RAPPORT D'ACTIVITÉS 2016
ACTIVITEITENVERSLAG 2016

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.

RAPPORT D'ACTIVITÉS 2016

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 2016* a été approuvé par le Comité permanent de contrôle des services de renseignements et de sécurité lors de la réunion du 26 septembre 2017.

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

Rapport d'activités 2016
Comité permanent de contrôle des services de renseignements et de sécurité

ISBN 978-94-000-0897-7
D/2017/7849/129
NUR 823

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

A.M.	Arrêté ministériel
Ann. parl.	Annales parlementaires
ANS	Autorité nationale de sécurité
A.R.	Arrêté royal
AR C&HS	Arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
AR 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
BISC	*Belgian Intelligence Studies Centre*
CCB	Centre pour la cybersécurité Belgique
CCIRM	*Collection coordination and intelligence requirements management*
CEDH	Convention européenne des droits de l'homme
CGRA	Commissariat général aux réfugiés et apatrides
CHOD	*Chief of Defence*
CIC	Code d'instruction criminelle
Comité permanent P	Comité permanent de contrôle des services de police
Comité permanent R	Comité permanent de contrôle des services de renseignement et de sécurité
Commission BIM	Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité
Commission vie privée	Commission de la protection de la vie privée
COPPRA	*Community policing and prevention of radicalisation and terrorism*
CNCIS	Commission nationale de contrôle des interceptions de sécurité
CNCTR	Commission nationale de contrôle des techniques de renseignement

CNS	Conseil national de sécurité
COC	Organe de contrôle de l'information policière
CP	Code pénal
CPE	Commission d'enquête parlementaire
CRIV	Compte Rendu Intégral – *Integraal Verslag*
CTG	*Counter Terrorism Group*
CTIF	Cellule de traitement des informations financières
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten*
DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
DGCC	Direction générale du centre de crise
DG EPI	Direction générale des Établissements pénitentiaires
DGEPM	Direction générale Exécution des Peines et des Mesures
DGTA	Direction générale Transport aérien
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*
GCHQ	*General Communications Headquarters*
HUMINT	*Human intelligence*
ICT	*Information and communications technology*
IMINT	*Image intelligence*
IOB	*Intelligence Outlook Bulletins*
IOCCO	*Interception of Communications Commissioner's Office*
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
MRD	Méthodes de recueil des données
NRBC (armes)	(Armes) nucléaires, radiologiques, chimiques et biologiques
NSA	*National Security Agency*
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*
OVG	*Operation Vigilant Guardian*
PES	Potentiel économique et scientifique
PNR	*Passenger Name Record*
POC	*Point of contact*
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
RFI	*Request for information*
SGRS	Service Général du Renseignement et de la Sécurité
SIGINT	*Signal intelligence*
SLA	*Service Level Agreement*
SOCMINT	*Social media intelligence*
SPF	Service public fédéral
TFUE	Traité sur le fonctionnement de l'Union européenne
VSSE	Sûreté de l'État

PRÉFACE

Les attaques terroristes qui ont frappé l'Europe ces dernières années ont un impact considérable. On ne s'étonnera donc pas que la question de la sécurité constitue une priorité. Le radicalisme et le terrorisme sont devenus une réalité quotidienne. Cela vaut également pour l'espionnage et l'ingérence politique étrangère. Étant donné les risques de désorganisation pour notre société, ces pratiques doivent être combattues. Pouvoir vivre en sécurité est, en effet, un droit humain fondamental. Et les autorités ont le devoir de garantir cette sécurité.

Les nouvelles initiatives, nombreuses, qui ont été prises en la matière, exercent une influence profonde sur l'équilibre précaire entre, d'une part les droits et les libertés du citoyen, et d'autre part la limitation (temporaire) de ces droits et libertés, en raison des risques qu'il encourt pour sa sécurité.

Le Comité permanent R est lui aussi confronté à cette recherche d'un certain équilibre. À l'instar d'autres institutions à dotation[1], le Comité a été instauré pour remplir ses missions de contrôle de manière indépendante et impartiale, entre autres pour donner l'assurance au citoyen que les droits qui lui sont conférés par la loi, voire par la Constitution, sont et demeurent garantis. Dans les rapports au sein des trois pouvoirs d'un État de droit démocratique, il est d'une importance capitale que le système des '*checks and balances*' puisse être appliqué de manière correcte et efficace. Un parlement qui, notamment par le biais du Comité permanent R, peut exercer sa mission de contrôle de manière efficace, a sans aucun doute sa place dans ce processus.

La qualité du travail que ces institutions à dotation peuvent fournir est non seulement essentielle pour garantir les droits du citoyen, mais constitue aussi un facteur nécessaire de la confiance que les diverses structures étatiques doivent pouvoir inspirer à ce citoyen.

Toutefois, dans une société en mutation, où les risques sécuritaires et les restrictions budgétaires vont croissant, exercer la mission de sauvegarde des droits fondamentaux des citoyens est toujours plus ardu. Sans compter les missions (de contrôle) toujours plus nombreuses qui ont été confiées ces

[1] Il s'agit du Comité permanent de contrôle des services de police, de la Commission de la protection de la vie privée, de l'Organe de contrôle de l'information policière, du Médiateur fédéral, du Conseil supérieur de la Justice, de la Commission BIM et des Commissions de nomination réunies pour le Notariat. En 2017, ces institutions ont informé le président de la Chambre des Représentants, dans un courrier commun, des conséquences des restrictions budgétaires.

dernières années par les pouvoirs exécutif et législatif au Comité permanent R. Pourtant, des moyens supplémentaires n'ont pas été prévus pour assurer ces nouvelles missions.[2]

Les institutions à dotation doivent faire face à un manque criant de moyens. Le Comité permanent R ne fait pas exception. On devine sans peine que davantage d'économies, d'une part, et davantage compétences, d'autre part, auront un impact sur la qualité du fonctionnement du Comité. Le Comité permanent R est convaincu de la nécessité d'un débat sur les moyens limités. Mais un tel débat ne doit pas seulement être mené dans le cadre de l'application d'un certain nombre de normes budgétaires, il doit l'être tout autant dans le cadre des équilibres indispensables qui doivent pouvoir jouer dans un État de droit démocratique.

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

26 septembre 2017

[2] En octobre 2016, le Comité a fait part de ses inquiétudes à la Commission de la Justice de la Chambre, en pleine discussion sur la modification de Loi organique des services de renseignement et de sécurité. Par cette loi, les services de renseignement se voient attribuer de nouvelles compétences qui doivent être contrôlées par le Comité permanent R.

CHAPITRE I
LE SUIVI DES RECOMMANDATIONS DU COMITÉ PERMANENT R

Chaque année, le Comité permanent R formule, pour les pouvoirs législatif et exécutif, des recommandations qui portent en particulier sur la légitimité, la coordination et l'efficacité de l'intervention des deux services de renseignement belges, de l'OCAM et, dans une moindre mesure, de ses services d'appui. Les recommandations émises par le Comité en 2016 figurent au dernier chapitre du présent rapport d'activités.

Il est de tradition que le premier chapitre énumère les principales initiatives prises l'année précédente par les différents acteurs, dans la lignée des recommandations du Comité permanent R, et qu'une attention particulière soit portée aux recommandations que le Comité estime essentielles, mais qui n'ont pas encore été mises en œuvre.

Le *Rapport d'activités 2006* avait déjà offert un aperçu des recommandations les plus importantes que le Comité permanent R et sa Commission de suivi avaient formulées entre 1994 et 2005, et un aperçu du suivi qui leur avait été réservé.[3]

Le Comité permanent R s'était proposé de procéder 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 du *Rapport d'activités 2015*, il a, en effet, été suggéré que 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 »*.[4] Cette liste de recommandations devait se présenter sous la forme d'un tableau de bord.

Le Comité a démarré ce projet en 2016. Toutefois, d'autres priorités – en particulier les missions assignées dans le cadre de la commission d'enquête parlementaire sur les attentats de Bruxelles et la genèse de la transaction pénale

---

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

4 *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.

élargie – ont bousculé le programme. Cette mission n'a donc pas pu être finalisée. Toutefois, à la mi-2016, les enquêtes de contrôle du Comité permanent R relatives au terrorisme et au radicalisme, ainsi que le suivi qui y a été réservé, ont été envoyées, et ce à la demande du Président de la commission parlementaire sur les attentats (voir Chapitre V).

La mission de la Commission de suivi a été reprise et affinée par le Comité permanent R en 2017. Le Comité est occupé à examiner quelles recommandations ont déjà été concrétisées pour cette période, et à vérifier si les recommandations qui ne l'ont pas été sont toujours d'actualité. Ces recommandations seront reformulées si cela s'avère nécessaire et utile. Le rapport est prévu pour la fin 2017.

CHAPITRE II
LES ENQUÊTES DE CONTRÔLE

En 2016, le Comité permanent R a finalisé quatorze rapports d'enquête, dont trois avec le Comité permanent P (II.1 à II.14). En outre, le Comité permanent R a ouvert, en 2016, trois nouvelles enquêtes de contrôle, dont une avec le Comité permanent P. Cette enquête de contrôle a été initiée à la demande de la Commission de suivi; les deux premières l'ont été à l'initiative du Comité permanent R. Une d'entre elles – à savoir l'enquête relative aux attentats de Zaventem et de Maelbeek (II.4) – a encore été finalisée en 2016. Les deux autres enquêtes qui ont été ouvertes sont brièvement décrites au point II.15.

Au total, le Comité a reçu 29 plaintes ou dénonciations en 2016. Depuis cette année, le processus de travail 'plaintes et dénonciations' fait l'objet d'un assouplissement, d'une déformalisation et d'une standardisation.[5] Après vérification de plusieurs données objectives, le Comité a rejeté toutes ces plaintes ou dénonciations, soit parce qu'elles étaient manifestement non fondées (art. 34 L.Contrôle), soit parce que le Comité n'était pas compétent pour en traiter les griefs. Dans ces derniers cas, les plaignants ont été renvoyés, si possible, aux instances compétentes (le Comité permanent P, la Police fédérale, le Procureur du Roi). Aucune des plaintes introduites en 2016 n'a donné lieu à l'ouverture d'une enquête de contrôle, tandis qu'une plainte a été insérée dans un dossier d'information en cours.

II.1. LA PROBLÉMATIQUE DES *FOREIGN TERRORIST FIGHTERS*

Depuis 2013, la zone de combat syrienne exerce un fort pouvoir d'attraction sur ce que l'on appelle les *foreign terrorist fighters* (FTF)[6] venus des quatre coins du

---

5 Dans un premier temps, la recevabilité/le bien-fondé de la plainte sont examinés avant qu'elle ne soit traitée par le service d'Enquêtes R. En cas de 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).

6 Le Comité évoquait plutôt les personnes parties combattre en Syrie; des personnes qui sont parties en Syrie ou dans les pays limitrophes (zones de conflit djihadistes) ou en sont revenues (*returnees*) et qui participent à la lutte armée aux côtés de groupements terroristes, également appelées *foreign fighters*. La Circulaire du 21 août 2015 des ministres de l'Intérieur et de la

monde. Il s'est avéré que, proportionnellement, de nombreux combattants venaient de Belgique.

Aussi le Comité permanent R a-t-il décidé, en octobre 2014, d'ouvrir une enquête de contrôle relative *« à la position d'information des deux services de renseignement (VSSE et SGRS) sur le recrutement, l'envoi, le séjour et le retour en Belgique de jeunes (belges et étrangers résidant en Belgique) qui partent ou sont partis combattre en Syrie ou Irak et au transfert des renseignements aux diverses autorités »*. L'enquête devait répondre aux questions suivantes : quelle était la mission des services de renseignement dans ce contexte et de quelle manière a-t-elle été dirigée ? Les services avaient-ils une vue sur la phase de recrutement et sur la phase de départ ? Étaient-ils en mesure de se faire une idée de qui partait combattre en Syrie ? Connaissaient-ils les activités de ces combattants sur place ? L'évolution de la situation à l'étranger se traduisait-elle par d'éventuelles menaces en Belgique, et si oui, lesquelles ? Et qu'en était-il du suivi et de l'approche de leur retour en Belgique ? Comment la collaboration (entre le SGRS, la VSSE, l'OCAM mais aussi la police) s'est-elle déroulée en la matière ? Comment ont-ils fait rapport et à qui ?…

Un premier rapport intermédiaire a été établi début 2015[7], tandis que le rapport a été finalisé en février 2016.

II.1.1. UNE ÉVOLUTION CONSTANTE

La problématique et l'approche des *foreign terrorist fighters* n'ont cessé d'évoluer. Les services de renseignement ont adapté leurs priorités et instauré des changements structurels et organisationnels. Le Parlement a quant à lui précisé le cadre réglementaire, et le gouvernement a pris toutes sortes d'initiatives.[8]

Justice et la COL 10/2015 du Collège des Procureurs généraux sont plus complètes, faisant référence aux *foreign « terrorist » fighters*. Tant la Circulaire que la COL 10/2015 définissent six catégories, en fonction du statut de la personne : (1) celles qui sont présumées se trouver dans une zone de conflit djihadiste, (2) celles qui sont en route vers une zone de conflit djihadiste (3) celles qui reviennent vers la Belgique ou y sont revenues, en provenance d'une zone de conflit djihadiste (*returnees*) ; (4) celles qui reviennent vers la Belgique après avoir été en route vers une zone de conflit djihadiste ; (5) celles pour lesquelles des indices sérieux existent indiquant qu'elles partiront vers une zone de conflit djihadiste et (6) l'aide et le recrutement.

7 Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2015*, 21-25 ('II.4. Le suivi par les deux services de renseignement belges de personnes parties combattre en Syrie : rapport intermédiaire'). L'impact de cette problématique sur le fonctionnement de la VSSE et du SGRS y était repris, de même que les moyens mobilisés par les deux services. Les problèmes et les risques organisationnels auxquels les deux services de renseignement étaient confrontés ont eux aussi été développés.

8 Dans ce contexte, le Comité se référait, entre autres, à la Circulaire du 25 septembre 2014 relative à la gestion de l'information et aux mesures de suivi concernant les *foreign fighters* séjournant en Belgique.

Dès 2014, la direction de la VSSE avait envisagé d'apporter des adaptations importantes à sa stratégie et à son organisation. Dans l'intervalle, le gouvernement a pris plusieurs décisions visant à renforcer le service et lui a alloué des ressources complémentaires. Dans le cadre de la mission de renseignement, 'la lutte contre les combattants djihadistes' était l'une des trois priorités du Plan d'action 2015. La structure du service a également subi des modifications substantielles.[9]

Les principaux destinataires des notes de la VSSE étaient surtout le Parquet fédéral/le Procureur fédéral, suivis par l'Office des étrangers et l'OCAM. Il y avait assez peu d'échanges d'informations avec le SGRS.[10] Le nombre de notes stratégiques était relativement peu élevé. Les méthodes de recueil des données étaient utilisées majoritairement pour les *foreign fighters* : quelque 60 % de toutes les MRD mises en œuvre par la VSSE (principalement l'identification, la localisation…) entre juin et octobre 2015 étaient liées à cette problématique.

Le SGRS considérait lui aussi avoir pour mission, au vu de ses spécialités (majoritairement orientées vers l'étranger) et des ressources de collecte spécifiques, de fournir à différentes instances et aux diverses plateformes de concertation (comme les *local task forces*) des renseignements concernant les menaces pesant sur des Belges ou des intérêts belges à l'étranger, mais aussi concernant l'impact de phénomènes étrangers sur la Belgique. Le SGRS déployait à cet effet un large éventail de moyens de collecte (HUMINT, SIGINT, IMINT, OSINT et SOCMINT).

L'organisation des services de renseignement, mais également les structures de collaboration au sens plus large du terme (par exemple, la *National Task Force* (NTF) et les *local task forces* (LTF)) ont été remodelées en vue d'adopter une approche plus ciblée et plus rationalisée, ce qui impliquait la disparition, au 1er septembre 2015, de la *'Taskforce foreign fighters'* et de la *'Platform returnees'*. D'autres structures du Plan R – la *National Task Force* (NTF) et les *local tasks forces* (LTF) – ont été actualisées. La *National Task Force* a été étendue par la nomination de représentants des Régions et des Communautés, et un 'groupe de travail FTF' a été constitué sous la NTF. Au niveau de l'arrondissement, les LTF sont constituées d'une composante stratégique et, au niveau local, d'une composante opérationnelle.

L'approche concrète des FTF revêtait plusieurs aspects : constater l'absence ou la présence d'un *foreign fighter*, vérifier et étoffer les informations ainsi qu'évaluer la menace individuelle et le suivi (normalisé et personnalisé) de cette personne. Sur ce plan, tous les services concernés se sont vu confier des tâches clairement

9 Au moment de l'enquête, il était encore trop tôt pour évaluer dans quelle mesure la nouvelle structure contribuait efficacement à l'élaboration d'une meilleure position d'information à l'égard des *foreign terrorist fighters*. Il était toutefois clair que cette thématique avait un impact non négligeable sur le fonctionnement et la charge de travail de la VSSE.

