en Ant.* Kamer 2016-17, 31 maart 2017, QRVA 112, 341, Vr. nr. 953)

Vraag van D. Ducarme aan de minister van Justitie over het 'implementatie van het protocol tot oprichting van de Belgian Intelligence Academy' (*Vr. en Ant.* Kamer 2016-17, 7 april 2017, QRVA 113, 171, Vr. nr. 1362)

Vraag van J.-M. Nollet aan de minister van Justitie over de 'onderzoek van de Veiligheid van de Staat in bedrijven' (*Vr. en Ant.* Kamer 2016-17, 7 april 2017, QRVA 113, 176, Vr. nr. 1608)

Vraag van B. Pas aan de minister van Justitie over 'de activiteiten van de radicaalislamitische groepering Hizb ut-Tahrir' (*Vr. en Ant.* Kamer 2016-17, 7 april 2017, QRVA 113, 177, Vr. nr. 1573)

Vraag van B. Pas aan de minister van Justitie over de 'terrorisme – minderjarigen' (*Vr. en Ant.* Kamer 2016-17, 7 april 2017, QRVA 113, 186, Vr. nr. 1706)

Vraag van B. Pas aan de minister van Justitie over de 'humanitaire organisaties en ontwikkelingssamenwerking als dekmantel voor islamextremisme en terrorisme' (*Vr. en Ant.* Kamer 2016-17, 7 april 2017, QRVA 113, 189, Vr. nr. 1747)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken, over de 'minderjarigen die geplaatst worden wegens banden met terroristische milieus' (*Vr. en Ant.* Kamer 2016-17, 24 april 2017, QRVA 115, 110, Vr. nr. 1867)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'deradicalisering' (*Vr. en Ant.* Kamer 2016-17, 24 april 2017, QRVA 115, 128, Vr. nr. 1887)

Vraag van B. Pas aan de minister van Justitie over de 'maatregelen naar aanleiding van terrorisme – screening predikers' (*Vr. en Ant.* Kamer 2016-17, 24 april 2017, QRVA 115, 177, Vr. nr. 1172)

Vraag van K. Metsu aan de minister van Justitie over de 'imams in België' (*Vr. en Ant.* Kamer 2016-17, 24 april 2017, QRVA 115, 180, Vr. nr. 1410)

Vraag van G. Dallemagne aan de minister van Justitie over de 'transfers van buitenlandse fondsen naar moskeeën in België – werkzaamheden van de CFI' (*Vr. en Ant.* Kamer 2016-17, 24 april 2017, QRVA 115, 183, Vr. nr. 1465)

Vraag van B. Pas aan de minister van Justitie over 'de haatprediker Hamzat Chumakov' (*Vr. en Ant.* Kamer 2016-17, 24 april 2017, QRVA 115, 191, Vr. nr. 1568)

Vraag van B. Pas aan de minister van Justitie over 'financiering van terrorisme' (*Vr. en Ant.* Kamer 2016-17, 24 april 2017, QRVA 115, 211, Vr. nr. 1673)

Vraag van B. Pas aan de staatssecretaris voor Asiel en Migratie over 'de uitreiking van visa aan imams' (*Vr. en Ant.* Kamer 2016-17, 24 april 2017, QRVA 115, 394, Vr. nr. 680)

Vraag van O. Maingain aan de minister van Buitenlandse Zaken over 'de spionageactiviteiten van de Turkse ambassade ten aanzien van de Turken in ons land' (*Hand.* Kamer 2016-17, 26 april 2017, CRIV54COM648, 15, Vr. nr. 17764)

Vraag van M. De Coninck aan de staatssecretaris voor Asiel en Migratie over 'visa voor imams' (*Hand.* Kamer 2016-17, 3 mei 2017, CRIV54COM651, 35, Vr. nr. 17921)

Vraag van A. Top aan de minister van Mobiliteit over 'de antiterrorismeplannen voor de Brusselse stations' (*Hand.* Kamer 2016-17, 3 mei 2017, CRIV54COM655, 8, Vr. nr. 17826)

Vraag van W. De Vriendt aan de minister van Defensie over 'de operatie "Vigilant Guardian"' (*Vr. en Ant.* Kamer 2016-17, 5 mei 2017, QRVA 116, 446, Vr. nr. 1117)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'federale en lokale politie – evolutie' (*Vr. en Ant.* Kamer 2016-17, 16 mei 2017, QRVA 117, 132, Vr. nr. 1291)

Vraag van K. Lalieux aan de minister van Binnenlandse Zaken over de 'veiligheid in het openbaar vervoer' (*Vr. en Ant.* Kamer 2016-17, 16 mei 2017, QRVA 117, 150, Vr. nr. 1921)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'stroomstootwapens voor de lokale politie' (*Vr. en Ant.* Kamer 2016-17, 16 mei 2017, QRVA 117, 173, Vr. nr. 2024)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over het 'gebruik van tasers' (*Vr. en Ant.* Kamer 2016-17, 16 mei 2017, QRVA 117, 184, Vr. nr. 2058)

Vraag van E. Kir aan de minister van Binnenlandse Zaken over het 'Noordstation – politiecontroles in het kader van de terreurbestrijding' (*Vr. en Ant.* Kamer 2016-17, 16 mei 2017, QRVA 117, 241, Vr. nr. 2145)

Vraag van Ph. Goffin aan de minister van Justitie over de 'islamconsulenten in de gevangenissen' (*Vr. en Ant.* Kamer 2016-17, 16 mei 2017, QRVA 117, 306, Vr. nr. 208)

Vraag van B. Pas aan de staatssecretaris voor Asiel en Migratie over de 'haatpredikers' (*Vr. en Ant.* Kamer 2016-17, 16 mei 2017, QRVA 117, 456, Vr. nr. 897)

Samengevoegde vragen van R. Hedebouw, B. Pas, V. Caprasse en W. De Vriendt aan de eerste minister over 'het inzetten van politieagenten voor de NAVO-top en het bezoek van president Trump en president Erdogan aan België' (*Hand.* Kamer 2016-17, 18 mei 2017, CRIV54PLEN169, 1, Vr. nrs. 2056, 2057, 2072 en 2059)

Gedachtewisseling en samengevoegde vragen van R. Hedebouw, W. De Vriendt, P. Pirlot, V. Yüksel, A. Capoen, S. Crusnière en G. Dallemagne aan de minister van Buitenlandse Zaken over 'de Navo Top van 25 mei 2017 te Brussel' (*Hand.* Kamer 2016-17, 23 mei 2017, CRIV54COM670, 1, Vr. nrs. 18244, 18437, 18439, 18441, 18589, 18602, 18677, 18683 en 18748)

Samengevoegde vragen van A. Carcaci, G. Dallemagne en D. Ducarme aan de minister van Binnenlandse Zaken over 'het verschijnsel van de radicalisering en de aanslag in Manchester' (*Hand.* Kamer 2016-17, 24 mei 2017, CRIV54PLEN170, 6, Vr. nrs. 2080, 2081 en 2082)

Vraag van A. Lambrecht aan de minister van Justitie over 'de erkenning van moskeeën' (*Hand.* Kamer 2016-17, 30 mei 2017, CRIV54COM677, 20, Vr. nr. 18513)

Vraag van I. De Coninck aan de minister van Mobiliteit over 'de afgeschafte treinen' (*Vr. en Ant*. Kamer 2016-17, 30 mei 2017, QRVA 119, 177, Vr. nr. 2002)

Vraag van A. Lambrecht aan de minister van Justitie over 'het overleg over de erkenning van moskeeën' (*Hand.* Kamer 2016-17, 7 juni 2017, CRIV54COM681, 18, Vr. nr. 18998)

Samengevoegde vragen van O. Maingain en Ph. Blanchart aan de minister van Binnenlandse Zaken over 'de veiligheid van de scholen die geacht worden banden te hebben met de Gülenbeweging' (*Hand.* Kamer 2016-17, 7 juni 2017, CRIV54COM684, 4, Vr. nrs. 17765 en 18321)

Samengevoegde vragen van B. Vermeulen, K. Jadin, H. Bonte en S. Lahaye-Battheu aan de minister van Binnenlandse Zaken over 'de Lokale Integrale Veiligheidscellen en de lokale taskforces' (*Hand.* Kamer 2016-17, 7 juni 2017, CRIV54COM684, 18, Vr. nrs. 18182, 18889, 18969 en 19107)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over het 'OCAD – jacht op extremisten' (*Vr. en Ant.* Kamer 2016-17, 7 juni 2017, QRVA 120, 160, Vr. nr. 1964)

Vraag van F. Schepmans aan de minister van Binnenlandse Zaken over de 'veiligheidsmaatregelen in de luchthavens' (*Vr. en Ant.* Kamer 2016-17, 7 juni 2017, QRVA 120, 210, Vr. nr. 2165)

Vraag van F. Dewinter aan minister van Binnenlandse Zaken over 'de link tussen de aanslag in Manchester en België' (*Hand.* Kamer 2016-17, 8 juni 2017, CRIV54PLEN172, 29, Vr. nr. 2125)

Samengevoegde vragen van A. Carcaci en Ph. Pivin aan de minister van Binnenlandse Zaken over 'de boodschap waarin Islamitische Staat België bedreigt' (*Hand.* Kamer 2016-17, 8 juni 2017, CRIV54PLEN172, 32, Vr. nrs. 2126 en 2127)

Samengevoegde vragen van K. Jadin, P. Buysrogge, A. Top en G. Calomne aan de minister van Defensie over 'de diensten voor cyberveiligheid van Defensie' (*Hand.* Kamer 2016-17, 14 juni 2017, CRIV54COM687, 2, Vr. nrs. 18203, 18606, 19024 en 19163)

Vraag van K. Jadin aan de minister van Defensie over 'de munitie- en wapentests in het kamp Elsenborn' (*Hand.* Kamer 2016-17, 14 juni 2017, CRIV54COM687, 10, Vr. nr. 18193)

Samengevoegde vragen van K. Jadin en V. Yüksel aan de minister van Defensie over de 'tekenen van radicalisering in kazernes' (*Hand.* Kamer 2016-17, 14 juni 2017, CRIV-54COM687, 14, Vr. nrs. 18655 en 19222)

Samengevoegde interpellatie en vraag van G. Calomne en S. Crusnière aan de minister van Binnenlandse Zaken over 'de identiteitskaart met vingerafdruk' (*Hand.* Kamer 2016-17, 14 juni 2017, CRIV54COM688, 14, Vr. nrs. 18737 en 224)

Vragen van E. Kir aan de minister van Binnenlandse Zaken over 'het dreigingsniveau na de aanslagen in Londen' (*Hand.* Kamer 2016-17, 14 juni 2017, CRIV54COM688, 33, Vr. nr. 19082)

Vraag van F. Schepmans aan de minister van Binnenlandse Zaken over de 'antiterreuroefeningen' (*Vr. en Ant.* Kamer 2016-17, 20 juni 2017, QRVA 122, 139, Vr. nr. 1740)

Vraag van E. Burton aan de minister van Binnenlandse Zaken over de 'uitbouw van de LIVC's in de gemeenten' (*Vr. en Ant.* Kamer 2016-17, 20 juni 2017, QRVA 122, 163, Vr. nr. 2181)

Vraag van F. Schepmans aan de minister van Justitie over de 'samenwerking tussen het EU INTCEN en de Veiligheid van de Staat' (*Vr. en Ant.* Kamer 2016-17, 20 juni 2017, QRVA 122, 187, Vr. nr. 871)

Vraag van B. Pas aan de minister van Justitie over de 'islamconsulenten in de gevangenissen' (*Vr. en Ant.* Kamer 2016-17, 20 juni 2017, QRVA 122, 189, Vr. nr. 985)

Vraag van F. Dewinter aan de minister van Justitie over de 'inlichtingendiensten – dataverwerking' (*Vr. en Ant.* Kamer 2016-17, 20 juni 2017, QRVA 122, 192, Vr. nr. 1191)

Vraag van S. de Coster-Bauchau aan de minister van Justitie over de 'Veiligheid van de Staat – aanwerving agenten' (*Vr. en Ant.* Kamer 2016-17, 20 juni 2017, QRVA 122, 205, Vr. nr. 1799)

Vraag van F. Dewinter aan de minister van Justitie over 'de screening van kandidaat-asielzoekers op IS-strijders' (*Vr. en Ant.* Kamer 2016-17, 20 juni 2017, QRVA 122, 207, Vr. nr. 1831)

Samengevoegde vragen van R. Terwingen en K. Jadin aan de minister van Binnenlandse Zaken over 'de LIVC's in de opvolging van het radicalisme' (*Hand.* Kamer 2016-17, 21 juni 2017, CRIV54COM694, 6, Vr. nrs. 19143 en 19217)