10 Environ 60 % des notes officielles transmises aux autorités belges (notes aux autorités (NA)) étaient destinées au Parquet fédéral ou au Procureur fédéral, 17 % à l'Office des étrangers, contre 6 % seulement au service de renseignement militaire.

décrites. En 2016, il a été décidé d'instaurer une 'base de données dynamique' afin de gérer et de partager les informations.[11]

II.1.2. LE CADRE LÉGAL[12]

II.1.2.1. La Sûreté de l'État

En vertu des articles 7, 1° et 8, 1° b) et c) L.R&S, relatifs aux menaces terroristes et extrémistes, la VSSE est habilitée à recueillir des renseignements concernant toute personne ayant l'intention de rejoindre la zone de conflit djihadiste en Syrie et en Irak, se trouvant sur place ou en revenant. Les personnes qui participaient (ou souhaitaient participer) à ces combats constituaient un risque potentiel ou réel pour la sûreté intérieure et extérieure du pays.

Dans ce contexte, la VSSE pouvait faire usage de toutes ses compétences, et ce dans le cadre de l'extrémisme et du terrorisme (méthodes ordinaires, spécifiques et exceptionnelles). Les méthodes exceptionnelles ne pouvaient être utilisées *stricto sensu* dans la lutte contre une menace purement extrémiste. Mais ce constat est à nuancer, dans le sens où ces méthodes peuvent tout de même être utilisées dans la lutte contre des processus de radicalisation. Alors qu'en théorie, les méthodes de renseignement ordinaires pouvaient également être utilisées à l'étranger, ce n'était pas le cas des méthodes spécifiques et exceptionnelles, dont l'application était limitée au territoire belge (art. 18/1, 2° L.R&S).[13]

Pour savoir si les informations collectées par la VSSE devaient ou pouvaient être transmises à des tiers, tout dépendait du service concerné et de la nature des informations. L'article 19 L.R&S permet à la VSSE de communiquer tous les renseignements et toutes les informations aux services de police et aux autorités judiciaires si ceux-ci sont pertinents dans le cadre de la finalité de leurs missions. Les informations indiquant une possible infraction devaient donc, en vertu de l'article 29 CIC ou de l'article. 19/1 L.R&S (et dans ce dernier cas également via la Commission BIM), être communiquées aux autorités judiciaires. En ce qui concerne la transmission d'informations à des services étrangers, le Comité permanent R a déjà souligné à plusieurs reprises que le cadre légal n'était pas suffisant, surtout en ce qui concerne la transmission de données à caractère personnel.[14]

---

11 Voir à ce propos : 'Chapitre VI. Le contrôle de banques de données communes'.

12 Différents aspects ont été modifiés après la clôture de l'enquête de contrôle par l'entrée en vigueur de 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* CP, *M.B.* 28 avril 2017. Cette nouvelle loi a rendu obsolètes plusieurs constats repris ci-après.

13 Les deux limitations ont été supprimées à la faveur de la Loi du 30 mars 2017 (*supra*).

14 La Directive du 26 septembre 2016 du Conseil national de sécurité 'concernant les relations des services de renseignement belges avec les services de renseignements étrangers' y remédie partiellement.

Enfin, les articles 9, 11 § 3 et 20 L.R&S assignent aux services de renseignement de collaborer le plus efficacement possible entre eux, mais aussi, par exemple, avec d'autres autorités administratives, services de police, autorités judiciaires (p. ex. sous la forme d'une assistance technique) et avec des services de renseignement étrangers. En ce qui concerne 'l'assistance technique' prêtée à la justice, le Comité a déjà plusieurs fois attiré l'attention sur le fait qu'une interprétation restrictive de cette disposition n'autorisait pas la VSSE (ni le SGRS) à utiliser les compétences de renseignement à des fins judiciaires.[15] Le Comité a pu constater que dans la problématique syrienne, la VSSE, en sa qualité d'expert, offrait de plus en plus souvent une assistance technique à la justice, et ce à différents niveaux. Le Comité a pu constater que les prescriptions légales avaient été respectées.

II.1.2.2. Le Service Général du Renseignement et de la Sécurité

En ce qui concerne le SGRS, la Loi du 30 novembre 1998 comportait trois points d'ancrage pour la collecte et le traitement de données concernant les *foreign terrorist fighters*.[16] Tout d'abord, il y avait « *l'accomplissement des missions des forces armées* » ; c'est-à-dire « *toute manifestation de l'intention de neutraliser, d'entraver, de saboter, de porter atteinte ou d'empêcher la mise en condition, la mobilisation et la mise en œuvre des Forces armées belges, des forces armées alliées ou des organismes de défense interalliés lors de missions, actions ou opérations dans le cadre national, dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale* » (art. 11 § 2, 3° L.R&S). La préservation de « *l'accomplissement des missions des forces armées* » permet de suivre toute « *activité* » (art. 11 § 1, 1° L.R&S) ou, mieux encore, toute « *manifestation de l'intention* » (art. 11 § 2, 3° L.R&S) pouvant mettre cet intérêt en péril. Contrairement à la VSSE, il ne doit pas nécessairement être question d'une menace (comme l'extrémisme ou le terrorisme).[17] Les activités extrémistes et terroristes de personnes se trouvant à l'étranger (*foreign fighters*), mais aussi en Belgique (par exemple, des extrémistes au sein de l'armée), font également l'objet de la mission de renseignement du SGRS. Toutefois, il convient de souligner que le SGRS, contrairement à la VSSE, n'est pas compétent pour suivre des phénomènes comme 'l'extrémisme' et le 'terrorisme'. En ce sens, le Comité permanent R avait déjà estimé que « *le suivi de l'islamisme*

15 Si, dans le cadre d'une enquête judiciaire, certains actes d'information doivent être posés, on ne peut recourir à des méthodes particulières de renseignement ; il convient d'utiliser les méthodes de recherche judiciaires appropriées (telles que les méthodes particulières de recherche).

16 La Loi du 30 mars 2017 (*supra*) a également modifié en profondeur la description des compétences du SGRS.

17 Le premier intérêt que le service de renseignement militaire doit protéger doit faire l'objet d'une menace bien déterminée avant que celui-ci ne soit compétent : un « *moyen de nature militaire* » doit être utilisé (art. 11 § 2 1° L.R&S).

radical entrait bien dans les compétences du SGRS, mais seulement dans la mesure où la sécurité militaire au sens large était en jeu, non seulement en Belgique mais aussi à l'étranger».[18] Le deuxième point d'ancrage était la sécurité des ressortissants belges à l'étranger. À cet égard, le SGRS devait prêter attention à «*toute manifestation de l'intention de porter collectivement atteinte, par la dévastation, le massacre ou le pillage, à la vie ou à l'intégrité physique de ressortissants belges à l'étranger et des membres de leur famille*». L'enquête de contrôle a cependant démontré que les analyses du SGRS allaient au-delà de la «*sécurité militaire*» ou de la «*protection de Belges à l'étranger*». Le troisième point d'ancrage était «*la protection et la survie de la population*», auxquelles il est clairement porté atteinte avec «*des moyens de nature militaire*», vu les (tentatives d') attentats.

À cet égard, le SGRS pouvait recourir à l'interception de communications envoyées depuis l'étranger (art. 259*bis* CP).[19] De telles interceptions étaient possibles dans le cadre de l'opération militaire menée contre l'EI (par exemple par la présence de F16), aux fins de la protection de Belges à l'étranger (principalement dans la région concernée) et de la population belge dans son ensemble. Dans le contexte de la problématique syrienne, les activités SIGINT ne pouvaient être menées pour d'autres motifs.

La mise en œuvre de méthodes de renseignement ordinaires était autorisée (même à l'étranger), mais dans la mesure où la collecte présentait un lien avec une menace pouvant être suivie par le SGRS. Bien évidemment, le SGRS pouvait, dans le cadre de la problématique syrienne, utiliser des méthodes de renseignement spécifiques ou exceptionnelles en présence d'une menace visant un intérêt à défendre parmi ceux qui sont énumérés dans la loi. La mise en œuvre de telles méthodes devait cependant être limitée au territoire belge (art. 18/1, 2° L.R&S).[20]

À l'instar de la VSSE, le SGRS devait collaborer de la manière la plus efficace possible avec d'autres autorités, sans utiliser de méthodes ne relevant pas de sa sphère de compétences, et uniquement pour appuyer la mission d'un autre service.

II.1.3. ÉVALUATION DE LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT

Par 'position d'information', il y a lieu d'entendre l'ensemble des renseignements dont un service de renseignement dispose au sujet notamment d'un thème, d'une

18 COMITÉ PERMANENT R, *Rapport d'activités 2007*, 31-32.

19 Modifié par l'entrée en vigueur de 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.* 28 avril 2017.

20 Modifié par la Loi du 30 mars 2017 (*supra*).

personne ou d'un événement spécifique. Dès le début de l'enquête de contrôle en octobre 2014, la VSSE affirmait avoir une position d'information relativement bonne sur la problématique syrienne. Il a toutefois été souligné que le service n'avait aucune idée des activités menées en Syrie et en Irak par environ la moitié des individus 'belges' (personnes séjournant dans notre pays, indépendamment de leur nationalité). À ce moment-là, le SGRS affirmait que sa position d'information ne lui permettait pas d'atteindre son niveau d'ambition. Le SGRS a apporté sa contribution au dossier syrien, mais celle-ci devait clairement être renforcée par un appui plus professionnel de sa capacité d'analyse et par l'utilisation de nouvelles techniques de collecte. À cet égard, le service faisait référence à un certain nombre de limitations.

Il y avait peu d'éléments (mesurables) permettant de procéder à une évaluation qualitative des produits finis et à l'évaluation de la position d'information d'un service de renseignement. Le Comité n'a donc pas évolué la position de renseignement en tant que telle, mais plutôt les processus de renseignement ayant conduit à cette position. Ils ont été comparés à plusieurs éléments formels (ci-après nommés les 'points de mesure') offrant, en termes de procédure, la garantie d'une position d'information obtenue de manière qualitative.[21] Cette approche constituait, dans le même temps, une forme d'analyse de risques : si certaines procédures ou certains processus de travail n'étaient pas suivi(e)s, cela pouvait être une indication que la position de renseignement reposait sur des bases peu solides.

II.1.3.1. Collecte de données et sources

La collecte de données et les sources constituaient le premier point de mesure. Le Comité a estimé que ni la VSSE ni le SGRS ne présentaient de risques spécifiques à ce niveau. La manière dont la collecte avait lieu ne présentait pas de risque spécifique pour le produit final. Dans leurs activités de collecte, les deux services recouraient à diverses disciplines, méthodes et sources en ce qui concerne les FTF. Dans le cas de la VSSE, ce sont surtout le HUMINT et les MRD qui étaient privilégiés. Les données qui étaient *in fine* transformées en renseignements étaient – dans la mesure du possible et au vu des circonstances – assez complètes et précises ; elles tentaient d'apporter une réponse aux questions qui ? quoi ? pourquoi ? quand ? et où ? Les informations étaient également transmises telles qu'elles avaient été formulées ou communiquées par la source ; autrement dit, elles étaient 'objectives'.[22] La manière dont les données relatives aux *foreign*

[21] Le Comité s'est basé sur la méthodologie de DE VALK et a opté pour un large échantillonnage. Voir : G.G. DE VALK, *Dutch Intelligence. Towards a Qualitative Framework for Analysis. With Cases Studies on the Shipping Research Bureau and the National Security Service (BND)*, Rijksuniversiteit Groningen, 2005.

[22] Le Comité a toutefois constaté qu'au SGRS, l'évaluation des sources n'était pas systématique, et que le service n'avait pas toujours suffisamment d'informations à leur propos.

terrorist fighters étaient collectées était donc relativement bonne. À tout le moins en ce qui concerne les procédures, on peut avancer que les deux services prenaient des mesures pour établir au mieux leur position d'information.

II.1.3.2. La gestion des données et des connaissances

Un deuxième point de mesure concernait la manière dont les données étaient sauvegardées, classées et gérées (la gestion des données et des connaissances).

Le système de gestion des données utilisé par la VSSE constituait une base solide pour le travail de renseignement, mais restait perfectible. Il n'était pas assez standardisé et présentait des redondances.

La gestion de données au sein du SGRS constituait un risque majeur. La manière dont les informations étaient enregistrées et gérées dans ce service était plutôt problématique. Non seulement rechercher des informations prenait du temps, mais trouver les informations correctes et complètes n'était pas non plus garanti. Lorsqu'il s'agissait de 'relier les points' (*connecting the dots*), le SGRS courait le risque que certaines données ne soient pas disponibles ou ne le soient pas assez rapidement, soit parce que le moteur de recherche ne les trouvait pas (par exemple, en raison de la problématique des dossiers distincts entre les divisions), soit simplement parce qu'elles n'avaient pas été téléchargées (*input* insuffisant dans la base de données). Dans le cadre de l'évaluation de l'élaboration de la position d'information du SGRS, il s'agissait d'un problème qui persistait depuis de nombreuses années et qui hypothéquait sérieusement la qualité de la position d'information.

II.1.3.3. Les processus d'analyse

La manière dont les informations entrantes sont analysées pour devenir des 'renseignements' (les processus d'analyse) constituait le troisième point de mesure. Le Comité a examiné la manière dont les documents d'analyse relatifs à la problématique syrienne étaient établis et quelle était la base méthodologique. L'utilisation de méthodes s'appuyant sur une base méthodologique solide est en effet essentielle pour garantir la qualité du produit fini.

Le Comité a dû constater, en ce qui concerne la VSSE, que les services d'analyse disposaient d'une boîte à outils (*toolbox*) spécifique, mais qu'ils n'utilisaient pas ces méthodes de manière systématique. Selon le service, ce manque de systématisme était compensé par le fait qu'un analyste ne se retrouvait jamais seul face à un problème, mais que ses collègues et sa hiérarchie veillaient également à la bonne qualité du produit.

Au SGRS, le service CI/homeland était plus avancé que la Division I dans le domaine de l'utilisation d'instruments et de méthodes d'analyse. La Division I avançait les mêmes arguments que la VSSE, à savoir que la qualité du produit ne

dépendait pas seulement de l'utilisation de méthodes formelles (qui demandent parfois beaucoup de temps et/ou sont trop théoriques), mais que la qualité est aussi garantie par l'interaction entre les différents analystes et leur hiérarchie.

Tant pour la VSSE que pour le SGRS, on trouve des avantages et des inconvénients à l'utilisation de méthodes rigoureuses ou non. Ce qui importe, c'est d'en être conscient (évaluation des risques).

II.1.3.4. Besoins des utilisateurs et feedback

Dans le quatrième point de mesure, la question était de savoir si le produit répondait aux besoins de l'utilisateur (*fit for use*) et s'il y avait un feedback. Le Comité a constaté à cet égard plusieurs lacunes pouvant avoir des retombées négatives sur les processus de renseignement, et donc sur les produits qui en découlent. Il convient de noter que ces lacunes n'étaient pas forcément imputables aux seuls services. Un premier problème concernait la manière dont les clients faisaient part de leurs souhaits et de leurs besoins (ou décidaient plutôt de ne pas le faire) et donnaient du feedback. Le Comité a constaté que lorsque les clients donnaient peu ou pas d'indications concernant leurs besoins – voire aucune indication – ou lorsque le feedback faisait défaut, les services éprouvaient parfois des difficultés à adapter leurs produits. En termes de transmission d'informations, le Comité a remarqué que, sur la forme, les services veillaient suffisamment à la bonne présentation de leurs produits et à la formulation de conclusions claires. De manière générale, les services s'efforçaient de rédiger leurs notes de telle sorte qu'elles présentent une utilité pour leurs clients. Au SGRS, du moins à la Division I, une directive formelle déterminait la manière dont un document devait être établi. Cette directive offrait une certaine garantie de qualité, à tout le moins sur la forme. D'autres éléments, comme les *Service Level Agreements* (SLA), la liste de distribution et l'existence de la fonction de *production support*, étaient des exemples à suivre.

II.1.3.5. Le caractère prédictif du travail de renseignement

Le caractère prédictif du travail de renseignement constituait le cinquième point de mesure. Le Comité permanent R a constaté que les deux services de renseignement fournissaient surtout des renseignements descriptifs et explicatifs, et dans une moindre mesure des renseignements prédictifs. Les *Intelligence Outlook Bulletins* (IOB) de la Division I du SGRS faisaient exception à cet égard. Lorsque les autorités compétentes (judiciaires, policières et politiques) souhaitaient obtenir, de la part des services de renseignement, des scénarios et des hypothèses étayées pour initier certaines actions, les renseignements fournis par les services étaient, la plupart du temps, moins adaptés.

II.1.3.6. La conception ou la planification de l'effort de renseignement

Le sixième point de mesure était la conception ou la planification de l'effort de renseignement global dans la problématique syrienne. L'objectif est de décrire tant les efforts que les méthodes de collecte et d'analyse. On tente ensuite d'établir des liens entre les deux. Il s'agissait d'un élément de travail important pour les deux services de renseignement. Le Comité a certes pu constater que des fondements existaient à la VSSE et au SGRS, mais ils devaient être mieux intégrés et élaborés qu'ils ne l'étaient au moment de l'enquête. Les processus de renseignement individuels n'étaient pas foncièrement bouleversés par cette lacune, mais les résultats globaux de l'effort de renseignement (en termes d'efficacité et de coordination) s'en trouveraient améliorés si l'on y prêtait davantage attention. En ce qui concerne l'approche de collecte proprement dite et son ampleur, il est évident que certaines données pouvaient échapper aux services. Le Comité permanent R a estimé que la méthode de collecte des deux services était suffisamment large et diversifiée et qu'elle offrait les garanties nécessaires à l'élaboration d'une position d'information correcte. Cela s'inscrivait à nouveau dans le droit fil du premier point de mesure.

II.1.3.7. En conclusion

Dans le cadre de l'élaboration de leur position d'information sur la problématique syrienne, les services de renseignement étaient parvenus à limiter différents risques liés aux points de mesure. Toutefois, plusieurs risques se sont manifestés, auxquels il convenait de remédier, selon le Comité. La problématique de la gestion des données était prioritaire à cet égard, surtout pour le SGRS.

II.1.4. LES SERVICES DE RENSEIGNEMENT ET LES *LOCAL TASK FORCES*

En ce qui concerne la composition, l'organisation et la forme donnée aux diverses *local task forces* (LTF), plusieurs différences notables ont été constatées. Ce n'était pas un problème en soi, vu que les situations pouvaient diverger en fonction du lieu. Il est néanmoins apparu que l'efficacité de la LTF était inversement proportionnelle à sa taille.

Le Comité a pu constater que les différents participants aux LTF (police, services de renseignement, parquet…) se présentaient aux réunions avec des attentes et des tâches différentes ('travail de renseignement' *versus* 'travail de police'). Ainsi, les services de renseignement étaient soumis à une série de restrictions (p. ex. en matière de classification, *need to know*, règle du tiers service), qui influençaient leur participation aux LTF.

Du point de vue du service de renseignement, la question des habilitations de sécurité constituait un obstacle majeur, qui freinait l'échange d'informations. Ces informations n'étaient pas toujours pleinement prises en compte ou appréciées par les autres acteurs. Cette problématique a été en partie résolue à la faveur de la nouvelle Circulaire FTF, qui stipule que tous les participants aux LTF doivent être titulaires d'une habilitation de sécurité de niveau SECRET. Le Comité permanent R a estimé qu'il s'agissait d'un pas dans la bonne direction. Cela implique, il est vrai, que tous les participants disposeraient de certaines informations classifiées qui ne pourraient pas être partagées avec des personnes ou avec les autorités des participants qui ne seraient pas titulaires d'une habilitation de sécurité.

Par ailleurs, le Comité a également estimé qu'une réflexion s'imposait sur les informations qui, précisément, devaient faire l'objet d'une classification. Dans ce cadre, l'Administrateur général prônait une plus grande ouverture de la part de la VSSE.

Des doutes et questions ont surgi concernant les attentes des collaborateurs de la VSSE comme du SGRS vis-à-vis des *local task forces*. La Circulaire FF 'initiale' était trop superficielle sur ce point : elle décrivait les missions sans 'attribuer' de tâches. Les participants demeuraient avec une série de questions restées sans réponse à ce stade : les LTF ont-elles été constituées à des fins d'échange d'informations (et si oui, pour quel type d'informations ?) ou s'agissait-il plutôt d'organes destinés au réseautage et à la sensibilisation ? Et, en fonction de l'objectif, quelle était la composition la plus indiquée ? Il a par exemple été suggéré d'envoyer aussi (de temps en temps) un analyste à la LTF. La VSSE pourrait ainsi, en plus de livrer des informations purement 'opérationnelles', endosser un rôle de contextualisation plus large. L'enquête de contrôle a permis de constater que les membres de la VSSE estimaient souhaitable que l'administration centrale leur donnent une orientation sur ce point. Les attentes du terrain n'ont pas été entièrement rencontrées à ce niveau.

La nouvelle Circulaire (*supra*) a, ici aussi, toute son utilité : l'approche concrète des *foreign fighters* est subdivisée en plusieurs sous-aspects (constater la présence ou l'absence de FTF, vérifier et étoffer les informations, analyser les menaces individuelles et assurer un suivi standardisé et personnalisé), chacun se voyant attribuer des tâches clairement définies.

II.1.5. COLLABORATION AVEC LES AUTORITÉS JUDICIAIRES

Aucun des services entendus n'a remis en cause le cadre légal de la collaboration, qui semblait suffisant et adapté aux besoins de la lutte contre les *foreign (terrorist) fighters* et les *returnees*. Tous les services interrogés ont souligné la bonne collaboration entre les services de renseignement, les services de police et le

Parquet fédéral[23] dans le cadre de la problématique syrienne. La collaboration s'était même améliorée depuis l'arrivée de la nouvelle direction de la VSSE.

Le Comité a cependant constaté une différence en termes de politique d'information, à la VSSE et au SGRS, vis-à-vis des autorités judiciaires. Il a également constaté un recours peu fréquent à l'article 19/1 L.R&S. Dans des dossiers concrets, la protection des sources des services de renseignement pouvait se révéler problématique, même si l'intervention du Parquet fédéral avait permis d'éviter des difficultés.

La collaboration directe entre les services de renseignement et les services de police était également jugée positive par les différents acteurs. Il a néanmoins été jugé souhaitable de déterminer concrètement le rôle de chaque service au niveau opérationnel, en tenant compte de l'expertise inhérente à chacun.

Un problème délicat soulevé par les services de police était celui de la (culture de) classification et des habilitations de sécurité. Les services de police reconnaissaient qu'ils devaient y apporter des améliorations en interne.

II.2. LA POSITION D'INFORMATION DE LA VSSE ET L'ATTENTAT MANQUÉ DU THALYS

II.2.1. LES FAITS

Le vendredi 21 août 2015, le Thalys reliant Amsterdam à Paris a été la cible d'une attaque terroriste. Quelques passagers sont toutefois parvenus à maîtriser rapidement l'auteur de cette attaque. Il a été identifié comme étant Ayoub El Khazzani, originaire du Maroc. Il serait monté à bord du Thalys à Bruxelles avec des armes qu'il aurait achetées en Belgique.[24] Le Comité permanent R a ouvert une enquête complémentaire, dans le prolongement de son enquête de contrôle sur les *foreign terrorist fighters* (II.1). Cette enquête ne concernait que la VSSE, le SGRS ayant déclaré ne disposer d'aucune information concernant Ayoub El Khazzani avant les faits.

II.2.2. L'AUTEUR ÉTAIT-IL CONNU DE LA VSSE ?

Ayoub El Khazzani était connu de la VSSE depuis 2012 : son nom est apparu pour la première fois en même temps que celui de son frère (Imram), dans un

---

23 Pour la période allant du 1er octobre 2014 au 31 mars 2015, la VSSE a reçu 132 demandes d'assistance technique (art.20 § 2 L.R&S), dont la plupart étaient liées à des dossiers de terrorisme international. Pour la période de mars-avril 2015, le SGRS a reçu 60 demandes d'assistance technique, dont 90 % étaient liées à la problématique des *foreign fighters* et auxquelles le service a réservé une suite favorable.

24 L'auteur a été officiellement mis en examen par le procureur de Paris pour tentative de meurtre lié au terrorisme et détention d'armes. Il est dans l'attente de son procès.

rapport établi par le service, en juin 2012, à la suite d'une réunion avec un service partenaire. Les frères étaient associés à un membre éminent d'une cellule djihadiste étrangère. Cette personne aurait fui vers la Belgique et serait le maillon d'un réseau plus large impliqué dans l'envoi de combattants en Syrie. Leur identité était reprise dans la base de données de la VSSE.

Dans les mois qui ont suivi, des renseignements et des photos ont été échangés, et il a été demandé à la VSSE de vérifier des informations, ce que le service a effectivement fait. Des vérifications à l'Office des étrangers n'ont rien donné. En octobre 2012, la VSSE a participé à une réunion avec le service partenaire au sujet de la cellule djihadiste et la présence de certains de ses membres sur le sol belge. La VSSE a appris à cette occasion qu'une instruction judiciaire était en cours concernant la cellule djihadiste. Le Comité permanent R n'a trouvé aucune trace de communication qui aurait révélé un échange d'informations entre la Police fédérale et la VSSE à ce propos.[25]

En avril 2013, El Khazzani a été placé sur une liste internationale, vraisemblablement par le service partenaire. Ensuite, on n'a plus entendu parler des frères El Khazzani.

Le 11 mai 2015, le correspondant a envoyé à la VSSE un nouveau document dans lequel figuraient des informations relatives à Ayoub El Khazzani. Le service partenaire manifestait son intérêt pour l'intéressé, pour ses contacts avec les milieux extrémistes belges et pour son rôle de liaison éventuel dans le cadre des filières transitant aussi par la Belgique. Dans ce document, il n'est fait mention nulle part d'un quelconque achat d'armes ou d'un plan visant à commettre une attaque terroriste. Le service partenaire n'a pas non plus envoyé de photo d'Ayoub El Khazzani, et un degré d'urgence n'a pas été ajouté. Deux jours plus tard, ce document a été transmis en interne au service d'analyse et au service central des services extérieurs. Le service central a fait suivre le document le jour même au poste de province compétent avec la mention 'pour enquête'.[26] Le poste de province a déclaré avoir effectué un contrôle du Registre national et s'être rendu à la Police locale en date du 30 juin 2015. Le Comité a constaté que la VSSE n'avait pas pris l'initiative de demander une photo de l'intéressé au service de police ou au service partenaire. La VSSE n'a pas répondu au correspondant étranger. Ce n'est pas inhabituel si le service ne dispose pas d'informations (concept de '*silent answer*').

Le 17 août 2015, la VSSE a reçu des informations complémentaires du service partenaire, qui a réitéré son intérêt pour Ayoub El Khazzani et qui a également

---

25 À noter que la VSSE n'avait pas directement accès aux banques de données policières. La VSSE a déclaré ne recevoir des informations que lorsque la police en prenait l'initiative ou lorsqu'elle en faisait explicitement la demande. En vertu de l'article 14 L.R&S, la VSSE peut toutefois demander tout type d'informations aux services de police.

26 C'est la seule fois que l'outil informatique prévu à cet effet dans la banque de données de la VSSE a été utilisé pour envoyer un message. L'enquête n'ayant rien révélé à ce moment-là concernant El Khazzani, le poste de province concerné a laissé la tâche en suspens dans la banque de données pour pouvoir, selon lui, la reprendre par la suite.

demandé d'identifier trois numéros de GSM. Les informations ont été communiquées au service d'analyse et aux services extérieurs le 18 août 2015, soit trois jours avant l'attentat manqué. Le 19 août, le service d'analyse a introduit la demande dans le système informatique à destination du poste de province concerné. Le 22 août 2015, c'est-à-dire après l'attentat manqué, la VSSE a procédé à l'identification demandée par le service partenaire. Elle a établi un document reprenant des informations sur Ayoub El Khazzani, qui a été arrêté entre-temps, ainsi que sur l'identification des trois numéros de GSM.

II.2.3. LE CONTEXTE DU DOSSIER

En vue de contextualiser les événements, le Comité a examiné comment la VSSE avait géré les demandes de correspondants étrangers à ce moment-là.

Les documents envoyés à la VSSE passent en premier lieu par un point d'entrée unique. Au moment de l'attaque commise dans le Thalys, la procédure était la suivante : ces documents étaient ensuite transmis tant aux services d'analyse qu'aux services extérieurs, et ce dans les limites de leurs compétences respectives. La procédure a été modifiée depuis la restructuration de la VSSE entreprise en septembre 2015. Les informations entrantes passent toujours par le point d'entrée unique, mais elles sont ensuite dirigées vers la section concernée du service d'analyse. Ce service détermine si et quel service extérieur est informé et demande de mener l'enquête quand il l'estime nécessaire.

En août 2015[27], la VSSE a reçu de correspondants étrangers environ 1200 documents, dont 25 % ont été transmis à la section qui enquête sur l'islam radical.[28] Une quarantaine de ces documents contenaient des informations nécessitant une action de la VSSE.[29] Seuls quelques documents concernaient l'identification de données téléphoniques. La demande portant sur Ayoub El Khazzani est la seule à avoir été honorée, mais après l'attaque.

---

27 Le mois au cours duquel l'identification de numéros de téléphone a été demandée par le service partenaire, mais aussi le mois au cours duquel l'attentat (manqué) a eu lieu à bord du Thalys.

28 Le Comité permanent R a fait remarquer que le nombre de documents reçus en août 2015 par la section qui s'occupe de 'l'islam radical' ne reflétait pas le flux habituel de documents entrants. Ainsi, cette section a reçu environ 850 documents de correspondants étrangers en septembre 2015 et environ 1050 en octobre de la même année.

29 L'encodage dans le système informatique des demandes de correspondants étrangers n'était pas uniforme. Ces demandes étaient libellées en 'requêtes', *requests for information* (RFI), 'demandes' ou encore 'demandes de traces'. La VSSE a déclaré disposer d'une capacité d'influence limitée sur les titres choisis par ses correspondants. Il peut dépendre de la langue du correspondant, des choix des traductions, des procédures standards en vigueur chez ces correspondants… En outre, les demandes du correspondant étranger ne mentionnaient pas le degré d'urgence (routine, urgent, *flash*). Ce constat ne vaut que pour les documents consultés par le Comité dans le cadre de cette enquête. Par conséquent, déterminer le degré de priorité des devoirs d'enquête était loin d'être évident.

En ce qui concerne les demandes d'identification téléphonique (art. 18/7 L.R&S) demandées par des correspondants étrangers, le Comité permanent R a également examiné les chiffres relatifs à la période allant de janvier à août 2015. Il est apparu que la VSSE avait procédé, à la demande d'un service étranger, à 130 identifications au cours de cette période.[30] Près de dix de ces méthodes – demandées pour la période allant du 1er juillet au 21 août 2015 – portaient sur le terrorisme extrémiste. Dans ces dossiers où la VSSE a procédé à une identification, entre la demande d'un service étranger et le suivi qui y a été réservé, le délai variait entre 6[31] et 64 jours. Dans le cadre spécifique de la demande d'identification des numéros de téléphone d'Ayoub El Khazzani, trois jours se sont écoulés.[32] Que l'identification n'ait pas eu lieu dans les trois jours n'avait rien d'exceptionnel, en a conclu le Comité.

Enfin, il convient de mentionner que cette identification n'a pas été concluante *a posteriori*, puisque les numéros provenaient de cartes prépayées, donc 'anonymes'. L'enquête que la VSSE a menée ensuite sur les numéros en question a cependant permis d'identifier les personnes avec lesquelles Ayoub El Khazzani avait été en contact en Belgique.

II.2.4. CONSTATATIONS ET CONCLUSIONS

La VSSE s'est basée sur les renseignements qu'elle avait reçus de l'étranger pour mener ses activités. Ces informations n'étaient pas très détaillées. Le Comité a dû constater que les demandes émanant du correspondant étranger ne bénéficiaient pas d'un suivi optimal :

- le dossier était géré de manière routinière. Ainsi, la VSSE n'a pas tenté d'obtenir des informations complémentaires sur le dossier en vue de faire progresser l'enquête ;
- il y avait un manque de guidance au niveau des sections centrales ;
- ni la VSSE ni le correspondant étranger n'ont défini le degré d'urgence ou d'importance relative au traitement des informations dans l'affaire El Khazzani. De plus, aucune menace précise n'a été mentionnée ;
- les informations de mai 2015 ont été traitées via le système ICT prévu à cet effet, mais les devoirs d'enquête, le rappel du service d'analyse et les résultats (mêmes négatifs) n'ont pas été repris dans le système. Le Comité permanent a estimé que la non-utilisation du système ICT affaiblissait la gestion des informations ;

30 Ces 130 méthodes portent sur toutes les matières devant être suivies par la VSSE, ce qui représente une moyenne de 16 identifications par mois.

31 À noter que ce délai assez court concerne une demande d'identification d'un service partenaire dans le cadre d'un dossier lié à la cellule de Verviers.

32 Il convient d'ajouter deux jours compte tenu du délai de transmission du document par l'officier de liaison du service partenaire.

– les services extérieurs n'ont pas communiqué au service d'analyse les résultats des devoirs d'enquête effectués en mai 2015, même s'ils se sont révélés négatifs, et aucune réponse n'a été adressée au correspondant étranger. Les résultats de ces devoirs d'enquête n'ont pas non plus permis de clôturer le dossier ni d'introduire de nouvelles hypothèses.

Le Comité permanent R n'a pas constaté d'échanges d'informations entre la VSSE et la Police fédérale.

Les frères El Khazzani figuraient sur une liste internationale. Sans contester l'utilité d'une telle liste, le Comité permanent R a souligné l'existence de nombreuses listes aussi bien nationales qu'internationales, dont la pertinence et l'actualité ne sont pas toujours garanties. La VSSE, qui contribuait à alimenter cette liste, a déclaré ne pas avoir les moyens de suivre et de vérifier chaque nom y figurant (plus de 2500), sans davantage de précisions sur le contexte et la menace que représente l'individu. Selon la VSSE, les services de renseignement devraient élaborer un système de gestion des risques qui serait associé aux djihadistes potentiels.[33] Un tel système devrait permettre de classer les intéressés en fonction de leur degré de dangerosité.

De manière plus générale, le Comité permanent R a remarqué que les moyens d'action des services de renseignement, qui ont pour mission d'effectuer des recherches sur des personnes représentant une menace, sont limités. La facilité avec laquelle les intéressés ont pu se déplacer en Europe, voire en dehors de ses frontières, la facilité avec laquelle ils peuvent utiliser toutes sortes de moyens de communication et peuvent résider anonymement dans des régions ou des pays sans être détectés, représentent un défi majeur pour les services de renseignement et de sécurité.