Samengevoegde vragen van B. Pas, G. Dallemagne, K. Degroote, Ph. Pivin, H. Vuye, S. Van Hecke, H. Bonte, A. Frédéric, S. Verherstraeten en P. Dewael aan de eerste minister over 'de mislukte terreurdaad in Brussel-Centraal' (*Hand.* Kamer 2016-17, 22 juni 2017, CRIV54PLEN174, 1, Vr. nrs. 2158 tot 2167)

Vraag van E. Kir aan de minister van Binnenlandse Zaken over 'de Algemene Nationale Gegevensbank – Registreren van Belgische onderdanen' (*Vr. en Ant.* Kamer 2016-17, 27 juni 2017, QRVA 123, 174, Vr. nr. 2247)

Vraag van E. Van Hoof aan de minister van Binnenlandse Zaken over 'de meldingen van discriminatie bij het IGVM' (*Hand.* Kamer 2016-17, 4 juli 2017, CRIV54COM700, 1, Vr. nr. 19034)

Samengevoegde vragen van G. Dallemagne, K. Degroote en R. Miller aan de eerste minister over 'de dreigende terroristische aanslag' (*Hand.* Kamer 2016-17, 6 juli 2017, CRIV54PLEN178, 1, Vr. nrs. 2201 tot 2203)

Vraag van G. Calomne aan de minister van Binnenlandse Zaken over de 'bescherming van buitenlandse diplomatieke vertegenwoordigingen' (*Vr. en Ant.* Kamer 2016-17, 7 juli 2017, QRVA 124, 196, Vr. nr. 2255)

Samengevoegde vragen van Ph. Pivin aan de minister van Binnenlandse Zaken over 'de samenwerking met de deelgebieden in het kader van de strijd tegen radicalisering' (*Hand.* Kamer 2016-17, 12 juli 2017, CRIV54COM714, 5, Vr. nrs. 19295 en 19870)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over 'de toepassing door de veiligheidsdiensten van een standaardmodel voor de objectivering van radi-

caliseringsprocessen' (*Hand.* Kamer 2016-17, 12 juli 2017, CRIV54COM712, 20, Vr. nr. 19621)

Vraag van V. Yüksel aan de minister van Binnenlandse Zaken over 'de actualisatie van de OCAD-lijst' (*Hand.* Kamer 2016-17, 12 juli 2017, CRIV54COM712, 36, Vr. nr. 19843)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'radicalisering en indoctrinatie via internet en sociale netwerken' (*Hand.* Kamer 2016-17, 12 juli 2017, CRIV54COM712, 46, Vr. nr. 19866)

Samengevoegde vragen van J. Van den Bergh, D. Geerts en K. Jadin aan de minister van Mobiliteit over 'de reizigerscontrole op internationale treinen' (*Hand.* Kamer 2016-17, 12 juli 2017, CRIV54COM714, 1, Vr. nrs. 18790, 18797 en 18874)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'de Lokale Integrale Veiligheidscellen' (*Vr. en Ant.* Kamer 2016-17, 14 juli 2017, QRVA 125, 139, Vr. nr. 2157)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'oprichting van een Belgische cel in Turkije' (*Vr. en Ant.* Kamer 2016-17, 14 juli 2017, QRVA 125, 162, Vr. nr. 2302)

Vraag van K. Jadin aan de minister van Werk over de 'werkloosheidsuitkeringen van personen die gelinkt worden aan terroristische activiteiten' (*Vr. en Ant.* Kamer 2016-17, 27 juli 2017, QRVA 126, 202, Vr. nr. 934)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'persoonsbescherming' (*Vr. en Ant.* Kamer 2016-17, 27 juli 2017, QRVA 126, 153, Vr. nr. 2294)

Vraag van B. Pas aan de minister van Justitie over het 'aantal verijdelde aanslagen' (*Vr. en Ant.* Kamer 2016-17, 27 juli 2017, QRVA 126, 360, Vr. nr. 1590)

Vraag van B. Pas aan de minister van Justitie over de 'buitenlandse financiering van moskeeën' (*Vr. en Ant.* Kamer 2016-17, 27 juli 2017, QRVA 126, 363, Vr. nr. 1633)

Vraag van Ph. Pivin aan de minister van Justitie over het 'beheer en controle van gebedshuizen' (*Vr. en Ant.* Kamer 2016-17, 27 juli 2017, QRVA 126, 368, Vr. nr. 1735)

Vraag van K. Van Vaerenbergh aan de minister van Justitie over de 'gevangenissen – maatregelen tegen radicalisme' (*Vr. en Ant.* Kamer 2016-17, 27 juli 2017, QRVA 126, 376, Vr. nr. 1856)

Vraag van A. Frédéric aan de minister van Justitie over de 'gedetacheerd personeel op het kabinet' (*Vr. en Ant.* Kamer 2016-17, 27 juli 2017, QRVA 126, 387, Vr. nr. 1880)

Vraag van M. Van Hees aan de minister van Defensie over de 'resultaten van de NAVO-top' (*Vr. en Ant.* Kamer 2016-17, 27 juli 2017, QRVA 126, 490, Vr. nr. 1225)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over de 'terugkerende Syriëstrijders of leden van gewelddadige islamitische organisaties actief in het Midden-Oosten' (*Vr. en Ant.* Kamer 2016-17, 16 augustus 2017, QRVA 127, 221, Vr. nr. 2026)

Vraag van D. Ducarme aan de minister van Justitie over de 'opvolging van teruggekeerde Syriëstrijders en van personen die er niet in slaagden Syrië te bereiken' (*Vr. en Ant.* Kamer 2016-17, 16 augustus 2017, QRVA 127, 260, Vr. nr. 930)

Vraag van E. Kir aan de minister van Justitie over de 'uitspraken van de minister van Binnenlandse Zaken in de pers in het kader van de terrorismebestrijding' (*Vr. en Ant.* Kamer 2016-17, 16 augustus 2017, QRVA 127, 296, Vr. nr. 1873)

Vraag van L. Onkelinx aan de minister van Justitie over de 'begrotingscontrole – Middelen van de Veiligheid van de Staat' (*Vr. en Ant.* Kamer 2016-17, 16 augustus 2017, QRVA 127, 296, Vr. nr. 1982)

Vraag van S. de Coster-Bauchau aan de minister van Binnenlandse Zaken over de 'betonblokken om aanslagen met vrachtwagens te voorkomen' (*Vr. en Ant.* Kamer 2016-17, 23 augustus 2017, QRVA 128, 245, Vr. nr. 2338)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over de 'beveiliging van voor het publiek toegankelijke privé-evenementen' (*Vr. en Ant.* Kamer 2016-17, 23 augustus 2017, QRVA 128, 170, Vr. nr. 2159)

Vraag van Ph. Pivin aan de minister van Werk over de 'controle op het verkoopverbod voor grondstoffen voor TATP' (*Vr. en Ant.* Kamer 2016-17, 4 september 2017, QRVA 129, 160, Vr. nr. 1599)

Vraag van Ph. Blanchart aan de minister van Binnenlandse Zaken over de 'situatie van scholen waarvan verondersteld wordt dat ze gelieerd zijn aan de Gülenbeweging' (*Vr. en Ant.* Kamer 2016-17, 4 september 2017, QRVA 129, 193, Vr. nr. 2211)

Vraag van Ph. Blanchart aan de minister van Binnenlandse Zaken over de 'situatie van scholen waarvan verondersteld wordt dat ze gelieerd zijn aan de Gülenbeweging' (*Vr. en Ant.* Kamer 2016-17, 4 september 2017, QRVA 129, 202, Vr. nr. 2249)

Vraag van G. Calomne aan de minister van Binnenlandse Zaken over de 'beschermingsmaatregelen voor culturele centra' (*Vr. en Ant.* Kamer 2016-17, 4 september 2017, QRVA 129, 205, Vr. nr. 2254)

Vraag van K. Gabriëls aan de minister van Binnenlandse Zaken over de 'private bewaking met technologie' (*Vr. en Ant.* Kamer 2016-17, 4 september 2017, QRVA 129, 209, Vr. nr. 2295)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over de 'Belgische teruggekeerde Syriëstrijders – verslag van het Center for the Analysis of Terrorism' (*Vr. en Ant.* Kamer 2016-17, 4 september 2017, QRVA 129, 215, Vr. nr. 2312)

Vraag van W. Demeyer aan de minister van Binnenlandse Zaken over de 'aankondigingen na de vergadering van de bijzondere Ministerraad van 14 mei 2017' (*Vr. en Ant.* Kamer 2016-17, 11 september 2017, QRVA 130, 52, Vr. nr. 2272)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'detectie van radicalisering in de gesloten centra' (*Vr. en Ant.* Kamer 2016-17, 11 september 2017, QRVA 130, 69, Vr. nr. 2381)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over 'de aanwerving en opleiding van inlichtingenagenten (OCAD en Veiligheid van de Staat)' (*Hand.* Kamer 2016-17, 20 september 2017, CRIV54COM727, 23, Vr. nr. 20176)

Vraag van O. Chastel aan de minister van Binnenlandse Zaken over de 'Veiligheid van de Staat – informanten in radicale moslimmilieus' (*Vr. en* Ant. Kamer 2016-17, 20 september 2017, QRVA 131, 63, Vr. nr. 2477)

Vraag van B. Pas aan de minister van Justitie over 'het ontmantelen van gebedsplaatsen waar jihadisme wordt gepredikt' (*Vr. en* Ant. Kamer 2016-17, 20 september 2017, QRVA 131, 106, Vr. nr. 1480)

Vraag van B. Pas aan de minister van Justitie over 'de omzendbrief van 18 juli 2016 inzake haatpredikers' (*Vr. en* Ant. Kamer 2016-17, 20 september 2017, QRVA 131, 121, Vr. nr. 1755)

Vraag van B. Pas aan de minister van Justitie over 'Diyanet-moskeeën – verslagen Staatsveiligheid' (*Vr. en* Ant. Kamer 2016-17, 20 september 2017, QRVA 131, 126, Vr. nr. 1839)

Vraag van F. Dewinter aan de minister van Justitie over 'de komst van 67 Marokkaanse imams en morchidats naar aanleiding van de Ramadan' (*Vr. en* Ant. Kamer 2016-17, 20 september 2017, QRVA 131, 144, Vr. nr. 1955)

Vraag van B. Pas aan de minister van Justitie over de 'islamconsulenten in de gevangenissen' (*Vr. en* Ant. Kamer 2016-17, 20 september 2017, QRVA 131, 151, Vr. nr. 2006)

Vraag van Ph. Pivin aan de minister van Justitie over de 'detectie van radicalisering in de gesloten centra' (*Vr. en* Ant. Kamer 2016-17, 20 september 2017, QRVA 131, 154, Vr. nr. 2036)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'douane-controle op het verbod van precursoren voor explosieven' (*Vr. en* Ant. Kamer 2016-17, 20 september 2017, QRVA 131, 315, Vr. nr. 1722)

Vraag van G. Dallemagne aan de minister van Justitie over 'de door een gedetineerde ontvangen wervingsbrief van IS' (*Hand.* Kamer 2016-17, 28 september 2017, CRIV54PLEN185, 10, Vr. nr. 2286)

Vraag van de F. Dewinter aan de minister van Binnenlandse Zaken over 'de Grote Moskee te Brussel' (*Hand.* Kamer 2016-17, 5 oktober 2017, CRIV54PLEN186, 31, Vr. nr. 2319)

Vraag van F. Dewinter aan de minister van Justitie over 'de opvolging van terugkerende Syriëstrijders' (*Vr. en Ant.* Kamer 2016-17, 11 oktober 2017, QRVA 132, 466, Vr. nr. 1194)

Vraag van G. Calomne aan de minister van Defensie over de 'outsourcing van overheidstaken – risico op het uitlekken van gevoelige informatie' (*Vr. en Ant.* Kamer 2016-17, 11 oktober 2017, QRVA 132, 585, Vr. nr. 1256)

Vraag van F. Dewinter aan de minister van Justitie over 'van terrorisme of terroristische medeplichtigheid verdachte asielzoekers' (*Vr. en Ant.* Kamer 2016-17, 11 oktober 2017, QRVA 132, 591, Vr. nr. 1265)

Vraag van J.-J. Flahaux aan de minister van Binnenlandse Zaken over de 'nieuwe vormen van terreurdreiging' (*Hand.* Kamer 2017-18, 18 oktober 2017, CRIV54COM755, 18, Vr. nr. 20620)

Vraag van B. Hellings aan de minister van Justitie over 'het ter beschikking stellen van de geclassificeerde archieven van de Veiligheid van de Staat om nieuw licht te werpen op het VN-onderzoek naar de verdachte dood van Dag Hammarskjöld' (*Hand.* Kamer 2017-18, 18 oktober 2017, CRIV54COM756, 2, Vr. nr. 20973)