II.3. LA POSITION D'INFORMATION DES DEUX SERVICES DE RENSEIGNEMENT AVANT LES ATTENTATS DE PARIS

II.3.1. RAPPEL DES FAITS

Le 13 novembre 2015, plusieurs attentats ont été perpétrés quasi simultanément à Paris. Peu après 21 heures, trois explosions ont retenti aux abords du Stade de France, où se déroulait un match de football opposant la France à l'Allemagne. Trois kamikazes ont actionné leur ceinture d'explosifs aux abords du stade. Une victime était à déplorer, en plus des auteurs. À peine un quart d'heure plus tard, des fusillades ont eu lieu à proximité de terrasses de cafés et de restaurants dans le centre de Paris. Des dizaines de personnes y laisseront la vie ou seront blessées.

[33] Les services de renseignement en ont discuté entre-temps.

Enfin, dans la salle de concert du Bataclan toute proche, 90 personnes seront tuées de manière brutale. Les trois auteurs périront aussi dans cette attaque.

Au total, 130 personnes ont trouvé la mort ce soir-là, et plus de 400 ont été blessées. Le mouvement terroriste État Islamique (EI) a revendiqué les attentats dans une communication officielle.

Presque immédiatement après les attaques sanglantes, le Comité permanent R a ouvert une *« enquête de contrôle sur la position d'information des deux services de renseignement sur les individus ou groupes ayant perpétré les attentats de Paris ou liés à ces attentats, avant le vendredi 13 novembre 2015 au soir »*.[34] En effet, des éléments indiquant l'existence de toute une série de liens avec la Belgique sont rapidement apparus : cinq terroristes provenaient ou résidaient en Belgique, les véhicules utilisés lors des attentats avaient été loués en Belgique, les terroristes disposaient de planques en Belgique, les ceintures d'explosifs avaient vraisemblablement été assemblées dans un appartement de Schaerbeek…

Le Comité permanent R a tout d'abord vérifié ce que la VSSE et le SGRS savaient des auteurs avant les attentats, et quels moyens de collecte ils avaient utilisés. Ensuite, il a examiné comment ces services avaient collaboré avec d'autres autorités (nationales et internationales) avant et après les attentats. Le Comité s'est également penché sur la manière dont les autorités concernées (gouvernement, parquet…) avaient été informées des menaces imminentes pour leur permettre de prendre les mesures nécessaires à temps. Enfin, le Comité a vérifié de quelle manière les deux services de renseignement avaient réagi aux événements en termes de 'gestion de l'organisation', et quels étaient les problèmes structurels et les risques auxquels ils étaient confrontés. Mais avant, le Comité a attiré l'attention sur l'évolution rapide du contexte juridique en matière de terrorisme et d'extrémisme.

II.3.2. L'ÉVOLUTION RAPIDE DU CONTEXTE JURIDIQUE

Depuis les attentats de New York (2001), Madrid (2004) et Londres (2005), de nombreux pays européens disposent d'une palette particulièrement large et diversifiée de mesures préventives – mais surtout répressives – contre le terrorisme. Ces mesures n'ont cependant pas permis d'éviter les attentats de

[34] L'enquête a été clôturée en juillet 2016 (Diffusion restreinte – 47 pages). Deux rapports intermédiaires avaient été établis auparavant pour la Commission de suivi de la Chambre. Le premier rapport, daté du 24 février 2016 (Diffusion restreinte – 41 pages), revêtait surtout un caractère descriptif et quantitatif. Le deuxième rapport, daté du 22 avril 2016 (Diffusion restreinte – 22 pages), se déclinait en deux parties. Dans la première partie, le Comité s'est penché sur la valeur ajoutée des HUMINT, SOCMINT et SIGINT dans l'élaboration de la position d'information et sur la manière dont les informations ont été diffusées. La seconde partie reprenait une série d'éléments structurels sur la manière dont les services de renseignement belges organisent la collecte et l'analyse et sur les risques qui y sont liés. Les résultats des deux rapports intermédiaires sont traités dans le présent résumé.

Paris ni, plus tard, ceux de Bruxelles. L'ampleur actuelle de la problématique, et la menace spécifique qui en découle, requièrent une approche ciblée et rationnelle. Dans ce contexte, les services de renseignement sont un maillon de la chaîne de la justice pénale, en général, et de la lutte contre l'islamisme radical, les *foreign fighters* et les *returnees*, en particulier.

Surtout après les attentats de Paris, toute une série de mesures ont été prises à divers niveaux de pouvoir. Le Comité s'est demandé si la coordination était suffisante et si la nécessité de chacune des mesures pouvait être démontrée. Il faisait référence, à cet égard, aux conclusions d'une enquête sur l'efficacité des mesures prises en Europe depuis 2001, à savoir qu'on a davantage besoin d'une évaluation *approfondie* des mesures que de l'introduction de nouvelles mesures.[35]

II.3.3. LA POSITION D'INFORMATION DES SERVICES ET L'APPORT DES DIFFÉRENTS MOYENS DE COLLECTE

Le Comité a tracé une ligne du temps reprenant les informations disponibles à la VSSE et au SGRS, avant le 13 novembre 2015, sur les personnes les plus importantes directement ou indirectement impliquées dans les attentats[36], et ce indépendamment de la nature de ces informations (échange de courriers, note d'analyse…) et de leur source (collecte des services, service étranger, autres autorités belges…). Ensuite, la position d'information et son élaboration ont été brièvement décrites sur base des questions suivantes : Quand chacun des protagonistes est-il apparu pour la première fois dans les radars du service de renseignement ? Que savait-on sur ces personnes (qui, quoi, quand, pourquoi et où) ? Des MRD ont-elles été mises en œuvre ? Quelles informations ont été échangées avec des services étrangers, et quelle a été l'interaction avec les services et les autorités belges ? Quels liens les services de renseignement ont-t-il établi entre les intéressés ?

II.3.3.1. La position d'information

La VSSE avait la plupart des protagonistes en ligne de mire (certains depuis un certain temps, d'autres depuis peu), que ce soit parce qu'il s'agissait de criminels ou de personnes radicalisées. Seul Abdelhamid Abaaoud, qui est considéré à ce jour comme l'un des meneurs du commando meurtrier, était clairement très dangereux. Aucun élément n'indiquait que les autres passeraient à l'action ; on ne pouvait pas non plus déduire qu'ils formaient une cellule opérationnelle.

---

35 B. HAYES et C. JONES, *Report on how the EU assesses the impact, legitimacy and effectiveness of its counter-terrorism laws*, Statewatch, SECILE-project, 2015, 59 p.

36 Il s'agissait au départ de dix personnes qui, au moment où le Comité a effectué son enquête, étaient désignées comme (co-)auteurs par différentes sources. Dans une phase ultérieure de l'enquête de contrôle, on a compté jusqu'à quatorze personnes, et dans la dernière partie de l'enquête, ce nombre a été ramené à huit.

Avant les attentats, le SGRS ne disposait d'informations qu'au sujet d'Abaaoud. Il était apparu en 2013 en marge d'une autre enquête.[37] Lorsque Abaaoud a rallié l'État Islamique, début 2014, le SGRS a tenté d'en savoir plus sur les activités qu'il menait à l'étranger. À compter du démantèlement de la cellule de Verviers en janvier 2015, il est devenu une priorité pour le SGRS. Le service a adressé plusieurs *Requests for Information* (RFI) à ses correspondants, sans que n'en ressorte aucun renseignement utile. En 2015, le SGRS a eu connaissance, via ses propres moyens de collecte, de la détermination de l'EI à commettre des attentats en Europe. Le service ne disposait cependant pas d'informations concrètes sur un lieu ou une date. Le SGRS a estimé, dans ce cas-ci, que ces informations étaient très importantes, et les a presque immédiatement communiquées aux autorités judicaires, aux correspondants étrangers et au Conseil national de sécurité.

II.3.3.2. L'utilisation de différents moyens de collecte

En ce qui concerne les moyens de collecte utilisés par la VSSE et le SGRS (HUMINT, MRD, SIGINT et SOCMINT), les constats suivants peuvent être mentionnés dans ce rapport public.

En ce qui concerne le '*human intelligence*' (HUMINT) :

- concernant certaines des personnes sur lesquelles portait l'enquête, la VSSE disposait d'informations parcellaires, provenant de sources humaines. Même si certaines de ces sources étaient décrites comme étant 'à haute valeur ajoutée', elles n'ont pas communiqué la moindre information en rapport avec les attentats imminents ;
- certaines de ces sources étaient gérées conjointement avec un service partenaire étranger ;
- dans le cadre de la lutte contre le terrorisme, les sources bien placées sont une denrée rare. Par conséquent, un nombre très restreint de sources humaines 'à haute valeur ajoutée' étaient à la base de la plupart des informations dont disposait la VSSE ;
- la VSSE affirmait que le manque d'effectifs limitait le travail avec les informateurs, en ce sens que peu de temps pouvait être consacré à l'entretien des contacts et à la recherche de nouvelles sources ;
- le SGRS recrutait des sources humaines dans le cadre des milieux islamistes et radicaux, en Belgique et à l'étranger.[38] Ce service peut donc collaborer plus souvent et échanger plus d'informations avec certains services partenaires ;

---

37 Il s'agissait de l'affaire Zerkani, qui a été condamné en 2016 pour infractions terroristes (voir également II.3.4.4).

38 Avant les attentats du 13 novembre 2015, le SGRS ne disposait d'aucune information HUMINT à propos des protagonistes précités, sauf à propos d'Abaaoud. Les informations HUMINT concernant l'intéressé n'étaient pas récentes, étaient peu volumineuses et peu spécifiques.

- pour la gestion de ces sources – mais aussi pour la recherche et l'analyse d'informations via l'OSINT et le SOCMINT – la connaissance des langues et la connaissance des milieux allochtones sont essentielles. C'est la raison pour laquelle la VSSE et le SGRS devraient promouvoir la diversité au sein de leurs services ;
- une meilleure coordination s'impose entre les différentes sections qui gèrent les sources humaines au sein du SGRS.

En ce qui concerne le '*social media intelligence*' (SOCMINT) :
- en 2015, une cellule SOCMINT a été créée au sein de la VSSE. Sa mission consistait à suivre et à rechercher des sites, des profils et des personnes, mais elle pouvait également prêter son concours à la section HUMINT et dans le cadre des MRD ;
- les informations SOCMINT relatives aux (co-)auteurs ont peu contribué à la position d'information de la VSSE, à l'exception des informations relatives à Abaaoud. Sur base des données, il a pu être établi que certaines personnes étaient (très) radicalisées, sans qu'il y ait d'indications sur des projets concrets d'attentats ;
- le Comité a pu constater que le SOCMINT ne cessait de gagner en importance comme instrument de collecte. Il requiert néanmoins beaucoup de temps et est difficile à gérer en termes de volume et de technicité ;
- le Comité a constaté que la capacité que tant la VSSE que le SGRS ont dédiée au SOCMINT était plutôt limitée, certainement vu le fait que le phénomène du terrorisme n'était pas le seul sur lequel ces services devaient se concentrer. Une collaboration plus poussée semble nécessaire pour y remédier.

En ce qui concerne le '*signals intelligence*' (SIGINT)[39] :
- le SGRS, par le biais de la section SIGINT, a accès à une manne d'informations provenant d'autres nations disposant de capacités SIGINT plus étendues. Elle peut ainsi bénéficier de la mutualisation de ressources internationales ;
- si la section SIGINT du SGRS dispose essentiellement de (meta)data qui, souvent, ne sont pas liées à une personne identifiée, cette section disposait de documents pouvant être associés à deux individus qui figuraient sur la liste des noms sélectionnés par le Comité ;
- la section SIGINT dispose d'une capacité unique concernant les numéros de téléphone étrangers. Néanmoins, le VSSE faisait rarement appel à cette section. Le Comité était d'avis qu'une collaboration devait être mise en place à ce niveau.

[39] On se réfère ici à l'interception de communications émises à l'étranger. Seul le SGRS en détient la compétence. Ce genre d'interceptions est légalement possible dans le cadre de l'opération militaire menée contre l'EI (par exemple, par la présence des F16), pour la protection des Belges à l'étranger (principalement dans la région concernée) et pour la protection de la population belge dans son ensemble.

En ce qui concerne les méthodes particulières de renseignement (MRD) :
- le Comité a constaté que la VSSE avait utilisé les MRD de manière adéquate ;
- avant les attentats du 13 novembre 2015, des méthodes particulières de renseignement ont été mises en œuvre par la VSSE à l'égard de trois des huit *targets* (ou de leur entourage) sélectionnés par le Comité.[40] Ces méthodes n'ont pas permis de recueillir des informations déterminantes qui auraient pu éviter les attentats. Les informations émanant des MRD viennent confirmer ou infirmer des informations issues d'autres moyens de collecte, donner des pistes pour la collecte, ou encore élaborer ou exclure des hypothèses d'enquête ;
- le SGRS n'a pas employé de MRD avant les attentats à l'égard des personnes sélectionnées ;
- les écoutes téléphoniques étaient très fréquemment mises en œuvre à la suite d'une demande formulée par un correspondant étranger, souvent dans le cadre d'une collaboration plus générale ;
- les personnes suivies dans le cadre du terrorisme semblaient souvent conscientes de faire l'objet d'une surveillance et développaient des contre-stratégies pour échapper au suivi.

Le Comité a estimé qu'un manque d'implication ne pouvait être reproché à la VSSE. Le service n'avait pas ménagé ses efforts pour tenter de recueillir des renseignements.

Le Comité a néanmoins formulé une remarque sur la possibilité d'améliorer la position d'information au moyen d'informations judiciaires. Une assistance technique était, en effet, toujours demandée à la VSSE dans le cadre de dossiers judiciaires du Parquet fédéral. Le service avait ainsi accès à ces dossiers, ce qui pouvait constituer une source d'informations. Le Comité s'est demandé si la VSSE saisissait systématiquement cette possibilité ou opportunité de collecte.

II.3.3.3. Le flux d'informations (interne et externe)

Le nombre de données entrantes et la quantité d'informations collectées par les services de renseignement eux-mêmes étaient extrêmement élevés. Certains éléments risquaient ainsi d'échapper à l'attention et/ou de ne pas être suffisamment mis en avant lors du traitement des informations et dans les rapports destinés à l'extérieur, ce qui pouvait éventuellement engendrer une perte de qualité en termes de contenu.[41]

---

40 Un nombre considérable de MRD ont évidemment été mises en œuvre juste après les attentats. Le Comité a également examiné cet aspect.

41 Le Comité permanent R a pu constater que dans un rapport émanant de l'étranger et qu'a reçu la VSSE à la mi-2015 concernant les éventuels plans terroristes de l'EI, il était question de contacts qu'avaient les *foreign fighters* à 'Molenbeek', tandis que le rapport destiné au Parquet à ce propos reprenait la mention plus générale de 'Bruxelles'. Et le Comité de constater qu'un rapport qu'a reçu le SGRS à l'été 2015 n'est pas allé plus loin. Ce rapport mentionnait qu'une

Le Comité permanent R s'est penché sur cette question, en analysant quelques cas, à savoir les renseignements collectés via le HUMINT sur Abdelhamid Abaaoud et Mohamed Abrini à la VSSE et les informations SIGINT du SGRS.

En ce qui concerne la VSSE, le Comité permanent R n'a constaté qu'une faible de perte de précision et d'exhaustivité (voire aucune perte) entre, d'une part, les informations HUMINT collectées sur Abaaoud, et d'autre part, les notes destinées à d'autres autorités. Ce qui a été rapporté par les sources a été relayé à l'extérieur, certes plus ou moins rapidement.

S'agissant d'Abrini, la situation était tout autre. Les sources HUMINT ont fourni énormément d'informations, mais la VSSE n'a pas établi de notes destinées à l'extérieur. Les informations sont restées en interne, ce qui ne sous-entend évidemment pas que la VSSE n'en a rien fait.

Les informations collectées par la section SIGINT du service de renseignement militaire avaient trois destinataires : le SGRS lui-même, les services partenaires belges et les partenaires SIGINT étrangers. En règle générale, les documents SIGINT destinés à l'usage interne du SGRS se sont révélés très détaillés. En revanche, les documents destinés à la VSSE et/ou aux autorités judiciaires étaient généralement beaucoup moins détaillés et complets.[42] Il était donc question d'une perte d'exhaustivité et de précision des renseignements transmis. Mais dans le cas présent, le Comité permanent R n'a pas pu constater qu'il s'agissait d'informations cruciales. Étant donné que les informations SIGINT ne sont, en principe, jamais envoyées dans leur forme brute à des partenaires externes, elles doivent être traitées, et cela prend un certain temps. Mais si des informations cruciales doivent être envoyées rapidement et dans leur forme brute, il y a toujours moyen de le faire.

II.3.3.4. L'analyse des informations collectées

L'analyse est une composante essentielle du travail de renseignement. Il existe toutes sortes de méthodologies permettant de structurer l'analyse, mais les services n'en tiraient pas encore suffisamment avantage. Le Comité permanent R a souligné que cela n'avait pas empêché les services de lancer les avertissements requis à des moments clés.

Une méthode importante consiste à ébaucher divers scénarios, et à émettre des hypothèses pouvant être confirmées ou infirmées.

---

unité militaire déployée pour prêter assistance à la police avait cru remarquer Abaooud dans la région bruxelloise, alors que tout le monde était persuadé qu'il se trouvait en Syrie. Il est vrai que l'unité militaire concernée a également fait suivre le rapport à la police.