Vraag van A. Frédéric aan de minister van Binnenlandse Zaken over 'de samenwerking tussen de federale politie en de inlichtingendiensten' (*Hand.* Kamer 2017-18, 18 oktober 2017, CRIV54COM756, 27, Vr. nr. 21141)

Vraag van Ph. Pivin aan de minister van Buitenlandse Zaken over de 'MIVB – veiligheidsagenten – screening door de NVO' (*Vr. en* Ant. Kamer 2017-18, 20 oktober 2017, QRVA 133, 232, Vr. nr. 987)

Vraag van G. Calomne aan de minister van Justitie over de 'mededeling van een lijst met vermeende terroristen door Interpol' (*Vr. en* Ant. Kamer 2017-18, 20 oktober 2017, QRVA 133, 249, Vr. nr. 2074)

Vraag van A. Top aan de minister van Defensie over de 'ADIV – budget en personeelsbestand' (*Vr. en* Ant. Kamer 2017-18, 20 oktober 2017, QRVA 133, 326, Vr. nr. 1275)

Vraag van P. Buysrogge aan de minister van Justitie over de 'VSSE en ADIV – Fondsen om informanten te vergoeden. Verslag toezichtonderzoek' (*Vr. en* Ant. Kamer 2017-18, 20 oktober 2017, QRVA 134, 415, Vr. nr. 1224)

Samengevoegde vragen van B. Hellings, J. Fernandez, M. Van Hees, M. De Coninck en I. Poncelet de staatssecretaris voor Asiel en Migratie over 'de gevolgen van het vonnis van de Luikse rechtbank van eerste aanleg betreffende de huidige en toekomstige

gedwongen repatriëringen van Sudanese burgers' (*Hand.* Kamer 2017-18, 25 oktober 2017, CRIV54COM758, 1, Vr. nrs. 21184, 21332, 21481, 21486, 21555, 21564 et 21581)

Samengevoegde vragen van I. De Coninck en V. Yüksel aan de minister van Mobiliteit over 'de aanwerving van een Syriëstrijder als treinbestuurder' (*Hand.* Kamer 2017-18, 7 november 2017, CRIV54COM761, 41, Vr. nrs. 21064 en 21110)

Vraag van B. Pas aan de minister van Justitie over 'de bouw van een megamoskee in Gent' (*Hand.* Kamer 2017-18, 8 november 2017, CRIV54COM765, 6, Vr. nr. 21463)

Vraag van A. Top aan de minister van Justitie over 'de Belgian Intelligence' (*Hand.* Kamer 2017-18, 8 november 2017, CRIV54COM765, 33, Vr. nr. 21597)

Samengevoegde vragen van R. Terwingen en J.-J. Flahaux aan de minister van Justitie over 'de rol van de LTF's en LIVC's in de nieuwe omzendbrief rond de veiligheidsaspecten bij de erkenning van geloofsgemeenschappen' (*Hand.* Kamer 2017-18, 8 november 2017, CRIV54COM765, 8, Vr. nrs. 21135, 21398 en 21399)

Vraag van R. Deseyn aan de eerste minister over de 'beveiligde smartphones' (*Vr. en Ant.* Kamer 2017-18, 15 november 2017, QRVA 135, 79, Vr. nr. 262)

Vraag van R. Deseyn aan de minister van Binnenlandse Zaken over de 'ransomware – Windows XP' (*Vr. en Ant.* Kamer 2017-18, 15 november 2017, QRVA 135, 220, Vr. nr. 2233)

Vraag van O. Chastel aan de minister van Binnenlandse Zaken over de 'Dienst voor persoonsbeveiliging' (*Vr. en Ant.* Kamer 2017-18, 15 november 2017, QRVA 135, 272, Vr. nr. 2476)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'het bewaken van bedreigde personen' (*Vr. en Ant.* Kamer 2017-18, 15 november 2017, QRVA 135, 290, Vr. nr. 2535)

Vraag van B. Hellings aan de minister van Buitenlandse Zaken over de 'procedure voor de afgifte van reisdocumenten aan erkende vluchtelingen' (*Vr. en Ant.* Kamer 2017-18, 15 november 2017, QRVA 135, 370, Vr. nr. 1170)

Vraag van B. Pas aan de minister van Justitie over de 'radicaalislamitische imams, moskeeën en verenigingen' (*Vr. en Ant.* Kamer 2017-18, 15 november 2017, QRVA 135, 375, Vr. nr. 1708)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'het meldpunt radicalisme bij Fedasil' (*Vr. en Ant.* Kamer 2017-18, 15 november 2017, QRVA 135, 498, Vr. nr. 905)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'radicalisering in asielcentra' (*Vr. en Ant.* Kamer 2017-18, 15 november 2017, QRVA 135, 533, Vr. nr. 1102)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'tijdelijke intrekking van de identiteitskaart' (*Vr. en* Ant. Kamer 2017-18, 21 november 2017, QRVA 136, 49, Vr. nr. 2415)

Vraag van G. Calomne aan de minister van Binnenlandse Zaken over de 'personeelssterkte van de politie in de Brusselse treinstations' (*Vr. en Ant.* Kamer 2017-18, 21 november 2017, QRVA 136, 54, Vr. nr. 2431)

Vraag van N. Lijnen aan de minister van Binnenlandse Zaken over de 'genezing homoseksualiteit' (*Vr. en* Ant. Kamer 2017-18, 21 november 2017, QRVA 136, 57, Vr. nr. 2485)

Vraag van G. Dallemagne aan de minister van Defensie over de 'Belgische militaire betrokkenheid in Mali' (*Vr. en* Ant. Kamer 2017-18, 21 november 2017, QRVA 136, 179, Vr. nr. 1315)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over de 'komst van 67 Marokkaanse imams en morchidats naar aanleiding van de Ramadan' (*Vr. en* Ant. Kamer 2017-18, 21 november 2017, QRVA 136, 266, Vr. nr. 1187)

Vraag van G. Calomne aan de minister van Justitie over 'de ondertekening van een samenwerkingsprotocol met de FBI' (*Hand.* Kamer 2017-18, 22 november 2017, CRIV-54COM767, 18, Vr. nr. 21956)

Vraag van de G. Calomne aan de minister van Binnenlandse Zaken over de 'Blue Light Mobile voor crisissituaties' (*Hand.* Kamer 2017-18, 22 november 2017, CRIV-54COM770, 36, Vr. nr.21402)

Vraag van de F. Dewinter aan de minister van Binnenlandse Zaken over 'de aanpak van de islamitische haatpredikers' (*Hand.* Kamer 2017-18, 23 november 2017, CRI-V54PLEN198, 21, Vr. nr. 2419)

Vraag van J.-J. Flahaux aan de minister van Binnenlandse Zaken over de 'eventuele gevolgen van de terugkeer van jihadgangers naar ons land na de Koerdische overwinningen op IS in Syrië' (*Vr. en Ant.* Kamer 2017-18, 28 november 2017, QRVA 137, 190, Vr. nr. 2591)

Vraag van G. Calomne aan de minister van Financiën over de 'bevriezing van de banktegoeden van terrorisme verdachte personen' (*Vr. en Ant.* Kamer 2017-18, 28 november 2017, QRVA 137, 373, Vr. nr. 1755)

Vraag van G. Calomne aan de minister van Financiën over 'terrorismebestrijding – medewerking van de douanediensten' (*Vr. en Ant.* Kamer 2017-18, 28 november 2017, QRVA 137, 384, Vr. nr. 1770)

Samengevoegde vragen van K. Jadin en P. Buysrogge aan de minister van Defensie over 'het Cyber Security Operations Center binnen ADIV' (*Hand.* Kamer 2017-18, 29 november 2017, CRIV54COM771, 1, Vr. nrs. 21290 en 21375)

Vraag van P. Buysrogge aan de minister van Defensie over 'de ADIV' (*Hand.* Kamer 2017-18, 29 november 2017, CRIV54COM771, 13, Vr. nr. 21381)

Samengevoegde vragen van G. Dallemagne, G. Calomne en G. Vanden Burr aan de minister van Defensie over 'de rellen in Brussel' (*Hand.* Kamer 2017-18, 29 november 2017, CRIV54COM773, 45, Vr. nrs. 22063, 22105 et 22148)

Vraag van G. Calomne aan de minister van Binnenlandse Zaken over 'de ondertekening van een samenwerkingsprotocol met de FBI' (*Hand.* Kamer 2017-18, 29 november 2017, CRIV54COM773, 42, Vr. nr. 21955)

Vraag van de K. Degroote aan de minister van Binnenlandse Zaken over 'de vrijstellingen voor de functie van bijzondere veldwachter' (*Hand.* Kamer 2017-18, 6 december 2017, CRIV54 COM777, 13, Vr. nr. 22260)

Vraag van O. Chastel aan de minister van Binnenlandse Zaken over de 'Syriëstrijders' (*Vr. en Ant.* Kamer 2017-18, 11 december 2017, QRVA 139, 253, Vr. nr. 2585)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'advies van het CTED' (*Vr. en Ant.* Kamer 2017-18, 11 december 2017, QRVA 139, 259, Vr. nr. 2627)

Vraag van V. Yüksel aan de minister van Binnenlandse Zaken over 'de aanpak van bekeerlingen onder FTF en HTF' (*Vr. en Ant.* Kamer 2017-18, 11 december 2017, QRVA 139, 272, Vr. nr. 2650)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'Belgische cel voor controle op potentiële returnees' (*Vr. en Ant.* Kamer 2017-18, 11 december 2017, QRVA 139, 225, Vr. nr. 2374)

Vraag van M. De Coninck aan de staatssecretaris voor Asiel en Migratie over de 'visa voor imams' (*Vr. en Ant.* Kamer 2017-18, 11 december 2017, QRVA 139, 415, Vr. nr. 947)

Vraag van B. Pas aan de staatssecretaris voor Asiel en Migratie over 'de uitreiking van visa aan imams' (*Vr. en Ant.* Kamer 2017-18, 11 december 2017, QRVA 139, 433, Vr. nr. 1094)

Vraag van G. Calomne aan de staatssecretaris voor Asiel en Migratie over de 'Identificatie van geradicaliseerde kandidaat-vluchtelingen' (*Vr. en Ant.* Kamer 2017-18, 11 december 2017, QRVA 139, 446, Vr. nr. 1192)

Vraag van B. Pas aan de staatssecretaris voor Asiel en Migratie over 'Marokko – Memorandum of Understanding' (*Vr. en Ant.* Kamer 2017-18, 11 december 2017, QRVA 139, 455, Vr. nr. 1235)

Vraag van G. Dallemagne aan de minister van Justitie over 'de concessieovereenkomst voor de Grote Moskee van Brussel en het Islamitisch en Cultureel Centrum van België' (*Hand.* Kamer 2017-18, 13 december 2017, CRIV54COM780, 5, Vr. nr. 22286)

Vraag van B. Pas aan de minister van Justitie over de 'veiligheidsonderzoeken naar personen' (*Vr. en Ant.* Kamer 2017-18, 18 december 2017, QRVA 140, 253, Vr. nr. 2141)

Vraag van B. Pas aan de staatssecretaris voor Asiel en Migratie over de 'administratieve overeenkomst met Algerije – stand van zaken' (*Vr. en Ant.* Kamer 2017-18, 18 december 2017, QRVA 140, 472, Vr. nr. 1311)

BIJLAGE D.
DE AANBEVELINGEN VAN HET VAST COMITÉ I (2006-2016)

VOORAFGAAND

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, het OCAD en – in beperkte mate – van zijn ondersteunende diensten. Deze aanbevelingen vloeien – in hoofdzaak – voort uit de diverse toezichtsonderzoeken en adviezen. Ze worden telkenmale opgenomen in het onderzoeksrapport, en vervolgens hernomen in de activiteitenverslagen van het Comité.[181]

Eerder – in het *Activiteitenverslag 2006* – werd een overzicht geboden van de belangrijkste aanbevelingen die het Vast Comité I en zijn Begeleidingscommissies gedurende de jaren 1994 tot 2005 hadden geformuleerd en welke gevolgen hieraan werd gegeven.[182] Een gelijkaardige oefening wordt in voorliggend document gemaakt voor de periode 2006-2016. Daarmee wordt uitvoering gegeven aan een vraag van de parlementaire Begeleidingscommissie.[183]

---

181 In het eerste hoofdstuk van de respectievelijke activiteitenverslagen worden de belangrijkste initiatieven opgesomd die de diverse actoren in het afgelopen jaar namen in de lijn van voorgaande aanbevelingen en wordt de aandacht gevestigd op aanbevelingen die het Comité essentieel acht, maar die vooralsnog niet werden geïmplementeerd. Nieuwe aanbevelingen vormen het onderwerp van het afsluitende hoofdstuk in het activiteitenverslag.