42 À la fin octobre 2015, par exemple, un document à usage interne a été établi au SGRS sur deux partisans d'Abaaoud, avec force détails. La note qui a été envoyée à la VSSE à ce sujet était beaucoup moins explicite. Plusieurs raisons ont ainsi été avancées, raisons qui ont un rapport avec les règles spécifiques au fonctionnement SIGINT, qui imposent par exemple que les informations brutes doivent être expurgées de données susceptibles de révéler la source des informations.

Par exemple, la VSSE s'est longtemps basée sur l'hypothèse selon laquelle les FTF avaient l'intention de s'établir définitivement ou de mourir dans ce qui allait devenir le Califat, et non de rentrer. La conséquence en a été, de manière générale, que l'impact du phénomène sur le sol européen a été initialement sous-estimé. Au début, la VSSE avait toutefois envisagé un 'scénario du pire', ne fût-ce que brièvement. De tels scénarios ont toute leur importance, parce qu'ils offrent un point d'appui pour définir par la suite, via des indicateurs, la direction que prend le scénario. Ce sont des instruments méthodologiques importants qui devraient pouvoir être davantage utilisés.

Le Comité permanent R estime cependant que de tels scénarios se conçoivent de préférence dans un cadre multidisciplinaire. Un scénario terroriste a, en effet, plusieurs composantes, tant civiles que militaires, si bien que la VSSE et le SGRS auraient pu collaborer en la matière. En d'autres termes, ce n'est pas parce que, de prime abord, le SGRS ne s'estimait pas compétent à l'égard des FTF 'civils', qu'il n'aurait pas pu apporter une contribution utile.

Enfin, selon le Comité, un lien doit être établi entre la collecte et l'analyse : les deux doivent s'alimenter mutuellement et s'équilibrer. C'est la raison pour laquelle le Comité a insisté sur l'importance d'une 'conception globale du renseignement' pour visualiser un phénomène déterminé, une menace concrète ou un *target*. En principe, cette conception ne devrait pas seulement exister au sein de chaque service, mais aussi tenir compte (et idéalement utiliser) les capacités de collecte et d'analyse d'autres services. Le *Memorandum of Understanding* (*infra*), établi après les attentats, va dans ce sens.

II.3.4. LA COLLABORATION AU NIVEAU NATIONAL

II.3.4.1. La collaboration dans le cadre des local task forces

En ce qui concerne le fonctionnement des *local task forces*, le Comité a constaté ce qui suit :

- les participants aux LTF doivent bien s'informer mutuellement de leurs besoins respectifs, de leurs possibilités et de leurs limites. De cette manière, il est possible pour chacun des participants de comprendre ce qu'une LTF peut ou non fournir ;
- dans le cas spécifique de la VSSE, il s'est avéré que les participants ne savaient pas toujours quelles informations pouvaient être partagées. Le Comité a recommandé que cet aspect soit éclairci au sein même des services, et que des représentants des postes de province qui participent aux réunions soient soutenus et guidés activement par l'administration centrale ;
- les services de renseignement devaient toujours réfléchir au niveau de classification le plus approprié de toute information, et ce vu qu'au moment

où l'enquête a été effectuée, tous les participants aux LTF n'étaient pas titulaires de l'habilitation de sécurité requise ;
– le SGRS participait moins aux LTF que la VSSE. La suggestion du SGRS de se faire représenter par la VSSE à ces réunions était envisageable, selon le Comité, mais à condition que les attentes mutuelles et les procédures d'échange d'informations entre le SGRS et la VSSE soient bien décrites ;
– étant donné que les protagonistes des attentats se trouvaient principalement à Bruxelles, les LTF d'autres arrondissements n'ont pu transmettre que peu d'informations.

II.3.4.2. La collaboration dans le cadre du Plan Radicalisme (Plan R)

En ce qui concerne le Plan R, le Comité a, en premier lieu, attiré l'attention sur la '*Joint Information Box*' (JIB). Les Comités permanents R et P avaient déjà effectué une enquête sur cette liste de vecteurs 'radicalisants' gérée par l'OCAM. L'enquête a essentiellement montré qu'au cours de la période sur laquelle portait l'enquête, la JIB était peu performante, et qu'en règle générale, elle donnait surtout lieu (et la plupart du temps, seulement) à un signalement policier.[43]

Outre la liste JIB, les différents groupes de travail thématiques et *ad hoc*, étaient également mentionnés. La VSSE et le SGRS faisaient partie de ces groupes de travail, qui avaient été créés dans le cadre du Plan R. Vu les délais impartis pour la réalisation de l'enquête, le Comité permanent R n'a pas pu examiner quelle était la contribution de ces groupes dans le contexte du suivi des FTF.

II.3.4.3. La collaboration entre la VSSE et le SGRS

Une collaboration optimale et efficace doit exister entre les deux services de renseignement. Le Comité avait déjà pu constater que la collaboration était perfectible, et il avait émis plusieurs recommandations en ce sens.[44] Les résultats de la présente enquête laissent supposer que la situation avant les attentats et au moment des attentats de Paris pouvait toujours être améliorée. Le Comité a, en effet, dressé les constats suivants :
– les réunions bilatérales entre la VSSE et le SGRS en vue d'échanger des informations opérationnelles étaient peu nombreuses. Des contacts étaient évidemment possibles dans d'autres circonstances (par exemple, dans le cadre des réunions LTF) ;

---

43 Le Comité se référait à cette enquête et aux recommandations formulées à ce moment-là. COMITÉ PERMANENT R, *Rapport d'activités 2015*, 7-11 ('II.1. Enquête de contrôle commune sur la *Joint Information Box* de l'OCAM') et 100-101 ('IX.2.1. Recommandations relatives à la *Joint Information Box*').

44 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 120-121 ('IX.2.2. Une collaboration plus étroite entre les deux services de renseignement').

– un nombre limité de documents était échangé entre les services de renseignement en matière de lutte anti-terroriste ;
– le SGRS peinait à définir son rôle dans la lutte anti-terroriste. Par conséquent, les différents partenaires ne savaient pas très bien ce qu'ils pouvaient attendre ;
– enfin, le Comité a attiré l'attention sur les problèmes en matière de gestion des informations[45] au SGRS, problèmes qui avaient déjà été constatés et qui ne facilitaient pas la collaboration avec ses partenaires, dont la VSSE.

II.3.4.4. La collaboration avec les autorités judiciaires et la police[46]

En ce qui concerne la collaboration avec la police et la justice, le Comité a dressé les constats suivants :
– s'il y a bien eu de nombreux contacts et de nombreuses formes d'échanges d'informations entre les services, en particulier entre la VSSE et la Police fédérale, ils n'ont donné que peu de résultats concrets concernant les personnes sur lesquelles portait l'enquête ;
– s'agissant de l'observation d'un des protagonistes, la VSSE et la police ont bien collaboré, à l'automne 2015, dans le cadre de la vérification d'un renseignement déterminé ;
– comme cela apparaîtra au point II.3.6.1, la VSSE a lancé des avertissements importants à certains moments, y compris aux autorités judiciaires et à la police ;
– pour ce qui est du SGRS, le Comité note surtout son rôle dans l'initiation et le traitement du dossier judiciaire Zerkani.[47] En effet, une note du SGRS informait pour la première fois les autorités judiciaires de la présence d'un groupe de personnes radicalisées à Molenbeek ;
– le Comité a constaté que depuis 2015, le SGRS réservait généralement une suite favorable aux demandes d'assistance technique du Procureur fédéral. Le

45 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 103 ('IX.2.12. Un système de gestion des données performant pour le SGRS') et *Rapport d'activités 2011*, 12-13 et 106-107.

46 Il existe toute une série de normes relatives à la collaboration et à l'échange d'informations entre les services de renseignement et les autorités policières et judiciaires : l'article 29 CIC, les articles 19, 19/1 et 20 § 2 L.R&S, la COL 9/2005 du Collège des Procureurs généraux relative à l'approche judiciaire en matière de terrorisme, la COL 9/2012 relative à la collaboration entre la VSSE/SGRS et les autorités, la COL 10/2015 du Collège des Procureurs généraux relative à l'approche judiciaire en matière des *foreign terrorist fighters* et la Circulaire du 21 août 2015 des ministres de la Justice et de l'Intérieur relative à l'échange d'informations et au suivi des *foreign terrorist fighters* en provenance de Belgique. Par ailleurs, un *Memorandum of Understanding* a été conclu entre le SGRS, la VSSE, l'OCAM et la Police fédérale après les attentats de Paris. Ce MoU prévoit une concertation régulière et structurelle dans le cadre de la lutte contre le terrorisme afin de dégager une position d'information commune.

47 Cette personne a été condamnée, avec plusieurs autres, par un arrêt de la cour d'appel de Bruxelles du 14 avril 2016. Elle ne fait cependant pas partie des protagonistes repris dans l'enquête de contrôle.

SGRS a déclaré le faire pour avoir accès au dossier, et donc pour parfaire ses connaissances sur les *foreign terrorist fighters*.

II.3.4.5. La collaboration avec l'OCAM

Conformément à l'article 6 L.OCAM, la VSSE et le SGRS sont tenus, en tant que services d'appui, « *de communiquer à l'OCAM, d'office ou à la demande de son directeur, tous les renseignements dont [elle] dispose[nt] dans le cadre de [ses] missions légales et qui s'avèrent pertinents pour l'accomplissement des missions prévues à l'article 8, 1° et 2°* ». Il convient de noter que la VSSE a toujours interprété cette obligation dans le sens qu'aucune information brute ne doit être transmise, mais seulement des renseignements traités.

Tant la VSSE[48] que le SGRS ont détaché deux experts permanents auprès de l'organe de coordination. Ces experts assurent également la fonction d'officiers de liaison.

II.3.4.6. La collaboration avec l'Office des étrangers (OE), le Commissariat général aux réfugiés et aux apatrides (CGRA) et Fedasil

La collaboration entre la VSSE et ces services est ancienne et ne se limite pas au terrorisme. La VSSE dispose d'un officier de liaison permanent auprès des trois services. Ces fonctions ont pris une importante particulière avec la crise migratoire de l'été 2015, lorsqu'il a été demandé à la VSSE d'effectuer un screening de tous les demandeurs d'asile.[49]

Le SGRS entretient lui aussi, depuis un certain temps, des contacts avec les trois services. Il a récemment désigné un point de contact pour centraliser l'échange d'informations.

II.3.4.7. La collaboration avec la Direction générale des Établissements pénitentiaires

Le Comité permanent R avait déjà effectué une enquête sur la collaboration entre la VSSE et les établissements pénitentiaires.[50] Il a constaté qu'à la mi-2015, la

---

48 En vue d'optimaliser le flux d'informations avec l'OCAM, la VSSE a désigné une personne de contact après les attentats de Paris. Cette personne est proche de la direction et entretient des contacts réguliers avec l'expert détaché auprès de l'OCAM.

49 Entre le 7 septembre 2015 et le 11 mai 2016, 17643 personnes ont fait l'objet d'un screening. 82 d'entre elles étaient connues dans les banques de données de la VSSE, dont 15 pour radicalisme. Six enquêtes à peine ont été ouvertes concernant des personnes susceptibles d'être liées à l'EI, mais aucune de ces enquêtes n'a démontré un lien avec les auteurs des attentats de Paris. Selon la VSSE, le résultat de ces enquêtes était limité, malgré un investissement assez important.

50 Voir 'II.6. La VSSE et le Protocole de coopération avec les Établissements pénitentiaires' dans ce rapport d'activités.

VSSE avait créé cellule 'GP' ('Gevangenissen/Prisons'). Cette cellule traite de nombreuses informations dans le cadre de la radicalisation et du terrorisme.[51]

II.3.4.8. La collaboration avec les unités opérationnelles de la Défense

Dans le cas spécifique du SGRS, le Comité a attiré l'attention sur les liens qui existent entre le service de renseignement et les unités opérationnelles de l'Armée, ayant pour tâche de veiller à la sécurité, en appui de la police. Un déploiement à grande échelle permettait naturellement à ces unités de recueillir des informations (par exemple, des faits suspects dont elles étaient témoins) et de les rapporter. Ainsi, un détachement opérationnel a signalé la présence éventuelle d'Abaaoud en Belgique, au cours de l'été 2015. Cette information a été communiquée à la police, mais également au SGRS via la chaîne de commandement militaire.

En raison des délais impartis, le Comité n'a pas été en mesure d'enquêter sur ces flux d'informations, ni sur la manière dont le SGRS a rempli sa mission première dans le cadre de la *force protection* des unités de l'armée déployées sur le terrain (voir II.4.3.3).

II.3.4.9. La collaboration avec la Direction générale du centre de crise

Enfin, les contacts entre la VSSE et le SGRS, d'une part, et le Centre de crise, d'autre part, étaient également fréquents. Ces contacts ne se limitaient pas au terrorisme; ils pouvaient aussi, par exemple, porter sur la sécurité publique générale (manifestations). La VSSE dispose d'un officier de liaison permanent à la DGCC.

II.3.5. LA COLLABORATION AU NIVEAU INTERNATIONAL

L'article 20 L.R&S stipule que les services de renseignement doivent veiller à assurer une collaboration avec leurs homologues étrangers. La manière dont la VSSE et le SGRS ont mis en œuvre cette disposition est résumée ci-après.

II.3.5.1. La collaboration internationale de la VSSE

La VSSE est membre de diverses plateformes multilatérales de coopération (Club de Berne, *Terrorism Group*…), et y collabore avec d'autres services au niveau opérationnel (par exemple, l'échange d'informations) *et* analytique. On y prépare également des orientations politiques en matière de sécurité nationale et

[51] Au moment où l'enquête a été réalisée, le Comité permanent R a constaté que la masse d'informations ne permettait pas un traitement de toutes les données.

internationale au sens large. Si la collaboration opérationnelle a généralement lieu au niveau bilatéral, une collaboration opérationnelle intense existe aussi au niveau multilatéral.

Par ailleurs, il existe également des forums qui ne sont pas axés sur les services de renseignement, mais qui n'en jouent pas moins un rôle important dans la lutte contre le terrorisme (par exemple, Europol, l'OTAN…). La VSSE dispose d'officiers de liaison permanents dans certaines organisations.

Au moment où l'enquête a été menée, la VSSE entretenait des contacts bilatéraux avec des services issus d'une septantaine de pays. L'intensité et la fréquence de la collaboration variaient considérablement. Les relations les plus fréquentes et les plus intenses dans le cadre de la lutte contre les FTF étaient celles entretenues avec nos voisins et avec certains pays non européens proches de la zone de conflit.

Une forme avancée de coopération bilatérale est l'échange d'officiers de liaison. S'agissant des relations avec son homologue français, la VSSE tentait depuis longtemps déjà d'instaurer cette forme de coopération, mais elle ne s'est concrétisée qu'après les attentats de Paris.

La VSSE faisait également partie d'un groupe de travail de partenaires européens et non européens qui a été constitué peu avant les attentats, pour se concentrer sur Abaaoud. Pris de court par les attentats de Paris, le groupe de travail ne s'est jamais réuni.

Les hypothèses parallèles sur des projets d'attentats en Europe, où il aurait joué un rôle clé, ont mobilisé quinze services étrangers, qui, ensemble, disposaient de toute une série de moyens. Dans ce cadre, la VSSE a reçu énormément de renseignements. Il est néanmoins apparu que les personnes qui n'étaient pas connues à la VSSE, la plupart du temps, ne l'étaient pas non plus dans d'autres services étrangers.

La VSSE a également diffusé les informations dont elle disposait, ou a demandé à ses partenaires de compléter ses propres données. Les efforts menés au niveau international ont donné un résultat (limité) à l'été 2015 : trois pays différents ont appréhendé trois terroristes dont les propos indiquaient clairement l'extrême gravité de la menace qui pesait sur l'Europe.

À partir de la mi-août 2015, l'échange d'informations s'est intensifié : la VSSE a reçu de nombreuses notes comportant des renseignements ou des demandes de renseignements. La VSSE a elle-même donné ou demandé toute une série d'informations à ses partenaires étrangers.

On peut en conclure que l'échange d'informations a été intense, et qu'aucun élément n'indiquait que la VSSE ne partageait pas certaines données.

II.3.5.2. La collaboration internationale du SGRS

Le SGRS est lui aussi membre de diverses plateformes de coopération. Par exemple, le service participe, depuis août 2015, à une plateforme qui assure le

suivi des activités de membres et sympathisants de l'EI dans les médias sociaux. Le SGRS participait également à des groupes internationaux œuvrant à l'élaboration d'un contre-discours pour neutraliser la propagande de l'EI, qui est diffusée via internet et les médias sociaux.[52]

II.3.6. QUAND ET COMMENT LES SERVICES DE RENSEIGNEMENT ONT-ILS INFORMÉ LES AUTORITÉS COMPÉTENTES DE LA MENACE ?

Au cours de l'été 2015, les services ont reçu plusieurs signaux importants montrant clairement qu'une menace terroriste croissante visait spécifiquement l'Europe. Le Comité a examiné si et de quelle manière la VSSE et le SGRS en ont averti les autorités. Mais il a aussi vérifié comment les services avaient procédé les années précédentes. Le Comité a distingué quatre périodes.

En novembre 2012, le premier ressortissant belge connu a quitté la Belgique pour rallier la région syrienne. C'est la période au cours de laquelle a également été créé l'État islamique en Irak et au Levant (EIIL, qui est entre-temps devenu l'EI).

Une nouvelle période s'annonçait à compter de l'automne 2013 ; il était alors question des premiers *returnees*. Même en l'absence d'indices spécifiques, il était clair qu'ils pouvaient représenter une menace.

L'attaque du Musée juif de Bruxelles en mai 2014, la proclamation du Califat par l'EI en juin 2014 et l'appel à perpétrer des attentats, ont inauguré une nouvelle période. C'est à ce moment-là que la Belgique a rejoint, elle aussi, la coalition internationale, au sein de laquelle des militaires ont été déployés pour contrer l'EI.

La quatrième et dernière période a débuté lors de l'attaque contre Charlie Hebdo et du démantèlement de la cellule terroriste de Verviers en janvier 2015. Cette cellule était (en partie) téléguidée depuis l'étranger (avec Abaaoud comme figure centrale). Cette période s'est caractérisée par l'infiltration en Europe de candidats terroristes formés par l'EI. Plusieurs d'entre eux ont été arrêtés ; ils ont dévoilé les projets d'attentats contre la France, la Belgique et l'Allemagne. En août 2015, juste avant les attentats de Paris, il y a encore eu l'attentat manqué contre le Thalys, le train à grande vitesse.

II.3.6.1. La Sûreté de l'État

Le Comité a pu constater que la VSSE avait détecté la menace terroriste croissante et avait émis des avertissements à des moments clés.

---

52 Les jours suivant les attentats de Paris et de Bruxelles, le SGRS a développé une collaboration bilatérale étroite avec plusieurs partenaires européens et non européens. À cet égard, le Comité a constaté que le SGRS collabore aussi bien avec des services de renseignement militaires que civils.

Au cours de la première période, où il était surtout question d'individus se rendant en Syrie, la réaction de la VSSE était plutôt attentiste. Ce qui ne signifiait pas que la VSSE ne s'en préoccupait pas. Au contraire, en octobre 2012 déjà, une note était adressée aux autorités politiques pour attirer leur attention sur le phénomène des départs vers la Syrie. Dès ce moment-là, la VSSE avait averti les autorités que des combattants pourraient rentrer pour commettre des attentats. Le service pensait plutôt à des 'loups solitaires' qu'à des groupes organisés.

Lors de la transition entre la deuxième et la troisième période, la VSSE a lancé de plus en plus d'avertissements aux ministres compétents. Des briefings ont également été organisés, notamment sur la problématique des *returnees*, mais sans qu'il ne soit encore question d'éventuels attentats en Occident.

Cependant, à la fin de la troisième période – la menace était entre-temps devenue réelle – peu de notes (voire aucune) ont été envoyées aux (nouveaux) ministres, ce que la VSSE a expliqué par le fait que nombre de dossiers ont été traités par les autorités judiciaires après l'opération de Verviers.

Au cours de la période précédant les attentats, la VSSE a lancé deux avertissements importants, annonçant l'éventualité d'attentats en France, en Belgique et en Allemagne.

À la lumière de ce qui précède, le Comité permanent R a conclu que la VSSE avait tenté de réagir de manière adéquate à la menace qui s'annonçait. La VSSE a réalisé, à un moment clé, que la menace se concrétisait (d'abord les départs vers la Syrie, ensuite la menace des *returnees*), et a émis des avertissements à plusieurs reprises.

II.3.6.2. Le Service Général du Renseignement et de la Sécurité

Le Comité a vérifié si le SGRS avait, lui aussi, émis les bons avertissements au bon moment. À cet égard, il convient de tenir compte du fait que le SGRS n'était pas directement concerné par la problématique des civils partis combattre en Syrie. En principe, ce n'est que lorsqu'il s'agit de militaires ou d'anciens militaires, ou qu'il est question d'intérêts militaires (comme la protection de troupes ou d'installations militaires), que le SGRS agit dans le cadre de ses compétences.

Le terrorisme islamique était depuis longtemps un point d'attention pour le SGRS. Depuis 2011, il constituait une priorité, et plus particulièrement les individus, en Belgique ou à l'étranger, pouvant être liés à ces groupes et faisant peser une menace sur les intérêts militaires belges.

Au cours de la première période de la menace, les rapports du SGRS se limitaient à fournir des renseignements à la chaîne de commandement militaire pour ce qui concerne la *force protection*, en Belgique et à l'étranger.

En juillet 2013, le SGRS a créé un service Joint Terro. Juste après Verviers et suite à une réunion avec le Conseil national de sécurité, le SGRS a élargi la

définition de sa compétence et s'est également engagé sur le terrain 'civil'. À partir de moment-là, le SGRS a lancé plusieurs avertissements importants. L'objectif était non seulement d'avoir une vue sur le radicalisme au sein de l'armée en Belgique et sur la menace terroriste contre les troupes présentes sur les théâtres d'opérations (Afghanistan et Liban), mais également de cartographier les réseaux et les phénomènes extrémistes islamistes dans une région et un contexte bien plus larges. Et ce, en partant du principe que le terrorisme ne se cantonnerait pas nécessairement à la Syrie, mais finirait par nous atteindre. Le Comité permanent R a jugé la réaction pertinente.

En février 2015, le SGRS a donné un briefing au Conseil national de sécurité concernant la menace que représente l'EI pour la Belgique.

Une semaine avant les attentats de Paris, le SGRS a encore diffusé un renseignement très important sur un attentat imminent.

II.3.7. COMMENT LES SERVICES ONT-ILS RÉAGI À L'ÉVOLUTION DE LA MENACE ?

Le Comité permanent R a cherché à savoir comment les deux services de renseignement, comme organisations, avaient réagi à la menace terroriste croissante, et s'ils avaient adapté leurs structures et leurs processus de travail. Le Comité a examiné la problématique en se basant sur les quatre périodes précitées.

II.3.7.1. La Sûreté de l'État

Avec la création de la 'Taskforce Syrie' au printemps 2013, la VSSE s'est concentrée sur la problématique des *foreign fighters*. Le travail opérationnel semblait encore à un stade exploratoire, étant donné que la menace ne faisait que poindre et que, de toute manière, elle était encore éloignée de la Belgique. La VSSE participait également à un groupe de travail international nouvellement créé.

À partir de la deuxième période, les procédures de travail internes ont été adaptées. Cette adaptation consistait en une collaboration plus étroite entre les services de collecte et d'analyse de la VSSE dans la lutte contre l'extrémisme et le terrorisme. À compter de la fin 2013, il est également ressorti des chiffres en matière de méthodes particulières de renseignement que l'attention du service avait basculé vers le terrorisme en lien avec la Syrie.

À la fin de la troisième période, une réorganisation profonde a été planifiée. Ces adaptations structurelles faisaient partie du projet de Plan d'action 2015 figurant dans le Plan d'action 2014, où la lutte contre le terrorisme était considérée comme la priorité la plus importante. Dans le même temps, la VSSE a œuvré à l'amélioration de la collaboration avec l'administration pénitentiaire et à un renforcement de la capacité SOCMINT.

Au cours de la période précédant les attentats de Paris, le Plan d'action 2015, qui a été approuvé en juin par le Conseil national de sécurité et pour lequel le gouvernement a dégagé des moyens, a été implémenté. Cette réorganisation a, bien entendu, pris du temps, entre autres parce que la réforme a été court-circuitée par les événements de Verviers et par l'attentat manqué du Thalys. Lors de la dernière période, la VSSE a investi beaucoup de moyens pour tenter de suivre la trace des éléments terroristes, mais sans résultats probants.

II.3.7.2. Le Service Général du Renseignement et de la Sécurité

En ce qui concerne le SGRS, le Comité permanent R estimait que vu sa compétence limitée en la matière, des modifications importantes de la structure n'étaient pas nécessaires dans un premier temps.

Au début de la deuxième période – lorsqu'il était clair que les *returnees* pouvaient bien représenter un danger – le SGRS a procédé à une adaptation structurelle. Après Verviers, de nouveaux objectifs ont été fixés, et la compétence a été définie de manière plus large (*supra*). Le Comité permanent R a jugé la réaction pertinente, même si la mise en œuvre demeurait problématique eu égard aux moyens limités.

La troisième période a vu le SGRS adapter ses priorités et renforcer sa collaboration internationale en matière de SIGINT. À la fin 2014, il a été proposé de consacrer davantage de moyens de collecte à la collecte permanente de renseignements sur le terrorisme djihadiste. À la même période, la Belgique a décidé de rejoindre la coalition contre l'EI. Cette participation a permis au SGRS d'accéder à des informations émanant d'autres partenaires présents dans la zone de conflit.

La quatrième période a constitué un moment clé pour le SGRS. Sa compétence, qui était jusqu'alors 'militaire', était interprétée de manière plus large. Le SGRS s'intéresserait dorénavant aussi aux menaces avec 'des moyens militaires', même si elles étaient mises à exécution par des non-militaires ou si elles étaient dirigées contre des cibles non militaires. Le SGRS s'est par ailleurs investi dans le renforcement de la coopération internationale, saisissant ainsi les opportunités offertes par l'évolution militaire internationale.

II.3.8. QUELQUES PROBLÈMES STRUCTURELS ET LES RISQUES QUI EN DÉCOULENT

Le Comité permanent R a mis en avant quelques problèmes structurels qui se posaient dans les services et certains risques qui en découlent. Pour la VSSE, il s'agissait de l'accroissement de la charge de travail, tandis que pour le SGRS, c'est la situation problématique de la gestion des données qui était pointée.

II.3.8.1. La charge de travail croissante et la réorganisation inachevée à la VSSE

Au cours de l'enquête, le Comité a noté une forte augmentation de la charge de travail au sein de la VSSE, et ce principalement dans la lutte anti-terroriste : davantage de données traitées, niveau d'urgence plus élevé, menace accrue… En revanche, le service disposait, en 2015, de 15 % de collaborateurs en moins qu'en 2010.[53] Venaient s'y ajouter la problématique des heures supplémentaires et des jours de vacances non pris, ainsi que la tendance à la baisse de l'absentéisme pour maladie, qui se situait néanmoins toujours au-dessus de la moyenne fédérale. Aussi le Comité a-t-il insisté sur un transfert rapide du Service Protection des personnes de la VSSE à la Police fédérale[54], ce qui libérerait une vingtaine d'inspecteurs pour effectuer du travail de renseignement.[55] Dans un même souci, le Comité a attiré l'attention sur les problèmes qui compliquaient le recrutement de nouveaux membres du personnel.

Le Comité permanent R a pu constater la finalisation de la réforme interne à la VSSE au niveau des services de collecte. Au moment de l'enquête, ce n'était pas encore le cas pour les services d'analyse. En d'autres termes, il n'y avait pas de parallélisme entre la collecte, organisée en fonction des thématiques, et l'analyse, encore divisée en zones géographiques, ce qui compliquait la collaboration. Le regroupement physique des services de collecte et d'analyse, qui visait à améliorer la communication, n'était, de ce fait, pas non plus complètement concrétisé et compliquait la collaboration.

II.3.8.2. La gestion des informations au SGRS

Le Comité permanent R a rappelé que la gestion des informations était problématique au SGRS.[56] Même la hiérarchie de ce service avait plusieurs fois abordé le sujet.

L'enquête a révélé la faiblesse de la production émanant du SGRS concernant les protagonistes des attentats de Paris. Selon le SGRS, cette maigre production tenait au fait qu'il se concentrait d'abord sur les menaces militaires ou les menaces impliquant des militaires, et au fait que les auteurs (en premier lieu) ne relevaient pas de cette catégorie.[57] Mais ce n'était pas la seule explication. Au cours de son enquête, le Comité est tombé sur des informations qui étaient bel et bien disponibles, mais qui ne pouvaient pas être immédiatement retrouvées. Une

---

53 Début 2016, on a observé une nouvelle augmentation de personnel, à la faveur de la décision du gouvernement, courant 2015, de recruter de nouveaux inspecteurs et analystes.

54 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 45 et s.

55 Ce transfert est à présent effectif.

56 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 12-13 et 106-107.

57 Peu après les événements survenus à Verviers, un changement s'est opéré : il est devenu évident que les services de renseignement avaient affaire à des personnes qui s'inscrivaient dans la 'stratégie militaire' du groupe terroriste EI. À compter de ce moment, Abaaoud en particulier était clairement une cible légitime, y compris pour le service de renseignement militaire.

fois de plus, le Comité a donc dû constater que la gestion des informations au sein du SGRS était problématique. En effet, le système ne permettait pas de retrouver avec certitude la totalité des données disponibles.

Certes, le SGRS disposait d'un système simple et moderne, qui permettait de relier les données et qui était doté des fonctionnalités nécessaires pour gérer le flux d'informations d'un service de renseignement, mais par manque de personnel pour procéder à l'encodage nécessaire et par manque de formation en vue de l'utilisation du système, il n'était que peu, voire pas, utilisé. En résumé, le Comité a conclu que la gestion des flux d'informations comportait un risque pour l'ensemble du processus de renseignement au SGRS.

II.3.9. CONCLUSIONS GÉNÉRALES

Les efforts des services de renseignement n'ont pas permis de détecter à temps une cellule qui était en lien avec la Belgique et qui était en mesure de perpétrer des attentats à grande échelle. La collaboration internationale intense nouée entre près de vingt services européens et non européens n'a pas non plus permis de retrouver Abaaoud à temps.

En revanche, le Comité permanent R n'a pas détecté de défaillances manifestes dans la manière dont les deux services de renseignement ont tenté de remplir leurs missions respectives avant les attentats de Paris. Aucun élément n'indiquait la rétention de certaines informations au détriment des partenaires (étrangers).

Il n'en demeure pas moins que le Comité estimait – comme dans l'enquête sur le suivi des FTF (voir II.1) – que toute une série d'aspects étaient perfectibles (voir XI.1 et XI.2.1).

II.4. LA POSITION D'INFORMATION DES DEUX SERVICES DE RENSEIGNEMENT AVANT LES ATTENTATS DE ZAVENTEM ET DE MAELBEEK

II.4.1. RAPPEL DES FAITS

Depuis le déclenchement de la guerre civile en Syrie, en 2011, des centaines de Belges ont pris part à ce conflit. À un moment donné, la Belgique comptait proportionnellement le plus grand nombre de combattants étrangers sur le sol syrien. Mais depuis 2015-2016, le théâtre des opérations s'est déplacé. L'EI a perpétré des attentats terroristes aux quatre coins du monde.

La Belgique a été visée elle aussi. En janvier 2013, les médias rapportaient le départ de Bruxellois pour la Syrie et la menace d'attentat qui planait sur la capitale. Le 24 mai 2014, Mehdi Nemmouche a abattu quatre personnes au

Musée juif de Bruxelles. Il s'agit d'un combattant de retour de Syrie. Ensuite, le terrorisme a frappé Charlie Hebdo, Lyon, Paris… Le lien avec la Belgique sonnait comme une évidence.

Après les attentats de Paris, une traque (internationale) impliquant les services de police et de renseignement a été organisée pour retrouver les autres auteurs. Un des auteurs est Salah Abdeslam. Il aurait tenté de pénétrer dans le Stade de France avec une ceinture d'explosifs, mais se serait ravisé. Il a fui en direction de la Belgique, où il a disparu sans laisser de trace. Le niveau de la menace a été établi à 3, ce qui signifie que la menace est grave, possible et vraisemblable. Entre autres phénomènes : certains cinémas ont fermé leurs portes, les centrales nucléaires étaient en ligne de mire des milieux terroristes…

Le 15 mars 2016, l'unité anti-terroriste de la Police fédérale a effectué une perquisition à Forest dans le cadre de l'enquête sur les attentats de Paris. Les agents s'attendaient à trouver un logement vide, mais ils ont d'emblée essuyé des tirs. Quatre personnes ont été blessées. Lors de l'assaut des unités spéciales, un suspect a été abattu, une Kalachnikov à la main. Rétrospectivement, il s'est avéré qu'il s'agissait de Mohamed Belkaid, qui n'était connu auparavant que sous son nom d'emprunt, Samir Bouzid. Deux autres suspects sont parvenus à prendre la fuite. On peut déduire des traces laissées sur place qu'il pouvait s'agir de Salah Abdeslam et d'Amine Choukri, qui était encore porteur d'un faux passeport syrien au nom d'Ahmed Monir Alhay. L'enquête s'est poursuivie sans relâche.

Trois jours plus mars, le 18 mars, Salah Abdeslam a été arrêté dans une planque à Molenbeek. Amine Choukri, dont le véritable nom est Soufiane Ayari, a lui aussi été arrêté.

Le 22 mars 2016, les kamikazes Ibrahim El Bakraoui et Najim Laachraoui (alias Soufiane Kayal) se sont fait exploser dans le hall des départs de Brussels Airport. Un troisième terroriste était présent : Mohamed Abrini a abandonné son trolley rempli d'explosifs et a quitté l'aéroport à pied.

Trois quarts d'heure plus tard, une caméra de surveillance a filmé Khalid El Bakraoui – frère d'Ibrahim – et Osama Krayem (alias Naïm El Hamed) à un distributeur de tickets de la station de métro bruxelloise Pétillon. Entre-temps, la gare ferroviaire souterraine de l'Aéroport de Bruxelles National a été fermée. Le niveau de la menace a été porté à 4 : la menace était très grave et imminente. Vers 9h00, l'ordre a été donné d'évacuer les stations de métro bruxelloises et les cinq gares ferroviaires. La phase fédérale de la gestion de crise a été annoncée, et le plan d'urgence national en cas d'attentat terroriste, activé. Cela n'a pas pour autant permis d'empêcher le kamikaze Khalid El Bakraoui de se faire exploser à 9h11 dans une rame de métro qui était partie de la station Maelbeek en direction d'Arts-Loi.