182 VAST COMITÉ I, *Activiteitenverslag 2006*, 1-21.

183 In het kader van de bespreking van het *Activiteitenverslag 2015* werd immers gesuggereerd dat het Comité *'een lijst van de nog niet uitgevoerde aanbevelingen zou opstellen en dat de commissie aan de aanbevelingen een vergadering zou wijden om te zien welke initiatieven zij kan*

De talrijke aanbevelingen voor deze periode die ondertussen werden gerealiseerd door de inlichtingen- en veiligheidsdiensten en het OCAD, werden niet meer hernomen; de nog niet-gerealiseerde aanbevelingen werden afgetoetst aan hun actualiteitswaarde en, indien nuttig en noodzakelijk, geherformuleerd.

Wat de wijze van structureren van de aanbevelingen betreft, werd de structuur van de aanbevelingen van de experten van de parlementaire onderzoekscommissie 'terroristische aanslagen' weerhouden. Daarin wordt een onderscheid gemaakt tussen aanbevelingen bestemd voor de wetgevende macht, vervolgens de uitvoerende macht en ten slotte voor de diensten zelf. We merken op dat een deel van de eerder door het Vast Comité I geformuleerde aanbevelingen werden bevestigd door de rapporteurs van de parlementaire onderzoekscommissie. De hieronder opgenomen aanbevelingen overstijgen evenwel het domein van terrorisme en radicalisme; het betreft – zowel algemene als zeer specifieke (gedetailleerde) – aanbevelingen over de werking van de inlichtingen- en veiligheidsdiensten en het OCAD.

I. WETGEVENDE MACHT

I.1 Algemeen

I.1.1 Internationaal

1. Een duidelijk wettelijk kader voor de uitwisseling van informatie en persoonsgegevens met het buitenland

Wat de samenwerking betreft met buitenlandse diensten, drong het Comité reeds meermaals aan op een richtlijn uitgevaardigd door de Nationale Veiligheidsraad (in uitvoering van artt. 19 en 20 W.I&V). In september 2016 werd door de ministers van Justitie en Landsverdediging in een nota aan die Veiligheidsraad de als 'Vertrouwelijk Wet 11.12.1998' geclassificeerde 'Richtlijn aangaande de relaties van Belgische inlichtingendiensten met buitenlandse inlichtingendiensten' voorgelegd. Evenwel wordt daarin het doorgeven van informatie en persoonsgegevens aan buitenlandse diensten slechts zeer summier behandeld. Het Comité houdt dan ook vast aan zijn eerdere aanbevelingen en acht een initiatief prioritair.[184]

I.1.2 Nationaal

2. Een externe rectificatiemogelijkheid op de classificatie door inlichtingendiensten

Het Vast Comité I formuleerde reeds eerder de aanbeveling om tot een systeem te komen waarbij de classificatie die werd gegeven door de Belgische inlichtingendiensten, kan gerectificeerd worden indien ze niet beantwoordt aan de wettelijke bepalingen. Het Comité deed deze aanbeveling vanuit de bekommernis om op een betekenisvolle wijze

nemen' in *Parl. St.* Kamer 2016-17, nr. 54K2185/001 (Activiteitenverslag 2015 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Verslag namens 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 inlichtingen- en veiligheidsdiensten), 7.

184 Hierbij moet alleszins aandacht zijn voor het beginsel dat de inlichtingendiensten bij de informatie-uitwisseling zorgvuldig tewerk moeten gaan.

naar de Begeleidingscommissie te kunnen rapporteren. Immers, indien een classificatie niet gerechtvaardigd blijkt, verhindert dit weliswaar niet de kennisname van de gegevens door het Comité, doch wel de redactie van een sluitend rapport ten behoeve van de Begeleidingscommissie. In de huidige stand van de wetgeving kan enkel een vrijblijvend *appel* worden gedaan aan de verantwoordelijkheidszin van degene die de informatie classificeerde. Maar ook vanuit een bekommernis voor de rechten van burger kwam het Comité tot dezelfde aanbeveling.

3. Definiëren van de diverse rollen van de VSSE
De VSSE verleent diverse adviezen aan overheden. Het Vast Comité I was van mening dat de diverse rollen die aan de VSSE worden toegewezen, nader dienen te worden gedefinieerd. Zo bijvoorbeeld in het kader van de procedures tot verkrijging van de Belgische nationaliteit. Hierbij kan de regeling inzake veiligheidsverificaties en -onderzoeken als voorbeeld gelden.[185]

I.2 Wijziging Wet houdende regeling van de inlichtingen- en veiligheidsdienst

4. Gemeenschappelijke databanken en de interconnectie tussen databanken
Er moet gestreefd worden naar meer én betere, horizontale informatie-uitwisseling en -doorstroming. Weliswaar vergt dit een zeer grote inspanning inzake de uitbouw en eenmaking van gemeenschappelijke databanken alsook de interconnectie tussen de databanken. Dit vergt meer tijd en middelen dan er thans binnen de diensten beschikbaar zijn. Deze problematiek moet worden uitgeklaard en de juiste (eigen) positie van de inlichtingendiensten moet worden gegarandeerd.

5. Correcte interpretatie van het begrip 'technische bijstand'
Wat betreft de 'technische bijstand' aan het gerecht (art. 20 § 2 W.I&V), heeft het Comité reeds meermaals uitdrukkelijk gesteld dat deze bepaling de VSSE en de ADIV niet toelaat inlichtingenbevoegdheden te gebruiken voor gerechtelijke doeleinden. Hierover dienen de inlichtingendiensten permanent te waken.

6. Invulling van de wettelijke lacune in verband met dataretentie
Bij de uitwerking van de regeling inzake vordering van operatoren, werd geen rekening gehouden met de nieuwe bevoegdheid van de VSSE en de ADIV om de activiteiten van buitenlandse diensten op Belgisch grondgebied op te volgen. Het Vast Comité I beveelt aan dat de wetgever een maximale termijn voor kennisname van metadata zou bepalen.

7. Een wettelijk kader dat het beheer van de speciale fondsen nauwkeurig beschrijft
Er moet een wettelijke (of reglementaire) bepaling worden opgesteld die het beheer van de speciale fondsen nauwkeurig beschrijft. Tevens is het absoluut noodzakelijk dat voor beide inlichtingendiensten soortgelijke controles worden ingevoerd, zowel intern als extern. In

[185] Daarbij zou expliciet moeten worden voorzien in de mogelijkheid voor de procureur des Konings om in het kader van procedures van nationaliteitsverkrijging geclassificeerde informatie te ontvangen, te verwerken en te gebruiken. Daarbij moet evident rekening worden gehouden met de rechten van de betrokkene. Ook zou de korte termijn waarover de VSSE beschikt om haar opmerkingen te formuleren, herbekeken moeten worden.

een reglementaire bepaling kan 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.

8. Herziening van de regeling voor intercepties van buitenlandse communicaties
Het Comité wees op eerdere aanbevelingen om de regeling voor intercepties van buitenlandse communicaties door de ADIV te herzien. Belangrijke elementen zijn hierbij de mate waarin intercepties al dan niet gericht moeten gebeuren, de juiste draagwijdte van de mogelijkheid om signalen te 'zoeken', de mate van precisering van het jaarlijkse Afluisterplan, de mogelijkheid om aan data-*mining* te doen in bulkinformatie en de vraag of buitenlandse SIGINT-operaties moeten kaderen binnen een breder 'internationaal mandaat'. Bepaalde van deze aspecten werden nader geregeld in de Wet van 30 maart 2017, anderen dienen nog uitvoering te krijgen.

9. Een wettelijke regeling inzake informantenwerking
Er dient een duidelijke wettelijke regeling te komen inzake informantenwerking. Ook dient er een reflectie te worden gehouden over de wenselijkheid om – in volstrekt uitzonderlijke gevallen en mits een gedegen democratische controle – in de mogelijkheid te voorzien om informanten die over inlichtingen kunnen beschikken die cruciaal is voor de veiligheid van de rechtstaat, een welomschreven – al dan niet geldelijke – 'tegenprestatie' te verlenen.

10. Een wettelijke basis voor de screening van informanten
Om de pertinentie en de betrouwbaarheid van de aan te leveren of aangeleverde informatie te kunnen beoordelen, moeten de inlichtingendiensten kunnen beschikken over een zo accuraat mogelijk beeld van de betrokkene (*screening*). Er dient dan ook in een wettelijke basis te worden voorzien die de krijtlijnen van dergelijke controles vastlegt.

11. Een wettelijke regeling inzake burgerinfiltranten
Een informant wordt soms zo gerund of aangestuurd dat hij op bepaalde momenten begint te fungeren als een burgerinfiltrant die echte inlichtingenopdrachten krijgt toebedeeld. Deze vorm van inlichtingengaring is op diverse vlakken nog problematischer dan de 'gewone' informantenwerking. Anderzijds zijn de controlemogelijkheden van de dienst op de wijze waarop haar 'opdrachten' worden vervuld, beperkt. Het Vast Comité I herhaalde dan ook zijn aanbeveling om hieromtrent tot een wettelijke regeling te komen.

12. Bevoegdheidsuitbreiding van de ADIV en de VSSE
De BIM-Wet gaf aan de ADIV een bijkomende opdracht om '*in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren*' (art. 11 § 1, 2° W.I&V). Het Vast Comité I beval echter aan dat in dezelfde mogelijkheid zou worden voorzien in geval van aanvallen tegen informatiesystemen van andere overheidsdiensten of tegen de nationale kritieke infrastructuur.

13. De rol van inlichtingendiensten bij bepaalde buitenlandse investeringen in sectoren van militair en strategisch belang
Het Vast Comité I achtte het wenselijk om een wettelijke regeling tot stand te brengen voor de controle van en het toezicht op buitenlandse investeringen en commerciële activiteiten in sectoren die als strategisch en militair belangrijk worden beschouwd voor België. Daarbij zou de rol van de inlichtingendiensten vastgelegd moeten worden. Het Vast Comité I meende ook dat het potentieel militair belang van een onderneming die in België gevestigd is, de preventieve aandacht van de ADIV verdient wanneer de betrokken onderneming in buitenlandse handen overgaat.

1.4. Wijziging Wet betreffende de analyse van de dreiging

14. Definiëring van het begrip 'relevante inlichtingen'
Het begrip 'relevante inlichtingen' (art. 6 W.OCAD) moet uitgeklaard worden.

II. UITVOERENDE MACHT

II.1. Algemeen

II.1.1 Internationaal – Europees

15. Streven naar een verbeterde (Europese) aanpak wat geclassificeerde informatie betreft (inzake technische uitrustingen en homologatie)
Het Vast Comité I beval de grootste omzichtigheid aan bij de keuze van beveiligde technische uitrustingen voor de verwerking van gevoelige en geclassificeerde informatie. Technische uitrustingen moeten worden geëvalueerd, gecertificeerd en gehomologeerd –wat betreft hun betrouwbaarheid en veiligheid – volgens criteria en procedures die beantwoorden aan de normen van de Europese Unie. Het Vast Comité I beval daarenboven aan dat bij de gunning van opdrachten aan leveranciers van dergelijk materieel, het bezit van een veiligheidsmachtiging wordt opgelegd. In het kader van het voorafgaandelijke veiligheidsonderzoek zou bijzondere aandacht moeten worden besteed aan de eventuele banden van die leveranciers met sommige buitenlandse inlichtingendiensten.

16. Coördinatie van de vertegenwoordiging van politie-, administratieve, veiligheids- en inlichtingendiensten op internationale fora
De vertegenwoordiging van politie-, administratieve, veiligheids- en inlichtingendiensten op internationale fora dient gecoördineerd te verlopen.

II.1.2 Nationaal

17. Het aantrekken van personeel met de nodige kennis en gepaste vaardigheden en het bevorderen van diversiteit binnen de diensten
Zowel voor het runnen van informanten in de radicale milieus (HUMINT) als voor het opvolgen van open bronnen (OSINT en SOCMINT) is het aangewezen dat de diensten een beroep kunnen doen op collecte-agenten en analisten die de verschillende talen beheersen en die de leefwereld van deze personen goed kennen (diversiteit). Om bijvoorbeeld op een adequate wijze het radicaal islamisme te kunnen opvolgen, moet er bij de

inlichtingendiensten voldoende personeel aanwezig zijn met kennis van o.m. Arabische talen.[186]

18. De werking van de LTF's professionaliseren
Het Vast Comité I beveelt aan dat de verschillende deelnemers aan de LTF elkaar goed informeren van mekaars noden en behoeften, van de mogelijkheden van elkeen, maar ook van eenieders beperkingen.

19. Geen inlichtingenbevoegdheden gebruiken voor gerechtelijke doeleinden
Wat betreft de 'technische bijstand' aan het gerecht (art. 20 § 2 W.I&V), heeft het Comité reeds meermaals uitdrukkelijk gesteld dat deze bepaling de VSSE en de ADIV niet toelaat inlichtingenbevoegdheden te gebruiken voor gerechtelijke doeleinden. Hierover dienen de inlichtingendiensten permanent te waken.

20. De creatie van een informatieplatform inzake de strategische bescherming WEP
Het Vast Comité I beveelt aan dat er, onder de leiding van de Nationale Veiligheidsraad, een informatieplatform inzake de strategische bescherming van het wetenschappelijk en economisch potentieel in het leven wordt geroepen. Hierbij dienen zeker te worden aangesproken: de regionale en federale overheden bevoegd voor economie, de vertegenwoordigers van de private sector en de onderzoekswereld, de twee inlichtingendiensten, het Centrum voor Cybersecurity, de FCCU, het OCAD, het Crisiscentrum en de Nationale Veiligheidsoverheid. Het Comité heeft daarbij al kunnen vaststellen dat ook organisaties met een specifieke expertise, zoals het CFI en de Nationale Bank, over veel informatie beschikken die niet altijd voldoende benut wordt. Dit platform kan dienst doen als informatie-uitwisselingskanaal en de aanzet geven voor een geïntegreerd beleid waarin ook de rol van de twee inlichtingendiensten en het OCAD wordt gepreciseerd. Dit moet uiteindelijk leiden tot een duidelijke *tasking* van alle participanten en hun samenwerking. Anderzijds en tegelijk dienen de inspanningen voor een betere cyberveiligheid te worden verdergezet. Het Centrum voor Cybersecurity kan ook hier een kapitale rol in spelen. Dit vraagt eveneens om een evaluatie van de geschiktheid van de Wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren.

21. Homologatie van ICT-systemen en encryptie
De onverwijlde toewijzing van de opdracht tot homologatie van ICT-systemen met inbegrip van encryptie van eigen bodem moet onverwijld worden toegewezen aan een overheidsdienst, zoals de Nationale Veiligheidsoverheid (NVO) of het Centrum voor Cybersecurity.

22. Aanbevelingen met betrekking tot de Joint Information Box
De Vast Comités I en P formuleerden diverse aanbevelingen om het systeem van de *Joint Information Box* (JIB) fundamenteel te herbekijken. De rol van elke medewerkende dienst

186 Om dit doel te bereiken, dienen vooreerst inspanningen te worden geleverd die erop gericht zijn dat personen die dergelijke kennis bezitten, zich ook effectief aanmelden voor aanwervingsproeven. Verder moeten die proeven voor deze personen dermate worden aangepast dat een eventuele gebrekkige kennis van onze landstalen hen niet *a priori* uitsluit. Ten slotte moet aandacht worden besteed aan de wijze waarop de veiligheidsonderzoeken worden gevoerd in hoofde van personen die in het buitenland hebben verbleven.

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 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 het 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.

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.

23. Een samenwerkingsakkoord tussen de inlichtingen- en politiediensten

Tussen de inlichtingendiensten enerzijds en de (federale en lokale) politiediensten anderzijds moet gestructureerd overleg plaatsvinden om via welbepaalde procedures gegevens uit te wisselen. Het ontbreken van een samenwerkingsakkoord tussen deze diensten vormt zonder twijfel een tekortkoming in ons veiligheidssysteem.

24. Instructie Nationale Veiligheidsraad inzake veiligheidsonderzoeken

Het Comité acht het aangewezen dat de NVR een instructie zou uitvaardigen in het kader van veiligheidsonderzoeken en de aanwezigheid van een neutrale waarnemer in deze, en dit ongeacht de dienst die het onderzoek voert en ongeacht het statuut van de onderzochte persoon.

Tevens acht het Comité het nuttig dat personeel van bedrijven of instellingen die stoffen behandelen die kunnen worden gebruikt bij het ontwikkelen van NRBC-wapens, systematisch aan veiligheidsonderzoeken of -verificaties zouden moeten worden onderworpen.

25. Veiligheidsadviezen van toepassing maken voor verblijfsvergunningen voor vreemdelingen
Het systeem van de veiligheidsadviezen zou ook van toepassing moeten worden gemaakt voor de verblijfsvergunningen voor vreemdelingen en voor de afwijking van de nationaliteitsvoorwaarde voor leerkrachten. Dit vereist wel een gemotiveerde beslissing van de bevoegde overheid.

26. Interdepartementele samenwerking inzake cybersecurity, ICT-security en Cyberintelligence
Bepaalde aspecten van de Snowden-onthullingen wezen op zwaktes in de beveiligingssystemen van IT-netwerken van zowel private actoren als publieke instellingen. Het Comité herhaalde dan ook met klem dat er meer aandacht moest uitgaan naar *cyber-* en *ICT-Security* (INFOSEC) en dat deze problematieken – die niet alleen tot het takenpakket van de inlichtingendiensten behoren – een interdepartementale samenwerking vereisen. Zo bijvoorbeeld is in deze een cruciale rol weggelegd voor de Nationale Veiligheidsraad.

27. Samenwerkingsverbanden tegen proliferatie
Ten einde de proliferatie op een effectieve manier aan te pakken, beval het Vast Comité I aan dat de diverse overheden formele samenwerkingsverbanden zouden afsluiten. Dit was noodzakelijk gezien de complexe aard van het fenomeen, zowel qua techniciteit als qua regelgeving en bevoegdheid. Deze samenwerkingsverbanden dienen enerzijds te worden afgesloten tussen het federale en het gewestelijke niveau wat betreft het afstemmen van de regelgeving en het bepalen van sancties, en anderzijds tussen alle diensten die enige verantwoordelijkheid hebben op het terrein wat betreft controle en toezicht.

II.2. Inlichtingendiensten algemeen

28. Het wegwerken van deficits en het versterken van de inlichtingen- en veiligheidsdiensten
Het Comité heeft steeds gepleit om de inlichtingendiensten voldoende middelen toe te kennen, niet alleen op het gebied van personeel en logistiek maar ook op wetgevend vlak. Uiteraard waren deze aanbevelingen niet exclusief gericht op een betere strijd tegen het extremisme en terrorisme; de toekenning van noodzakelijke middelen moet toelaten alle in de Inlichtingenwet opgesomde taken naar behoren uit te voeren. Het Comité wees er in dit kader op dat het personeelsbestand van de VSSE volledig de budgettaire evolutie van de dienst volgde. 2015 vormde een dieptepunt inzake personeelseffectieven: in 2010 beschikte de VSSE nog over 15% meer *full-time* equivalenten (FTE) in vergelijking met begin januari 2015. Begin 2016 was opnieuw een stijging merkbaar gelet op de aanwerving van nieuwe inspecteurs en analisten. Wat de ADIV betreft kon geen budgettaire evolutie worden opgemaakt omdat deze dienst niet over een eigen budget beschikt, maar als een entiteit binnen Defensie wordt beheerd. De beschikbare cijfers inzake het personeelsbestand van de ADIV tonen aan dat het aantal FTE sinds 2007 eerder stabiel is gebleven. Het Comité wees tot slot op het belang van een adequaat budget en kader van het OCAD dat sinds zijn oprichting in 2006 een belangrijke rol te spelen heeft in de strijd tegen terrorisme en extremisme.

29. Onderzoek naar de efficiëntie van de actiemiddelen waarover inlichtingendiensten beschikken
Het Comité beveelt aan dat de overheden een onderzoek zouden voeren naar de efficiëntie van de actiemiddelen waarover de inlichtingen- en veiligheidsdiensten op het terrein beschikken en naar de huidige beperkingen (bijvoorbeeld anonieme voorafbetaalde GSM-kaarten).

30. Uitvoering geven aan verplichtingen opgenomen in artikelen 19 & 20 W.I&V
De bevoegde ministers en de Nationale Veiligheidsraad dienen bepaalde aspecten van de voorwaarden voor samenwerking, informatie-uitwisseling en technische bijstand (cf. huidige richtlijn) verder te regelen en op die wijze uitvoering geven aan alle verplichtingen opgenomen in de artikelen 19 en 20 W.I&V.

31. Richtlijn inzake informantenwerking
Er dient een algemene richtlijn te worden opgesteld waarin alle aspecten van de informatenwerking aan bod komen. In het bijzonder moet meer aandacht besteed worden aan een formele risicoanalyse met een oplijsting van de diverse risico's, waaraan wordt meegewerkt door een persoon of afdeling die niet betrokken was bij het opstellen van het initiële rekruteringsvoorstel. De twee inlichtingendiensten moeten nadenken over de implementatie van een systeem dat wederzijds toelaat kennis te nemen van de identiteit van informanten waarmee de samenwerking op initiatief van een van beide diensten werd stopgezet.

32. De nood aan een politieke dekking voor samenwerkingsverbanden
Het Comité is van oordeel dat er vanuit de inlichtingendiensten een grotere openheid moet zijn over bestaande bi- of multilaterale samenwerkingsverbanden en dit in de eerste plaats ten aanzien van de bevoegde ministers. In dergelijke samenwerkingsverbanden kunnen immers engagementen worden genomen of keuzes gemaakt die een politieke aftoetsing en dekking behoeven. Anders gezegd, dienen de bevoegde ministers afdoende te worden geïnformeerd opdat zij steeds in de mogelijkheid zouden zijn om hun politieke verantwoordelijkheid op te nemen. Daarbij moet opgemerkt worden dat wat 'politiek relevant' is of niet, kan evolueren in de tijd.

33. De nood aan politieke sturing door de Nationale Veiligheidsraad
Het toenmalige Ministerieel Comité voor inlichting en veiligheid 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 Comité acht het wenselijk dat de nieuwe Nationale Veiligheidsraad en bij uitbreiding het Strategisch Comité en het Coördinatiecomité voor inlichting en veiligheid hun sturende rol – mede op aangeven van de twee inlichtingendiensten – zouden opnemen in diverse domeinen.

34. Duidelijke en afdwingbare taakverdeling OCAD – inlichtingendiensten
In het kader van de strijd tegen terrorisme is vaak een dringende reactie vereist. Mede hierdoor zijn de analisten vaak niet in de mogelijkheid om strategische analyses op te stellen en wordt de informatiegaring georiënteerd op onmiddellijke noden, eerder dan op een

lange termijn-analyse. De VSSE dient een reflectie te houden over zijn eigenheid als inlichtingendienst en zijn rol in de strijd tegen terrorisme.

II.3. VSSE

II.4. ADIV

35. Formele goedkeuring lijst inzake bescherming van het WEP
Het Comité wijst op het ontbreken van de (wettelijk vereiste) formele goedkeuring door de Nationale Veiligheidsraad opgestelde lijst met bedrijven waarvan de ADIV het WEP moet beschermen.

III. OVERHEDEN EN DIENSTEN

III.3. Inlichtingendiensten algemeen

Internationaal

36. Niet aanvaarden van gegevens van derde landen die op onrechtmatige wijze werden verzameld
De VSSE en de ADIV kunnen uiteraard informatie of inlichtingen ontvangen van buitenlandse partners. Zij kunnen die informatie zelf verwerken en/of doorzenden naar de bevoegde Belgische diensten (bijv. het OCAD). In dit kader wees het Comité er in het verleden al op dat de '*ontvangende dienst minimale inspanningen zou leveren om te achterhalen op welke wijze de betrokken inlichtingen werden verkregen*', dit om toe te laten gegevens van derde landen die op onrechtmatige wijze zijn verzameld, desgevallend niet te aanvaarden.

37. Kritische evaluatie van de regels van de internationale inlichtingencultuur – Zorg dragen voor de accuraatheid en juridische gegrondheid van de informatie-transmissie
De Commissie Burgerlijke Vrijheden, Justitie en Binnenlandse Zaken van het Europese Parlement '*dringt er bij de lidstaten op aan gegevens van derde landen die op onrechtmatige wijze zijn verzameld niet te aanvaarden en toezichtsactiviteiten op hun grondgebied door overheden of bureaus van derde landen die volgens nationaal recht onrechtmatig zijn of niet voldoen aan de juridische waarborgen die in internationale of EU-instrumenten zijn vastgelegd, waaronder de bescherming van de mensenrechten in het kader van het VEU, het EVRM en het Handvest van de grondrechten van de EU, te weigeren.*' Het Vast Comité I merkte op dat de praktijk echter leert dat 'aanleverende inlichtingendiensten' in regel hun bronnen (en dus de oorsprong van een inlichting) afschermen en dat de 'ontvangende diensten' dit ook aanvaarden. Deze vorm van verstandhouding maakt deel uit van de internationale inlichtingencultuur, net zoals de regel van de derde dienst, het *do ut des*-principe en de eisen van geheimhouding. 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. Daar-

enboven 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.