Dans les deux cas, il s'agissait d'attentats suicide, où les auteurs, armés d'explosifs 'maison' (bombes remplies de clous placées dans des valises), se sont fait exploser dans la foule. Le bilan est très lourd : 35 personnes ont perdu la vie, tandis que le nombre total de blessés dépassait les 300.

Certains auteurs étaient des *foreign terrorist fighters* (FTF) rentrés au pays et liés au groupe terroriste État islamique (EI), qui a revendiqué les attaques le jour même, en avançant diverses raisons (Bruxelles comme capitale de l'Union européenne, participation de la Belgique aux attaques en Syrie, détention de Malika El Aroud et de Salah Abdeslam, interdiction du port du hijab…).

Un lien avec les attentats de Paris est rapidement apparu : Najim Laachraoui a été signalé comme étant en compagnie de Salah Abdeslam, et son ADN a été trouvé sur la ceinture d'explosifs qui a été utilisée dans la salle de concert du Bataclan. Tout de suite après les attentats, la VSSE a déclaré qu'il était de plus en plus évident que les attentats de Bruxelles étaient le prolongement des attentats de Paris. En effet, dans les deux cas, il s'agissait d'attentats revendiqués par l'EI, en partie préparés (et perpétrés) par les mêmes personnes et sur un mode similaire.

Mohamed Abrini, qui était recherché depuis les attentats de Paris, a été arrêté le 8 avril 2016 à Anderlecht. Le même jour, Osama Krayem était lui aussi arrêté à Laeken. Le même sort a été réservé au Rwandais Hervé Bayingana-Muhirwa.

Il était suspecté d'avoir aidé Abrini et Krayem après les attentats en ce qui concerne la planque. Bilal El Makhouki, condamné en 2015 lors du procès Sharia4Belgium, a lui aussi été placé en détention.

Le 11 avril 2016, Ibrahim Farisi a été arrêté avec son frère Smail. Ibrahim Farisi était le locataire de l'appartement situé à Etterbeek, d'où sont partis les auteurs des attentats du métro de Bruxelles. Il utilisait le flat pour obtenir une allocation du CPAS, mais l'avait prêté à Khalid El Bakraoui.

Par ailleurs, Ali El Haddad Asufi, qui aurait eu une fonction logistique dans la préparation des attentats, et Youssef El Ajmi, un ami d'enfance de Khalid El Bakraoui et d'Ali El Haddad Asufi, ont eux aussi été arrêtés. Par ailleurs, l'enquête a mené à l'arrestation de Jawad et Mustapha Benhattal et de Samir Chahjouani, le 17 juin 2016.

Quelques mois après les attentats, Oussama Atar (alias Abou Ahmad), un cousin des frères El Bakraoui, s'est également retrouvé dans le collimateur comme éventuel cerveau des attentats. Atar avait précédemment été détenu à Abu Ghraib. Il a été incarcéré jusqu'en 2012 en Irak, mais a bénéficié d'une libération anticipée après la demande d'Amnesty International et des autorités belges de le rapatrier en Belgique pour raisons humanitaires. Depuis lors, Atar était introuvable. Il serait un pionnier des départs de combattants vers la Syrie.[58]

II.4.2. OBJECTIF DE L'ENQUÊTE DE CONTRÔLE

L'enquête a suivi le même canevas que l'enquête sur les attentats de Paris (II.3).[59] Le Comité permanent R a noté, immédiatement après les faits, les noms des

[58] Le nom de Yassine, le plus jeune frère d'Atar, a également fait surface. Il a été arrêté, et des traces d'explosifs auraient été trouvées sur ses doigts.

[59] L'enquête de contrôle « *relative à la position d'information des deux services de renseignement sur les individus ou groupes ayant perpétré des attentats ou liés aux attentats de Bruxelles-*

personnes impliquées dans les attentats comme (présumés) auteurs ou co-auteurs.[60] Tout d'abord, la position d'information à l'égard des personnes sélectionnées, avant les attentats de Bruxelles, a été esquissée. Le Comité s'est ensuite penché sur les différents moyens de collecte (HUMINT, SOCMINT, SIGINT et MRD). La collaboration des services avec leurs partenaires et correspondants, tant au niveau national qu'international, a par ailleurs été abordée. Enfin, le Comité a procédé à la description des activités déployées par la VSSE au cours de la période précédant les attentats.

II.4.3. LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT

II.4.3.1. La Sûreté de l'État

Le Comité a tout d'abord établi un aperçu du nombre de documents en possession de la VSSE, dans lesquels le nom (ou l'alias) des (co-)auteurs (sélectionnés) figurai(en)t, et ce depuis les attentats de Paris jusqu'aux attentats de Bruxelles. Les chiffres variaient de quelques documents à plusieurs centaines. Pour la période précédant le 22 mars 2016, le Comité a également noté quand un (co-)auteur avait été remarqué pour la première fois, et quand le service avait reçu ou traité des informations à son sujet. Le Comité a ensuite tracé une ligne du temps pour chacun des (co-)auteurs, reprenant les flux d'informations et donnant une brève description de la position d'information et de son évolution. La 'source' des informations (collecte des services eux-mêmes, par exemple via des MRD, informations de services belges ou étrangers…) a également retenu toute l'attention.

Les enquêtes du Comité permanent R ont montré que depuis les attentats de Paris, de gros efforts avaient été réalisés pour localiser Abrini et Abdeslam. Les services concernés avaient déployé les grands moyens, tant au niveau national qu'au niveau international. Concernant Abdeslam, la VSSE a échangé des informations avec 27 services étrangers sur quatre continents; s'agissant d'Abrini, 12 service étrangers étaient impliqués. La ligne du temps montrait

---

Zaventem, avant le 22 mars 2016 ainsi que sur les individus ou groupes qui ont permis à Salah Abdeslam de vivre dans la clandestinité, jusqu'à son arrestation le 18 mars 2016 » a été ouverte le 20 juillet 2016. Le rapport final est daté du 4 novembre 2016. Les délais impartis pour la réalisation de cette enquête n'ont pas permis au Comité permanent R d'examiner tous les aspects de la problématique. Le Comité pensait aux thèmes suivants: les *leads* qui ont peut-être fait défaut aux services de renseignement, la manière dont les services ont été gérés par leurs directions respectives, la manière dont la collaboration entre les services de police et de renseignement concernés s'est déroulée, la gestion de crise à la VSSE dans l'approche pratique des attentats du 22 mars.

60 D'autres personnes éventuellement impliquées n'ont été connues que par la suite: il s'agit notamment d'Ali El Haddad Asufi, Youssef El Ajmi, Jawad et Mustapha Benhattal, Samir Chahjouani ainsi que d'Oussama et Yassine Atar.

clairement que l'intensité du flux d'informations avait progressivement diminué à partir de février 2016.

Cependant, des méthodes particulières de renseignement ont encore été mises en œuvre à l'égard d'Abrini jusqu'au dernier moment avant les attentats. Rétrospectivement, sur base des contacts connus d'Abdeslam qui étaient liés aux attentats de Bruxelles, on aurait pu conclure qu'il était possible de relier les noms des intéressés avant les attentats. Mais c'était loin d'être évident. En effet, beaucoup de (co-)auteurs utilisaient des noms d'emprunt et n'ont pu être identifiés que tardivement (ou juste après les attentats). À titre d'illustration, et dans un cas précis, les services pensaient avoir affaire à deux individus distincts, alors qu'en réalité, il s'agissait d'une seule et même personne. L'élaboration d'une position d'information solide en était sérieusement compliquée.

Laachroui et Belkaid ont retenu l'attention de la VSSE parce qu'en septembre 2015, ils avaient été remarqués en compagnie de Salah Abdeslam. À ce moment-là, il était clair pour le milieu du renseignement international (et pour la VSSE) qu'ils appartenaient à un même réseau. Mais ils n'étaient pas encore connus sous leur véritable identité. Najim Laachraoui avait de faux papiers d'identité au nom de Kayal, et Belkaid était en possession d'une fausse carte d'identité au nom de Bouzid. Ils ont pu vivre cachés tout ce temps.

Les frères El Bakraoui étaient connus de la VSSE depuis décembre 2015, mais au départ, avec un profil strictement criminel. Juste après l'assaut de Forest, la donne a changé lorsqu'il est apparu que Khalid avait loué la planque sous un nom d'emprunt.

Osama Krayem – alias Naïm al Hamed – était 'l'homme au sac à dos' qui était en contact avec El Bakraoui peu avant qu'il ne se fasse exploser dans le métro à Maelbeek. En outre, il était impliqué dans la préparation de l'attentat de Zaventem. Il est entré en Europe via la Grèce, comme réfugié syrien, sous un faux nom. Krayem n'était pas connu de la VSSE sous sa véritable identité, et ce jusqu'à l'assaut de Forest, parce que de faux papiers lui appartenant ont été retrouvés.

Avant les attentats du 22 mars 2016, Farisi, Bayingana Muhirwa, Ayari[61] et El Makhouki n'étaient pas des cibles prioritaires pour la VSSE. Mais il s'est avéré que certains d'entre eux avaient joué un rôle de soutien. Ainsi, Farisi avait contribué à faire disparaître des traces dans une planque et avait hébergé des fugitifs. À l'issue de l'enquête de contrôle, on ignorait quel rôle spécifique d'autres personnes avaient joué.

II.4.3.2. Le Service Général du Renseignement et de la Sécurité

Le SGRS ne connaissait, dans ses fichiers, que le nom de quatre des (co-)auteurs, à savoir Salah Abdeslam, Mohamed Abrini, Najim Laachraoui et Khalid El

61 En ce qui concerne Soufiane Ayari, la VSSE savait, avant les attentats, que Salah Abdeslam était aller le chercher dans un autre pays européen. De fausses identités ont, ici aussi, été utilisées.

Bakhraoui.[62] Le Comité a en outre constaté qu'en ce qui concerne ces quatre personnes, le service de renseignement militaire ne disposait pas de la moindre information provenant de sa propre collecte (*infra*). Les informations disponibles émanaient de partenaires nationaux et internationaux, et de la presse nationale et internationale. La plupart des informations disponibles étaient des informations SIGINT transmises par des partenaires étrangers et portaient essentiellement sur les attentats de Paris.

Vu les rares informations (qui, en plus, ne concernaient que quatre (co-) auteurs), force est de constater que la position d'information du SGRS était mauvaise.[63] Le Comité permanent R s'en est étonné, vu que le service considérait le suivi du terrorisme djihadiste comme prioritaire et qu'il a ou avait un rôle[64] à jouer dans le cadre de la *force protection* à l'égard des militaires qui exercent des missions de surveillance aux côtés de la police dans des villes belges.

II.4.3.3. Un flux d'informations particulier au sein de la Défense : l'Operation Vigilant Guardian

Depuis janvier 2015, des militaires patrouillent devant une série de bâtiments stratégiques. Le nombre de militaires a évolué en fonction du niveau de la menace, passant de 150 à plus de 1800 unités. Cette *Operation Vigilant Guardian* (OVG) a pour but d'appuyer la Police fédérale.

Comme lors des opérations où des troupes sont déployées à l'étranger, certains aspects du renseignement interviennent dans le cadre de cette mission sur le territoire belge. Outre les activités de surveillance et de sécurisation, les militaires déployés jouent un rôle de 'détecteur' : ils observent des événements et des incidents pour ensuite les rapporter. Cette 'activité de renseignement' se déroule en principe comme suit : les militaires concernés reçoivent au préalable un briefing détaillé ou non sur l'environnement, ce qui les attend et ce à quoi ils doivent prêter attention. Il importe que pendant ou après la mission, ils fassent également rapport à la chaîne de commandement militaire, auprès des officiers spécialement désignés à cet effet ('G2') au sein de leur unité. De là, les informations partent vers le SGRS. Cependant, les procédures établies dans le cadre de l'OVG sont différentes. Les détachements militaires déployés – ceux qui le sont sur le terrain sous la direction de la Police fédérale – font rapport en

62 Les autres (co-)auteurs n'apparaîtront dans les radars du SGRS qu'après les attentats de Bruxelles.

63 Le Chef du SGRS s'exprimait dans des termes identiques dans le rapport qu'il a rédigé et adressé à la Commission d'enquête parlementaire 'attentats'. En outre, le SGRS a déclaré pouvoir partager en grande partie les conclusions du rapport du Comité permanent R. Le service a une fois de plus attiré l'attention sur le manque criant de personnel auquel il est confronté.

64 On a pu constater lors d'une enquête antérieure que la Loi sur les services de renseignement et de sécurité offrait trois critères pour le recueil et le traitement de données en matière de *foreign terrorist fighters*. Voir à ce propos 'Chapitre II.1.2.2. Le Service Général du Renseignement et de la Sécurité'.

premier lieu à la police.[65] Ces informations sont, il est vrai, rapportées en même temps à la Défense (C-Ops), qui coordonne et suit toutes les opérations. Toutefois, contrairement à ce qui se passe lors d'opérations à l'étranger, le contenu des informations n'est traité ni au sein des unités opérationnelles (dans le chef de leurs officiers 'G2') ni au niveau central (C-Ops). Depuis le C-Ops, les informations partent en copie vers le SGRS, qui les enregistre. En principe, les analystes du SGRS y ont immédiatement accès.

Le Comité permanent R a passé en revue tous les rapports établis par les détachements militaires déployés à Bruxelles et à Zaventem entre le 13 novembre 2015 et le 22 mars 2016. Il s'agissait de 24 documents. Le Comité a pu constater que le SGRS recevait bien ces rapports par l'intermédiaire de C-Ops, mais qu'il n'en traitait pas le contenu.[66] Le service de renseignement militaire estimait que la responsabilité du traitement de ces rapports incombait à la Police fédérale.

Le Comité permanent R ne partage pas ce point de vue : le SGRS n'est pas dispensé de vérifier si, dans les documents envoyés, il n'y a pas, le cas échéant, des informations qui peuvent concerner le service. Le SGRS affirmait également ne pas être impliqué dans la préparation des militaires en vue de leur mission dans l'OVG, et n'avoir aucune vue sur la qualité des rapports.

De l'examen de trois cas, le Comité permanent R a pu conclure que le flux d'informations depuis le terrain, dans le cadre de l'*Operation Vigilant Guardian*, soulevait des questions, en ce sens que les informations n'arrivaient pas dans toutes les composantes et services potentiellement concernés.

Ainsi, début mars 2016, deux rapports mentionnaient la présence possible à l'aéroport de Zaventem d'un des futurs auteurs. Des militaires d'un bataillon spécialisé dans la collecte de renseignements étaient à l'origine d'un de ces rapports.[67] Dans un rapport antérieur, datant de novembre 2015, il était fait mention d'une personne qui filmait un dispositif de sécurité des militaires depuis une voiture ; l'intéressé avait, en plus, dissimulé son visage. Le SGRS n'a traité ni transmis aucun de ces trois rapports à la VSSE[68] ou à l'OCAM.[69]

---

65 La Défense a envoyé un officier de liaison à la Police fédérale. Sa mission consiste notamment à rédiger, pour la police, un rapport de synthèse des rapports d'information établis dans le cadre de l'OVG. Le Comité permanent R n'a pas pu constater si et de quelle manière la police faisait un certain usage de ces rapports de synthèse ou des rapports initiaux provenant du terrain. Cet aspect ne relève pas de sa compétence.

66 Le SGRS a déclaré qu'il proposerait à l'État-major de la Défense d'inscrire la procédure à suivre dans le plan d'opérations concerné du Chef de la Défense (CHOD).

67 Les militaires se sont basés sur une liste de noms et de photos de personnes suspectées d'être impliquées dans les attentats de Paris. Même lorsqu'une évaluation de cette liste était demandée au SGRS, le service a répondu que cela ne relevait pas de sa compétence.

68 Le Comité permanent R a vérifié si la VSSE avait, le cas échéant, obtenu ces informations via la Police fédérale. Aucune trace n'a été retrouvée dans la banque de données de la VSSE.

69 Le même problème a été constaté lors de l'enquête sur les attentats de Paris (voir 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris').

Le Comité permanent R estime que, du point de vue de la collecte de renseignements sur le terrain, les détachements OVG peuvent sans aucun doute apporter une contribution précieuse. Certes, les militaires déployés fournissent des informations, mais ils ont aussi besoin que des renseignements leur soient fournis pour remplir correctement leur tâche et pour pouvoir se protéger de manière adéquate. Ici aussi, le SGRS détient une compétence dans le cadre de la *force protection*.

II.4.4. LES MOYENS DE COLLECTE

II.4.4.1. La Sûreté de l'État

Le Comité a pu clairement déduire du nombre de rapports que la VSSE avait activé ses sources (HUMINT) après les attentats de Paris.

En réaction à ces attentats, les services de renseignement et la Police fédérale ont réactivé le groupe de travail créé dans le cadre du Plan R pour traiter la thématique des médias sociaux. Ce groupe de travail, qui regroupe les cellules SOCMINT de la police, du SGRS et de la VSSE, vise à améliorer la collaboration.