38. Standaardisatie van procedures in het kader van de internationale uitwisseling
In het kader van de internationale uitwisselingen en meer bepaald van het beheer van de informatieaanvragen die afkomstig zijn van buitenlandse correspondenten, beveelt het Vast Comité I aan om gestructureerde en internationaal gestandaardiseerde procedures te ontwikkelen. De informatieaanvragen dienen verplicht elementen te omvatten zoals de dringendheidsgraad, de antwoordtermijn… Ze moeten bovendien worden aangevuld met alle elementen die nuttig of nodig zijn voor de uitvoering van de aanvraag. Hetzelfde geldt voor de instrumenten die noodzakelijk zijn in het kader van de strijd tegen het terrorisme, d.w.z. de nationale en internationale lijsten. De lijsten met terroristen of geradicaliseerde personen zouden moeten worden gestandaardiseerd.

39. De nood aan een politieke dekking voor samenwerkingsverbanden
(*supra* 32.)

40. Een strikte naleving van artikel 33 W.Toezicht, ook op internationaal vlak
'*De inlichtingendiensten, het Coördinatieorgaan voor de dreigingsanalyse en de andere ondersteunende diensten, zenden uit eigen beweging aan het Vast Comité I de interne reglementen en richtlijnen over, alsook alle documenten die de handelswijze van de diensten regelen*', aldus artikel 33 § 2 W.Toezicht. Het Vast Comité I moest vaststellen dat deze verplichting niet strikt wordt nageleefd (in het bijzonder wat betreft de ADIV, het OCAD en de ondersteunende diensten). Deze verplichting geldt ook voor afspraken, MOU's of akkoorden gesloten op internationaal vlak, weze het bi- of multilateraal. De nauwgezette toepassing door de gecontroleerde diensten van dit artikel vormt een *conditio sine qua non* met het oog op een doeltreffende uitvoering van de opdracht van het Comité. Om deze reden onderlijnde het Comité andermaal het belang van de tijdige, volledige en ambtshalve toezending van deze gegevens.

Nationaal

41. Verbeterde samenwerking en het zoeken naar synergieën
De coördinatie en samenwerking tussen beide inlichtingendiensten moet verbeterd worden, meer bepaald door een rationele exploitatie van de middelen, het uitwisselen van informatie en inlichtingen en de productie van gemeenschappelijke analyses, zonder dat deze diensten daarbij hun identiteit en specifieke kenmerken verliezen.

Zo bleek de samenwerking tussen beide Belgische inlichtingendiensten in het kader van de Syriëproblematiek beperkt en punctueel. Het Vast Comité I beveelt aan dat beide diensten zouden onderzoeken welke synergiën mogelijk zijn en of er ruimte is voor een versterkte samenwerking, onder meer op het vlak van OSINT, SOCMINT, (CYBER) HUMINT en SIGINT. Eveneens kan eraan gedacht worden dat de VSSE de ADIV zou

vertegenwoordigen binnen bepaalde werkgroepen (bijvoorbeeld binnen de LTF's of in contacten met het gevangeniswezen).

42. Planmatig aanpakken van de inlichtingenprocessen
De inlichtingenprocessen moeten planmatig worden aangepakt waarbij vooraf bepaald wordt wat de onderzoeksvragen zijn met betrekking tot de te volgen fenomenen, hoe men de informatie zal ver zamelen (collectemethoden) en hoe men de informatie zal analyseren (analysemethoden).[187]

43. Uitvoeren grondige strategische analyses, met formulering hypothesen en in kaart brengen scenario's: genereren van 'voorspellende inlichtingen' – methodologie uitwerken op grond van multidisciplinaire benadering
Het Vast Comité I meent dat het produceren van zogenaamde voorspellende inlichtingen tot de essentie van een inlichtingendienst behoort. Het Comité beveelt aan dat de VSSE en de ADIV met hun 'klanten' onderzoeken in welke mate er voorspellende inlichtingen nodig of nuttig zijn, wat het concept precies inhoudt, wat men er kan van verwachten en hoe de diensten hun ambitie ter zake zouden kunnen realiseren.

Een belangrijke methode is het opstellen van mogelijke scenario's (zoals *worst case-scenario's*) en het stellen van hypotheses die nadien kunnen bevestigd of ontkracht worden. Dit belangrijke methodologisch instrument zou meer kunnen worden toegepast. Het Comité meent dat dergelijke scenariovorming bij voorkeur multidisciplinair gebeurt: een terrorisme-scenario heeft meerdere componenten (zowel burgerlijke als militaire) zodat de VSSE en de ADIV ter zake moeten samenwerken.

44. Het inrichten van een gemeenschappelijk samenwerkingsplatform
Het Comité moest vaststellen dat de VSSE en de ADIV in de periode vóór de Snowden-onthullingen nooit en nadien slechts beperkt onderling informatie hebben uitgewisseld over de bedreigingen gevormd door massale data-captatie en politieke en economische spionage. Het Comité stelt deze vaststelling vooreerst tegenover de wettelijke verplichting die berust bij de diensten om informatie uit te wisselen (art. 19 W.I&V). Daarenboven wijst het Comité op het bestaan van een onderling samenwerkingsakkoord (Protocolakkoord van 12 november 2004) dat er net op gericht is om spontaan informatie door te geven die tot de bevoegdheidssfeer van de andere dienst behoort. Minstens na de onthullingen hadden de mechanismen beschreven in dit Protocolakkoord gebruikt moeten worden om beider informatiepositie te verstevigen. Het Comité wees in het bijzonder op de in het Protocol opgenomen mogelijkheid om een '*ad hoc* samenwerkingsplatform' op te richten waarbinnen gezamenlijke analyses kunnen worden opgesteld.

45. Interactie tussen de gegevensbanken van beide diensten
De uitwisseling van informatie is van groot belang. Zonder twijfel bestaat er op basiscollecteniveau heel veel meer informatie bij de diverse Belgische inlichtingen- en politiediensten dan waartoe de VSSE en de ADIV toegang hebben. Er moet gestreefd worden naar meer én betere, horizontale informatie-uitwisseling en -doorstroming. Weliswaar

[187] In het kader van de strijd tegen terrorisme is vaak een dringende reactie vereist. Mede hierdoor zijn de analisten vaak niet in de mogelijkheid om strategische analyses op te stellen en wordt de informatiegaring georiënteerd op onmiddellijke noden, eerder dan op een lange termijn-analyse.

vergt dit een zeer grote inspanning inzake de uitbouw, interconnectie en eenmaking van (gemeenschappelijke) databanken. Dit vergt meer tijd en middelen dan er thans binnen de diensten beschikbaar zijn. Deze problematiek moet worden uitgeklaard en de juiste (eigen) positie van de inlichtingendiensten moet worden gegarandeerd.

46. Beraden over het 'need to know' en het 'need to share'-principe
Het feit dat binnen de ADIV slechts een zeer beperkt aantal personen rechtstreeks toegang heeft tot SIGINT-informatie en alsook de strikte geheimhouding rond dit thema, kan de totstandkoming van een overkoepelend beeld met betrekking tot SIGINT-capaciteiten en –strategieën van buitenlandse grootmachten, bemoeilijkt hebben. Het Comité was dan ook van oordeel dat de ADIV zich zou moeten beraden over de vraag hoe in deze het principe van de *need to know* beter kan worden verzoend met de *need to share*.

47. Verbeteren rekrutering en aandacht voor diversiteit in personeelsbeleid en talenkennis (*supra* 17.)

48. Inzetten op HUMINT in geradicaliseerde en terroritische milieus
Informatie die via HUMINT wordt aangeleverd, is vaak beslissend in die zin dat ze een nuttige bijdrage levert in een disruptieve strategie of bij het voorkomen van een aanslag. Het is echter niet eenvoudig om bronnen te rekruteren in geradicaliseerde en terroristische milieus. Dit moet een prioriteit vormen.

49. Gebruik van gestandaardiseerde analysetechnieken
De analyse vormt een essentiële component van het inlichtingenwerk. Inzake analyse zijn heel wat gestandaardiseerde technieken voorhanden. Het gebruik van dergelijke technieken is niet om te voldoen aan en of ander axioma, wel om analytische gebreken (cognitieve of feitelijke fouten) te voorkomen. Het gaat om het vermijden van risico's die zich binnen de inlichtingenprocessen kunnen voordoen en finaal een invloed kunnen hebben op de informatiepositie. Het Comité stelt vast dat de diensten niet op een coherente wijze een beroep doen op formele analysemethoden. Het beveelt dan ook aan dat de diensten een plan zouden ontwikkelen waarin duidelijk en transparant wordt bepaald hoe zij tegenover deze problematiek staan, welk beleid zij ter zake voeren en hoe ze de (analytische) risico's onder controle houden.

50. Planmatige aanpak van fenomenen
De inlichtingenprocessen zijn gebaat met een planmatige aanpak of *design* waarbij vooraf bepaald wordt wat de onderzoeksvragen zijn met betrekking tot de te volgen fenomenen, hoe men de informatie zal verzamelen (collectemethoden) en hoe men de informatie zal analyseren (analysemethoden). Een dergelijk *design* is afgeleid uit het hogere strategische niveau, maar verschilt van bijvoorbeeld een traditioneel collecteplan, omdat de het zowel collecte- als analysemethoden overkoepelt. Op die manier kunnen collecte en analyse beter worden gestroomlijnd en zullen de inlichtingenprocessen efficiënter kunnen verlopen. Bij beide diensten bestaat hieraan nood. Het Vast Comité I beveelt aan dat de diensten een dergelijke aanpak in hun werking integreren en bij het aanvatten van een nieuw of zich ontvouwend fenomeen – zoals bijvoorbeeld de Syriëcrisis – doelbewust een collecte- en analyse-overkoepelend *design* opmaken. In principe zou dit *design* echter niet enkel binnen elke dienst moeten bestaan, maar ook rekening houden met, en idealiter gebruik maken van collecte- en analysecapaciteiten van andere diensten.

51. Bevraging van de 'klanten'
Beide diensten moeten hun 'klanten' expliciet bevragen over welke inlichtingen deze precies willen beschikken en hoe ze de inlichtingen evalueren (*feedback*). Dit vormt een gedeelde verantwoordelijkheid. Enerzijds moeten de diensten duidelijk maken onder welke voorwaarden, hoe en naar wie ze inlichtingen willen of kunnen verspreiden en welke 'ambitie' daarbij vanwege de dienst mag verwacht worden (beschrijvende, verklarende of voorspellende inlichtingen). Maar anderzijds moeten de klanten daar natuurlijk zelf aan meewerken, dit wil zeggen, aangeven wat ze verwachten en welke hun (inlichtingen-) behoeften zijn.

52. Permanente vorming en reële kwaliteitsbewaking inzake collecteverslagen
Het Comité is zich bewust van het feit dat het in het inlichtingenwerk niet steeds evident is op het moment van de collecte zelf uit te maken welke informatie ooit relevant zal blijken of niet. Dit neemt niet weg dat de eisen ter zake zoals die omschreven zijn in de W.I&V alsook in de Privacywet (doelbindingsprincipe, adequaatheid, correctheid…) moeten nageleefd worden. Dit betekent bijvoorbeeld dat of en op welke wijze een bepaald feit in een collecteverslag wordt opgenomen, een cruciaal gegeven vormt. De wijze waarop die *input* dient te gebeuren zou het voorwerp moeten zijn van permanente vorming en onderworpen worden aan een ernstige kwaliteitsbewaking.

53. Vorm, inhoud en timing van de 'analyseproducten'
Het Comité had eerder de aanbeveling geformuleerd om in de analyseproducten die bestemd zijn voor andere overheden, een aanduiding te geven van de bron(nen) van de informatie. Immers, dit kan de bestemmeling helpen bij de beoordeling van de betrouwbaarheid van het product. Het Comité herhaalt deze aanbeveling. Tevens moeten instructies uitgevaardigd worden over het moment waarop en de vorm waarin de analyseproducten naar andere overheden moeten gezonden worden en moet een aanduiding worden gegeven van de exacte bestemmelingen.

54. Gemeenschappelijke dreigingsanalyse inzake het WEP
De twee inlichtingendiensten, het OCAD en het Belgisch Centrum voor Cybersecurity, dienen samen een analyse op te maken van het fenomeen van de bedreiging die uitgaat van buitenlandse interceptiesystemen voor het Belgische WEP en tevens de kritieke infrastructuren in kaart te brengen.

55. Kennisgeving van personen die het voorwerp uitmaken van een veiligheidsonderzoek
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.

56. De organisatie van informatiesessies over het gebruik van speciale fondsen
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.

57. De algemene houding inzake loyaliteit op sociale netwerken expliciteren
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 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.

58. Overzenden van alle relevante informatie aan het OCAD
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.

59. Het afsluiten van een samenwerkingsakkoord tussen de inlichtingen- en politiediensten (*supra* 23.)

60. De inkennisstelling van personen die het voorwerp uitmaken van een dreiging
De inlichtingendiensten moeten criteria uitwerken voor het in kennis stellen van personen die het voorwerp zijn van een dreiging (art. 19 W.I&V).

61. Aandacht voor massale data-captatie en politieke en economische spionage
Beide inlichtingendiensten moeten meer aandacht hebben voor de risico's die nieuwe technologische mogelijkheden met zich kunnen brengen op vlak van massale data-captatie en economische en politieke spionage, ook al gaan die uit van 'strategische partners'. Hierover zouden risicoanalyses moeten worden opgesteld, waarbinnen ook aandacht is voor de aanwezigheid van internationale instellingen op Belgisch grondgebied. De aandacht voor deze fenomenen is wat betreft de VSSE en de ADIV noodzakelijk om een goede informatiepositie op te bouwen om de mogelijkheden en de werkwijzen van andere diensten te kennen, niet alleen om desgevallend de overheden in te kunnen lichten of tegenmaatregelen te treffen, maar ook om zijn eigen collecte-technieken te evalueren.

62. Gemotiveerde, consulteerbare en verifieerbare beslissingen
Het Comité was er zich van bewust dat het voor een inlichtingendienst onmogelijk is iedereen die een potentiële dreiging vormt (even intensief) op te volgen, dit gelet op de evidente beperkte middelen. Er dienen dus keuzes te worden gemaakt. Die keuzes moeten gebaseerd zijn op reële analyses die resulteren in gemotiveerde, consulteerbare en verifieerbare beslissingen. Het Comité wees in deze op het feit dat de VSSE zelf de noodzaak

hiertoe heeft erkend in zijn '*Instructie voor de bilaterale samenwerking met de correspondenten*'. Onder de hoofding '*Transparantie en traceerbaarheid*' wordt vereist dat er van elke actie een '*administratief spoor*' bestaat, dit onder meer met het oog op de controle door het Vast Comité I.

III.4. VSSE

63. Naleving van artikel 36bis van de Privacywet
Het Comité beveelt de VSSE aan de nodige stappen te zetten om te voldoen aan de verplichting opgenomen in artikel 36*bis* van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens in het kader van de informatie-uitwisseling met de penitentiaire administratie. Deze bepaling verplicht een dienst vooraf de machtiging te bekomen van het Sectoraal Comité voor de federale overheid voor '*elke elektronische mededeling van persoonsgegevens door een federale overheidsdienst*'.

64. Onderzoek naar informatiestromen en ICT-middelen
Het Vast Comité I beveelt aan dat de VSSE een onderzoek instelt naar haar werkprocessen, de informatiestromen en de ICTmiddelen die het geheel ondersteunen.

65. Een nieuw samenwerkingsprotocol tussen de VSSE en het DG EPI
Het Vast Comité I is van oordeel dat het samenwerkingsprotocol tussen de VSSE en het DG Penitentiaire Inrichtingen in zijn huidige vorm achterhaald is. Het protocol dient te worden aangepast of herschreven zodat het kan anticiperen op toekomstige uitdagingen, zoals nieuwe fenomenen en evoluties in zowel gebruiken als methoden. Ook moeten praktijken die door de jaren heen zijn ontstaan naast het huidige protocol, geïntegreerd of geregulariseerd worden. De al door de VSSE genomen initiatieven buiten het protocol om zouden hierin kunnen bestendigd worden.

66. Betere informatie-uitwisseling en -verwerking tussen de VSSE en het DG EPI
Het Vast Comité I is van oordeel dat bij de informatie-uitwisseling het werken met een vast aanspreekpunt (POC) de voorkeur verdient boven de informatie-uitwisseling via de provincieposten van de VSSE, vermits alle uitgewisselde informatie dient geconcentreerd te worden op de hoofdzetel te Brussel. Ook herinnert het Vast Comité I er aan dat omzichtig moet worden omgesprongen met het gebruik van de diverse lijsten (DG EPI-lijst, JIB-lijst…) en dat de finaliteit van de diverse lijsten duidelijk moet worden vastgesteld en gerespecteerd. Verder moet er een oplossing gevonden worden voor het uitwisselen van 'gedefederaliseerde' informatie en moeten bepaalde ambiguïteiten (zoals de onnodige opsplitsing van diverse modaliteiten van informatie-uitwisseling) worden weggewerkt.

67. Gedocumenteerde werkafspraken tussen de VSSE en de FOD Buitenlandse Zaken
Ondanks het feit dat de FOD Buitenlandse Zaken inzake 'de opvolging van de opvolging van bepaalde diaspora' wordt beschouwd als de belangrijkste klant van de VSSE en zij bovendien de aangewezen dienst is om de VSSE bij te staan in het *counteren* van de activiteiten van de buitenlandse inlichtingendiensten op Belgisch grondgebied, valt de ontstentenis van gedocumenteerde werkafspraken tussen beide instellingen op.

68. Wijziging van de reglementering van de speciale fondsen
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;

69. Het opstellen van een deontologische code
Het Comité had eerder 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 overtredingen. 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.

70. Finaliseren van het arbeidsreglement
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 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.

71. Het afsluiten van een protocolakkoord met de in Brussel gevestigde Europese instellingen
De aanwezigheid op Belgisch grondgebied van internationale instellingen zoals de NAVO, de SHAPE en de Europese Unie maakt van ons land een bevoorrecht doelwit van internationale spionage. Daarom is het noodzakelijk dat België beschikt over goed werkende contraspionagediensten. Op basis van het toezichtonderzoek naar de spionage in het Justus Lipsiusgebouw herhaalde het Comité dan ook zijn aanbeveling om aan de VSSE en de ADIV voldoende menselijke, technische en wettelijke middelen toe te kennen opdat beide diensten deze opdracht op efficiënte wijze zouden kunnen vervullen. Meer specifiek beval het Vast Comité I aan dat de VSSE met de in Brussel gevestigde Europese instellingen een protocolakkoord zou sluiten om de samenwerking en informatie-uitwisseling nader te regelen.

72. Onderzoek instellen naar werkprocessen, informatiestroom en ICT-middelen
Wat betreft de VSSE, stelde het Comité vast dat de concepten die aan de basis van de organisatie van de databank liggen, fundamentele problemen met zich meebrachten omdat ze niet eenduidig werden geïnterpreteerd of als dusdanig werden toegepast. Hierdoor dreigde het inlichtingenwerk aan doelmatigheid en doeltreffendheid te verliezen omdat het risico bestond dat niet (al) de juiste verslagen 'aan de oppervlakte komen' wanneer dit nodig was met het oog op het analysewerk. Ook bestond het risico dat verkeerde conclusies werden getrokken. Het Vast Comité I beval aan dat de VSSE een onderzoek zou instellen naar de werkprocessen, de informatiestroom en de ICTmiddelen die het geheel ondersteunen.

73. Actualiseren van beschikbare informatie in het kader van naturalisaties
Het Comité beval tevens aan dat informatie die door de VSSE wordt aangeleverd in het kader van de verkrijging van de Belgische nationaliteit systematisch wordt geactualiseerd indien die informatie betrekking heeft op '*gewichtige feiten eigen aan de persoon*' en die dus een tegenindicatie kunnen vormen in de toekenning van de Belgische nationaliteit.

74. Beperkingen inzake informatiegaring bij (rechts)personen
De VSSE mag bij elke persoon of organisatie die behoort tot de privésector informatie inwinnen over de dreigingen die ze opvolgt (art. 16 W.I&V). Daarbij blijft de betrokkene weliswaar gebonden door het beroepsgeheim waaraan hij desgevallend is gehouden en door de eisen van de Wet Verwerking Persoonsgegevens. Deze regelingen leggen beperkingen op inzake het meedelen van gegevens aan derden (zoals de VSSE). Daarnaast heeft de burger het recht om niet mee te werken aan een inlichtingenonderzoek. Daarom beval het Vast Comité I aan dat de leden van de VSSE in hun contacten met particulieren aandacht zouden schenken aan de wijze waarop hun optreden door personen die niet gewoon zijn om met de dienst contact te hebben, wordt gepercipieerd. Ook dient in de opleiding aandacht te worden besteed aan de correcte bejegening van de burgers waarmee de leden van de VSSE contact treden.

III.5. ADIV

75. Meer doeltreffend beheer en onderlinge afstemming databanken (eerste stap) – één gecentraliseerde databank (tweede stap)
Het Vast Comité I beveelt – niet voor de eerste maal – aan dat er dringend werk wordt gemaakt van de uitbouw van de databanken van de ADIV (input van gegevens, eenduidige en algemene rubricering van gegevens, toegangsrechten vanuit de verschillende divisies), dat de papieren collecties versneld zouden geïnformatiseerd worden, dat er performante zoeksystemen zouden uitgewerkt worden en dat een aantal gerelateerde problemen (bijvoorbeeld RFIMS, rubricering van binnenkomend informatie bij CCIRM) prioritair worden aangepakt.

76. Gekwalificeerde vertalers voor SIGINT
Het Comité stelde de noodzaak vast aan gekwalificeerde vertalers voor de SIGINT-afdeling van de ADIV.

77. Het nauwer omschrijven en tijdig overzenden van de interceptielijst
De overzending van de interceptielijst loopt al te vaak vertraging op. Het Comité kan hierdoor zijn controletaak niet ten volle waarnemen en dringt er dan ook op aan dat de lijst tijdig wordt overgezonden. Tevens benadrukte het Comité opnieuw dat de interceptieplannen nauwer zouden worden omschreven wat betreft de geviseerde personen en organisaties.

78. Kritische ingesteldheid bij de analyse van gedragingen van personen
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, kunnen onderscheiden van gedrag dat wijst op een radicale en sektarische ontsporing.

79. Wijziging van de reglementering van de speciale fondsen

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 er op 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 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.

80. Aandacht besteden aan tekenen van bekering tot radicale islam

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. 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. 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.

81. Herziening van het veiligheidsreglement
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.

82. Uitvoerige verslaggeving bij veiligheidsincidenten
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.

83. Afsluiten van protocolakkoorden tussen de ADIV en het DG EPI, de Dienst Vreemdelingenzaken en het Commissariaat-generaal voor de Vluchtelingen en de Staatslozen

84. Informatiestromen in ICT-toepassingen optimaliseren
Wat betreft de informatiestromen en ICT-toepassingen binnen de ADIV formuleerde het Comité destijds volgende concrete aanbevelingen: Het *Request for Information (RFI)*-systeem zou de behandeling, de opvolging en de afhandeling van informatieverzoeken (sterk) verbeteren; De aangevatte integratie van de gegevensverzameling en de databanken moet voortgezet en zo mogelijk versneld worden; Om het grote volume aan gegevens en documentatie te kunnen beheersen, moest de ADIV verschillende initiatieven nemen. Vooreerst moest worden bepaald welke informatie nodig was voor het realiseren van de doelstellingen en de af te leveren producten. Daarnaast moest gezorgd worden voor een goede samenwerking tussen de collecte-afdelingen en de analysebureaus. Ten slotte diende evident geïnvesteerd te worden in de absoluut benodigde ICT- en personele middelen. In het algemeen beval het Comité aan voldoende middelen in ICT-technologie te investeren, en dit sneller dan voorzien in de investeringsplannen. Het Comité stelde in 2016 echter vast dat het databeheersysteem van de ADIV nog steeds niet op punt stond. Het beval opnieuw aan dat hier dringend werk zou worden van gemaakt.

85. De bescherming van persoonsgegevens buiten beveiligde sites
De ADIV leverde heel wat inspanningen inzake de bescherming van geclassificeerde gegevens die beveiligde sites verlaten. Het verdient echter aanbeveling dat dezelfde inspanningen zouden uitgaan naar de bescherming van persoonsgegevens die niet noodzakelijk geclassificeerd zijn. Artikel 16 § 4 van de Wet Verwerking Persoonsgegevens van 8 december 1992 eist immers dat de verantwoordelijke voor de verwerking de gepaste technische en organisatorische maatregelen treft ter bescherming van persoonsgegevens tegen onder meer toevallig verlies. Bijkomend beval het Vast Comité I aan voorschriften uit te werken rond de eventuele mededeling van een veiligheidsincident aan de personen over wie infor-

matie verloren ging. Hierbij moet uiteraard een afweging worden gemaakt tussen de risico's voor de dienst en de belangen van de betrokken persoon.

86. Een gegarandeerde vertegenwoordiging bij de Canvek
Het Comité benadrukte het belang van de aanwezigheid van een lid van de ADIV op de vergaderingen van de CANVEK, alhoewel dit niet steeds het geval bleek. De inbreng van de militaire inlichtingendienst in dit adviesorgaan moet gegarandeerd zijn. Dit is uiteraard een van de gevolgen van een meer structureel probleem: de ADIV zet te weinig analysecapaciteit in voor de opvolging van de proliferatie.

87. Aanbevelingen in het kader van buitenlandse missies van de ADIV
Het Vast Comité I: beval aan dat de ADIV de verbanden definieert die tussen operationele, tactische en strategische inlichtingen en de wettelijke opdrachten beschreven in de W.I&V, moeten gelegd worden; raadde de ADIV aan om een bundel op te maken van de teksten die toepasselijk zijn tijdens een ontplooiing van de ADIV, met daarin zowel de internationale als de nationale regels. Wat deze laatste betreft, drong een betere integratie en grotere coherentie van de inhoud zich op; meende dat het noodzakelijk is om de opleiding van het personeel voorafgaand aan het vertrek voor een opdracht te versterken, en spoorde de ADIV aan de al ondernomen verbeteringen voort te zetten; meende dat het noodzakelijk is dat de ADIV de *Comprehensive Preparation of the Operational Environnement*-methode toepast (of elke andere methodologie die hetzelfde doel beoogt) en vooral rekening houdt met de behoeften die de militaire partners in het kader van de voorbereiding van opdrachten uitdrukken; beval aan dat de ADIV ten aanzien van zijn klanten een proactieve houding zou aannemen, om zo meer precies te kunnen bepalen welke hun verwachtingen zijn maar ook om de klanten een duidelijk beeld te verschaffen over wat de ADIV kan aanleveren; raadde de ADIV aan een algemene inschatting te maken van de risico's voor het in de conflictzone ontplooide militair en burgerlijk personeel, en voorstellen te formuleren om met die risico's om te gaan; spoorde de ADIV aan om nader de rol te bepalen van analisten die ingezet worden in een omgeving waar aan collecte wordt gedaan, in het bijzonder met het oog op het garanderen van de objectiviteit van de analysefunctie; raadde de ADIV een meer systematische benadering aan bij het inzetten van het personeel in de conflictzone. Een dergelijke benadering, waarbij vertrokken wordt van de bedreigingen die de ADIV in het kader van de W.I&V moet opvolgen, is fundamenteel ten einde te bepalen welke de in te zetten menselijke en materiële middelen zijn; meende dat het ontplooide ADIV-personeel in de conflictzone over geschikt materieel moest beschikken, in het bijzonder wat betreft de communicatiemiddelen en de voertuigen die ter beschikking van de *Belgian National Intelligence Cell* worden gesteld.

88. Verslagen opstellen van de sweepings
Het Comité aan dat de ADIV verslagen zou opstellen van de *sweepings* die hij uitvoert op verzoek van diverse instanties (in Brussel gevestigde Europese instanties), zeker nu deze gewoonlijk buiten elk protocol om gebeuren.

89. Audit. Aanbevelingen inzake organisatorische voorwaarden noodzakelijk voor een goede inzet van de middelen
De personeels- en organisatiefunctie (P&O-functie) binnen de ADIV moest dringend versterkt worden. Deze versterking was een aanbeveling tot verandering en vormt dus een

conditio sine qua non teneinde andere aanbevelingen met kans op succes uit te kunnen voeren; Het Comité beval aan dat een recurrent proces zou worden opgestart om duidelijke en SMART-geformuleerde doelstellingen – in termen van af te leveren producten en *service levels agreements* (SLA) – te definiëren; Er diende te worden bepaald welke samenwerking tussen en binnen divisies opportuun én noodzakelijk was om deze doelstellingen te realiseren. De voorgestelde producten en SLA moesten daarenboven worden afgetoetst bij de interne en externe gebruikers en 'klanten'; Met het bepalen van de producten en de SLA, moest ook de vereiste personeelsinvestering in termen van tijdsbesteding en competenties worden ingeschat; Het competentiebeheer binnen de ADIV en het afstemmen van taken, functies en competenties vereiste een meer professionele aanpak; Het Vast Comité I was van oordeel dat creativiteit voor een inlichtingendienst een waardevol goed is en dus moest worden gestimuleerd; Voor elke doelstelling moest een planning, de betrokken actoren alsook de wijze van opvolging, worden vastgelegd. Dit was een aanbeveling voor verandering; Er diende in alle collecteplannen te worden bepaald welke de vereiste informatie was om de producten tot stand te kunnen brengen en wie deze informatie kon aanleveren. Met het oog hierop moest een informatiebeheerder worden aangesteld en moest het geautomatiseerde zoeken in bestanden worden vergemakkelijkt; Elke divisie diende periodiek zowel de eigen personeelsleden als deze van andere divisies voor te lichten over 'wie' 'welke' informatie heeft en 'wat' ter beschikking kan worden gesteld; Een *feedback*-mechanisme diende te worden ingebouwd voor alle afgeleverde producten. Ook dienden de interne en externe klanten hierover stelselmatig te worden bevraagd zodat zij een beter inzicht zouden krijgen in hun noden en in wat ze vanwege de ADIV mogen verwachten; De ADIV en de Algemene Directie *Material Resources* van de Krijgsmacht moesten, elk binnen hun budgettaire mogelijkheden, de werkingsmiddelen en de arbeidsomstandigheden permanent trachten te verbeteren. Daarbij moest duidelijk de nadruk liggen op de ICT-middelen, zonder evenwel de veiligheidsaspecten (beveiliging van documenten, infrastructuur en personen) uit het oog te verliezen.

90. Audit. Aanbevelingen inzake het beheer en de leiding van het personeel van de ADIV
Het Vast Comité I beval aan om duidelijke functiebeschrijvingen op te stellen; De (permanente) vorming diende te worden gewijzigd. De actuele en vereiste competenties moesten in kaart worden gebracht, een vormingsplan opgesteld en het in- en externe vormingsaanbod geïnventariseerd; Het Vast Comité I was van mening dat het creëren van een 'inlichtingentak' een aantal van de vastgestelde problemen (gedeeltelijk) kon oplossen en een reële verandering kon teweegbrengen; Er diende te worden verholpen aan de vele geldelijke en administratieve verschillen die bestonden tussen de diverse personeelsgroepen binnen de ADIV en tussen deze van de ADIV en andere diensten uit de inlichtingensector (VSSE en OCAD). Deze verschillen zijn immers nefast voor een degelijk personeelsbeheer; Bijzondere aandacht moest worden besteed aan de *coaching*, begeleiding en ondersteuning van het personeel van de ADIV en dit rekening houdend met hun specifieke situatie; Het Vast Comité I beval aan dat in het kader van de (versterkte) P&O-functie een cel werd opgericht waar de burgerpersoneelsleden terecht kunnen met de problemen die eigen zijn aan hun statuut en situatie; De beoordeling van personeelsleden van de ADIV gebeurde op basis van een reglementair kader dat deze dienst oversteeg. De P&O-functie moet er mee over waken dat de evaluaties goed worden uitgevoerd en begeleid. Ook diende per doelstelling en af te leveren product te worden omschreven op welke wijze de evaluatie zal

gebeuren; Het Vast Comité I beval aan dat de ongelijkheden in het statuut van de personeelsleden binnen de ADIV, werd aangepakt. Daarbij werd bij voorkeur een 'functionele logica' gevolgd in plaats van een 'groepslogica'. De analysefunctie verdiende in dat kader prioritaire aandacht. Immers, daar zijn de grootste verschillen, waardoor sneller een risico op discontinuïteit ontstaat; Het Comité beval aan dat binnen de ADIV een functie werd gecreëerd met als hoofdopdracht 'het beheer van de interne communicatie'.

91. Audit. Aanbevelingen inzake informatiestromen en ICT
Het Vast Comité I was van mening dat het *Request for Information (RFI)*-systeem de behandeling, de opvolging en de afhandeling van informatieverzoeken (sterk) zou verbeteren. Het Comité beval de ADIV aan pas na een bepaalde testperiode te onderzoeken of er zich bijkomend nog een reorganisatie opdrong. In tussentijd kon de ADIV zich concentreren op het technische aspect van het RFI-managementsysteem zonder daarbij onmiddellijk met organisatorische kwesties te worden geconfronteerd; Het Comité beval aan om de aangevatte integratie van de gegevensverzameling en de databanken voort te zetten en zo mogelijk te versnellen; Om het grote volume aan gegevens en documentatie te kunnen beheersen, moest de ADIV verschillende initiatieven nemen. Vooreerst moest worden bepaald welke informatie nodig was voor het realiseren van de doelstellingen en de af te leveren producten. Daarnaast moest gezorgd worden voor een goede samenwerking tussen de collecte-afdelingen en de analysebureaus. Ten slotte diende evident geïnvesteerd te worden in de absoluut benodigde ICT- en personele middelen; In het algemeen beval het Comité aan voldoende middelen in ICT-technologie te investeren, en dit sneller dan voorzien in de investeringsplannen.

92. Audit. Aanbeveling inzake risicobeheer
Het Comité beval aan acties te ondernemen om de risico's inzake discontinuïteit van de functie-uitoefening en verlies van kennis te beperken. Meer bepaald diende een previsioneel personeelsbeheer te worden gevoerd, diende de creatie van een 'inlichtingentak' (waarbij het verlies aan kennis minder groot was en de vervanging van personen vlotter kon verlopen) te worden overwogen en diende – opnieuw – geïnvesteerd in ICT; Het was aangewezen dat er binnen de ADIV uitgesproken aandacht werd betoond voor kennismanagement. Er moesten duidelijke instructies worden uitgewerkt om de aanwezige kennis in kaart te brengen, de relevantie ervan te beoordelen en maatregelen te nemen om ze op te slaan, te bewaren en te verspreiden. Het strekte tot aanbeveling binnen elke divisie een kennisbeheerder aan te stellen die het kennismanagement ondersteunt; Het Vast Comité I meende dat het risico op 'pragmatische prioriteitvorming' beperkt was, maar dat er wel waakzaamheid aan de dag moest worden gelegd. Een goede werving en een uitgebouwd systeem van functiebeschrijvingen kon dit risico nog inperken; Het Vast Comité I beval aan dat de ADIV werk zou maken van het ontwikkelen van het risicobeheer.

III.6 OCAD

93. Het optimaliseren van het personeelsstatuut
De Vaste Comités I en P bevelen het OCAD aan om geen detachering van niet-statutaire overheidsfunctionarissen, afkomstig uit steundiensten toe te laten, zonder een eventuele wijziging van de wet; de administratieve situatie van de gedetacheerde personen te regu-

lariseren; een personeelsdossier voor elk lid van het personeel aan te leggen, zonder onderscheid te maken of het gaat om een statutair personeelslid, een gedetacheerd personeelslid of zelfs een lid van de directie; aan de bevoegde ministers voorstellen toe te zenden tot wijziging van het Koninklijk besluit dat het statuut van het statutair en gedetacheerd personeel vastlegt; erover te waken dat bij elke beslissing om een einde te maken aan een detachering op disciplinaire gronden *sensu lato* genomen wordt zonder miskenning van het beginsel van behoorlijk bestuur dat inhoudt dat de betrokken persoon, die het voorwerp uitmaakt van een beslissing, moet worden gehoord.

94. Het gebruik van sociale netwerkdiensten door personeelsleden van het OCAD
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 voorzichtigheid die wordt verwacht van zijn medewerkers op sociale media en met betrekking tot de controlemiddelen die daartoe kunnen worden aangewend; 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, 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-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: de intrekking van de veiligheidsmachtiging, een tuchtvervolging overeenkomstig het tuchtstelsel van de analisten van het OCAD, 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.

95. Transparante en traceerbare contacten van het OCAD met gelijkaardige buitenlandse diensten
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)

96. Aanstellen centrale contactpunten in ondersteunende diensten van het OCAD
Het aanstellen van een duidelijk centraal contactpunt in elke ondersteunende dienst wordt aanbevolen. Het centrale contactpunt moet een volledig zicht hebben op de uitgewisselde info,

97. De traceerbaarheid van inlichtingen van ondersteunende diensten garanderen
Binnen elke ondersteunende dienst moet de traceerbaarheid van de inlichtingen gegarandeerd worden.

98. Uitklaren van de embargoporcedures
De begripsverwarring inzake diverse embargoprocedures moet verhelderd worden. De draagwijdte van de embargoprocedure voor het analysewerk van het OCAD moet gepreciseerd worden. Er dient voorzien te worden in een procedure bij een meningsverschil over het gebruik en de verspreiding van onder embargo aangeleverde informatie. De toepassing van de embargoprocedure moet kunnen gecontroleerd worden.

99. Verwarring omtrent de identiteit van het OCAD uitklaren
Het verdient aanbeveling dat het OCAD er steeds zou over waken dat er omtrent zijn unieke identiteit geen enkele verwarring kan ontstaan. Het OCAD is, in tegenstelling tot de ADIV en de VSSE, namelijk geen inlichtingendienst. Een actieve en consequente aandacht hiervoor in zijn communicatie en werking, en dit zowel in het binnen- als het buitenland, was dan ook essentieel. In dit kader verdiende het aanbeveling dat het OCAD uiterst behoedzaam is bij het ondernemen van buitenlandse zendingen en dat het zijn studiereizen strikt zou aflijnen.