Au cours de la période entre les attentats de Paris et ceux de Bruxelles, la cellule SOCMINT de la VSSE a rédigé 15 rapports concernant les (co-)auteurs. Ces informations n'ont pas fait ressortir le moindre élément indiquant un attentat imminent à Bruxelles. Il est néanmoins apparu que certains (co-)auteurs se connaissaient d'une manière ou d'une autre.

Le Comité a analysé, par (co-)auteur, les méthodes de recueil de données (MRD) spécifiques et exceptionnelles qui ont été mises en œuvre entre le 13 novembre 2015 et le 22 mars 2016. Les conclusions de ces analyses coïncidaient avec les conclusions qui ont été tirées à l'issue de l'enquête de contrôle relative aux attentats de Paris (voir II.3.2.2). Les MRD mises en œuvre ont fait avancer l'enquête sur les attentats de Paris. Il est vrai que les MRD n'ont donné aucune indication sur ce qui se passerait par la suite à Zaventem et à Maelbeek. Le Comité a pu constater que l'utilisation de moyens de communication par les terroristes était de plus en plus sophistiquée, ce qui avait contraint les services à multiplier le nombre de MRD.

Le Comité a constaté que dans le cadre des enquêtes judiciaires sur les (co-)auteurs des attentats de Paris, une certaine répartition des tâches avait été définie par le Parquet fédéral, et ce notamment pour éviter que les méthodes d'enquête des services de renseignement ne perturbent les méthodes mises en œuvre au niveau judiciaire.

Le Comité a toutefois pu constater que dans les jours qui ont suivi les attentats de Paris et de Bruxelles, la VSSE avait mis en œuvre de nombreuses MRD dont la finalité de renseignement n'apparaissait pas toujours clairement. La VSSE a reconnu que dans ces moments de crise post-attentats, des *targets* et des

sélecteurs avaient été répartis entre les services de renseignement et la Police judiciaire fédérale. Le service savait pertinemment qu'il lui était arrivé, dans des circonstances précises, de travailler pour les autorités judiciaires. La raison avancée était que la Police judiciaire manquait de personnel. Le Comité permanent R est conscient que la gestion de telles crises requiert de la souplesse de la part de tous les acteurs, mais estime qu'il convient de chercher des solutions en vue d'une répartition optimale des tâches.[70]

II.4.4.2. Le Service Général du Renseignement et de la Sécurité

Le SGRS a activé ses sources à la demande d'un autre service belge, plus spécifiquement concernant deux *targets*, mais aucune source n'a fourni d'informations concrètes.

Le Comité permanent R a pu constater qu'avant le 22 mars 2016, la section SOCMINT du SGRS n'avait effectué aucune collecte active sur les quatre *targets*. Ce n'est que le 21 avril 2016 qu'une liste comprenant vingt personnes à suivre a été diffusée. Cette section a toutefois été restructurée en octobre 2015. À cette époque, la direction du SGRS voulait doter la section d'une capacité analytique et dispenser au personnel une formation *ad hoc*. Le Comité permanent R a constaté que la section n'avait reçu des directives claires quant aux *targets* à suivre que le 25 avril 2016. Selon les membres du personnel de la section, ils n'étaient pas assez nombreux pour suivre toutes les cibles.

Seul le SGRS dispose d'une capacité SIGINT pour intercepter les communications à l'étranger (art. 44*bis* L.R&S). Ce moyen de collecte n'a pas été utilisé dans ce cadre. La section SIGINT du SGRS a néanmoins reçu des informations provenant de partenaires SIGINT étrangers concernant trois (co-)auteurs. Il était question d'un cas où des renseignements pertinents sont parvenus à la section SIGINT peu avant les attentats, qui a partagé ces informations tant en interne qu'avec l'extérieur (principalement avec la VSSE, l'OCAM et le Parquet fédéral). Le Comité permanent R a fait le même constat dans l'enquête sur les attentats de Paris (II.3).

Aucune méthode spécifique et/ou exceptionnelle de recueil de données n'a été mise en œuvre à l'égard des personnes qui se révéleront être les (co-)auteurs des attentats de Bruxelles.

Le Comité a remarqué que le SGRS n'avait pas exploité ses propres pistes après les attentats de Paris, mais qu'il s'était basé sur les constatations de la VSSE. Il a néanmoins appuyé la VSSE, notamment en matière de filature, et en mettant à disposition ses agents maîtrisant des langues spécifiques.

---

70 Après l'enquête de contrôle, des plateformes de concertation ont été créées pour fixer une répartition des *targets* à suivre. Le Comité n'a pas encore pu évaluer ces plateformes.

II.4.5. LA COLLABORATION AU NIVEAU NATIONAL

II.4.5.1. La Sûreté de l'État

Les éléments repris ci-après peuvent venir compléter les constats établis par le Comité dans le cadre de l'enquête sur les attentats de Paris (II.1).

Les services de renseignement et la Police fédérale ont décidé de créer une 'cellule de fusion' du renseignement. Au cours de la période entre les attentats de Paris et ceux de Bruxelles, la VSSE a reçu 200 communications de la Police fédérale sur les (co-)auteurs. L'OCAM a envoyé 33 communications à la VSSE, dont les mises à jour de la liste consolidée 'Syrie' et des fiches de renseignement, une série de rapports basés sur les médias sociaux et une série de données ponctuelles. Le SGRS n'a fourni que sept renseignements, essentiellement des renseignements SIGINT. La VSSE figurait également parmi les destinataires des rapports '*CI-weekly security situation*' rédigés par le SGRS.

Entre novembre 2015 et mars 2016, la VSSE a envoyé 61 notes aux autorités belges (Parquet fédéral, OCAM, Police fédérale, ministre de la Justice, Conseil national de sécurité, OE, CTIF, DG EPI, SGRS), dans lesquelles un ou plusieurs noms de (co-)auteurs étaient mentionné(s). Certaines de ces notes ont été envoyées simultanément à plusieurs services et autorités.

II.4.5.2. Le Service Général du Renseignement et de la Sécurité

Le Comité permanent R a pris connaissance des divers rapports '*CI weekly*', que le SGRS avait rédigés de la mi-novembre 2015 jusqu'au dernier moment précédant les attentats de Bruxelles. Il s'agit d'une publication presque hebdomadaire, classifiée confidentielle, (17 au total pour la période considérée), qui est envoyée à différents destinataires (CHOD, VSSE, OCAM, Police fédérale, Centre de crise et d'autres instances militaires nationales et internationales). La publication a pour but de fournir des informations sur la situation sécuritaire et sur les menaces pesant sur les intérêts militaires, mais cela concerne également, le cas échéant, la sécurité des Belges à l'étranger (qui fait aussi partie des missions du SGRS). Le *CI-weekly* est bien structuré et contient toujours un '*abstract'*, un '*assesment'* et un '*general threat analysis*'.

Le SGRS a publié un *CI weekly* la veille des attentats de Paris le 13 novembre 2015. On pouvait y lire que la participation de la Belgique à la coalition contre l'EI augmentait, il est vrai, les risques de représailles contre notre pays, mais qu'à ce moment-là, aucun élément concret n'indiquait de possibles attaques contre des intérêts militaires en Belgique ou ailleurs. Il y était néanmoins mentionné que la menace contre des intérêts occidentaux – y compris belges – était considérée comme grave. Autre élément important: le SGRS avait mis en garde contre une possible infiltration d'agents de l'EI via le flot de réfugiés provenant

du Moyen-Orient et d'Afrique. Dès avant les attentats de Paris, le SGRS avait pu déduire qu'il y avait des mouvements de combattants de l'EI en Europe. Le service a également partagé cette information avec la VSSE fin octobre 2015.

Le SGRS a aussi partagé des informations opérationnelles avec les autorités belges. Par exemple, le service a transmis à la VSSE des données SIGINT relatives à des personnes qui auraient joué un rôle à Bruxelles. Ce n'est que peu après les attentats de Paris que le SGRS a surtout pu fournir une contribution, mais les informations se sont taries à la mi-janvier 2016.

Juste après l'assaut de Forest, le SGRS est parvenu à réactiver son réseau. Le 18 mars 2016, le SGRS a envoyé une question à ses partenaires internationaux et a reçu la veille des attentats, d'un partenaire SIGINT étranger, des informations sur un des (co-)auteurs. Ces informations n'ont cependant pas pu être diffusées juste avant les attentats de Bruxelles.

Enfin, le SGRS a partagé d'autres informations : le 3 mars 2016, la VSSE a été informée d'une menace potentielle en mars 2016, ainsi qu'entre avril et juin 2016 (certes, essentiellement contre des cibles militaires). Outre dix autres villes européennes, Bruxelles était également citée. Le SGRS avait reçu ces informations d'un de ses partenaires. Le service a fait remarquer qu'il n'avait aucun élément permettant de confirmer ou d'infirmer ces informations, et a émis des doutes sur le *modus operandi* décrit dans le message. Le Comité permanent R estimait pouvoir établir que la communication – si elle contenait ne fût-ce qu'une part de vérité – ne fournissait de toute façon aucune information concrète sur les attentats qui allaient être commis près de trois semaines plus tard à Bruxelles.

II.4.6. LA COLLABORATION AU NIVEAU INTERNATIONAL

II.4.6.1. La Sûreté de l'État

Au cours de la période considérée, la VSSE a reçu plus de 200 communications d'environ 30 correspondants étrangers (*supra*). En complément des constats dressés lors d'une précédente enquête (II.3), le Comité a noté les éléments suivants :

- la VSSE a insisté sur le rôle important des officiers de liaison accrédités en Belgique dans le cadre de l'échange d'informations ;
- la VSSE souhaitait elle-même disposer d'officiers de liaison à l'étranger en vue de rendre l'échange d'informations plus efficace ;
- la collaboration internationale dans le monde du renseignement était en pleine évolution, à la recherche de plus d'efficacité et de rapidité, notamment par la mise en place d'une structure de collaboration permanente au sein du *Counter Terrorism Group* (CTG).

II.4.6.2. Le Service Général du Renseignement et de la Sécurité

Il a déjà été signalé que la plupart des informations dont disposait le SGRS provenaient de sources internationales (par exemple, les informations SIGINT). En ce qui concerne les plateformes internationales dont le SGRS fait partie, le Comité a formulé les remarques suivantes :

- ces plateformes se situent au niveau stratégique et politique, les informations de type opérationnel et tactique n'y sont pas partagées ;
- en mai 2016, le SGRS a réuni plusieurs services homologues étrangers afin d'échanger des informations opérationnelles sur l'EI ;
- entre 2014 et à la mi-2016, environ 200 réunions bilatérales entre le SGRS et les services partenaires étrangers se sont tenues sur le thème de la menace terroriste ;
- à partir de 2015 et jusqu'à la mi-2016, le Chef du SGRS a participé à vingt réunions de travail sur le thème de la menace terroriste.

II.4.7. LES SEMAINES QUI ONT PRECÉDÉ LES ATTENTATS, DU POINT DE VUE DE LA VSSE

Le Comité permanent R a particulièrement examiné les activités de la VSSE juste avant les attentats de Bruxelles (à partir du 1er mars 2016) et a vérifié de quelle manière les autorités en ont été informées.[71]

II.4.7.1. Les listes opérationnelles de targets de la VSSE

Dans ses 'listes opérationnelles de *targets*', la VSSE reprend, par semaine, les objets ou les pistes d'enquête prioritaires et la manière dont on tente de collecter des informations à ce sujet. Il est également indiqué quel service de collecte est concerné et qui est l'analyste responsable du suivi.[72]

Plus de soixante individus figuraient dans la liste du 7 mars 2016. À l'exception d'une personne, tous les futurs (co-)auteurs des attentats étaient repris dans cette liste, ce qui en faisaient des cibles prioritaires. Cette liste reprenait également les sources HUMINT qui devaient encore être recrutées, ainsi qu'une énumération des informations ponctuelles relatives à la menace que la VSSE avait reçues de la part de correspondants étrangers. Ces informations ne

---

71 Le Comité n'avait pas accès aux enquêtes judiciaires en cours à ce moment-là, dans le cadre desquelles la VSSE a été désignée en qualité d'expert (et dans lesquelles le service pouvait éventuellement puiser certaines informations ou certains renseignements).

72 Ces listes – qui, après les attentats de Paris, ont été formalisées comme instrument de travail et affinées – correspondent à d'anciennes recommandations du Comité permanent R, relatives à l'élaboration d'une 'conception globale de collecte et d'analyse' (même si cela doit être adapté dans ce cas-ci au contre-terrorisme).

faisaient pas référence aux faits en passe de se produire à Zaventem et à Maelbeek.

La liste de *targets* du 15 mars 2016 était en grande partie identique à la précédente. Certes, le nombre de menaces qui planaient sur la Belgique était plus élevé, mais le Comité a constaté que ces nouvelles mentions n'avaient rien à voir non plus avec les attentats qui allaient survenir peu après.

II.4.7.2. Les activités menées dans les premières semaines de mars 2016

La meilleure façon de décrire les activités et les points d'attention de la VSSE au cours des dernières semaines précédant les attentats, c'est au travers des réunions au cours desquelles il a été question d'un ou plusieurs (futurs) (co-)auteurs.

Entre le 4 et le 21 mars 2016, la VSSE a participé à au moins neuf réunions, au cours desquelles un ou plusieurs futurs (co-)auteurs des attentats de Bruxelles ont été mentionnés. Sept réunions ont eu lieu en présence de partenaires étrangers. Les attentats de Paris et ce qui les a précédés, étaient au centre des discussions. Les services ont cherché à reconstituer la préparation de l'attentat de Paris. Les (co-)auteurs étaient toujours considérés comme 'dangereux' et comme étant en mesure de planifier ou de commettre d'autres attentats. Il n'y avait cependant aucun élément indiquant une menace concrète et/ou imminente qui aurait visé spécifiquement la Belgique.

L'assaut des unités spéciales dans l'appartement de Forest, le 15 mars, était un moment important. Et pour cause, les personnes suspectées de terrorisme (il s'est finalement avéré qu'il ne s'agissait que de quelques-unes) ont été délogées de leurs planques. Après l'assaut, les réunions se sont succédé. La VSSE tentait toujours, avec deux services partenaires, de découvrir les détails du voyage qu'avait entrepris Salah Abdeslam à l'automne 2015, et au cours duquel il avait convoyé plusieurs personnes à Bruxelles (une d'entre elles a en effet été tuée à Forest). Une réunion s'est tenue le même jour avec le Parquet fédéral et la Police fédérale, réunion lors de laquelle les événements ont été discutés, et des pistes possibles ont été examinées.

Les 17 et 18 mars 2016, des réunions portant sur la personne qui avait été tuée à Forest ont eu lieu, notamment avec un service d'Europe du Nord. Cette personne a pu être identifiée (Belkaïd).

Outre les réunions au cours desquelles des données ont été échangées, des informations écrites l'ont également été avec des services belges. Ces échanges ont surtout fourni des informations ponctuelles et opérationnelles sur, entre autres, les éventuelles allées et venues d'Abdeslam.

II.4.7.3. L'assaut de Forest et l'arrestation d'Abdeslam à Molenbeek

L'assaut de Forest, le 15 mars 2016, a constitué un tournant. Belkaid a été tué et deux autres individus ont pris la fuite, à savoir Salah Abdeslam et l'homme qui

utilisait le nom 'Amine Choukri' (identifié par la suite comme étant Ayari). La VSSE a établi une note détaillée sur l'assaut de Forest pour le ministre de la Justice, esquissant l'état de la question et indiquant les pistes qu'elle avait suivies.

Après l'assaut de Forest et l'arrestation d'Abdeslam à Molenbeek, le Conseil national de sécurité a organisé des réunions d'urgence.

Le 21 mars 2016 au soir – la veille des attentats – une note a été adressée au ministre de la Justice. Plusieurs pistes d'enquête, dans la foulée de l'arrestation de Salah Abdeslam, y étaient développées. Le Comité a noté que :

- aucun indice qui aurait signalé des attentats imminents à Zaventem ou à Maelbeek n'a été trouvé lors de l'assaut de Forest ;
- la VSSE n'était pas au courant d'éventuelles opérations de reconnaissance effectuées par les auteurs potentiels, à Bruxelles ou ailleurs, en vue des attentats (comme cela s'est passé précédemment à Paris et ensuite à Nice)[73] ;
- peu après les faits survenus à Forest, la VSSE a pu consulter une fiche attribuée à l'EI (dans laquelle figuraient des détails – notamment *'suicide bomber'* – à propos de Belkaid). Le document faisait partie d'une série de documents similaires qui ont fait surface début mars 2016. La question de savoir où l'intéressé voulait vraiment se faire exploser – si les informations sur la fiche étaient correctes – demeure sans réponse.
- Abdeslam est resté muet dans les jours qui ont suivi son arrestation.

II.4.7.4. Des informations opérationnelles en priorité

Les informations échangées, tant au niveau national qu'au niveau international, étaient surtout des informations opérationnelles. Il en va de même pour les notes que la VSSE a rédigées et envoyées aux autorités : il s'agissait notamment de faits, et de pistes d'enquête. Le Comité n'a pas trouvé de notes reprenant des analyses plus développées ou des hypothèses/scénarios élaboré(e)s formellement sur la manière dont les événements devaient être interprétés ou ce qui pourrait s'ensuivre, et/ou des notes qui avertiraient les autorités de menaces imminentes. Interrogée à ce sujet, la VSSE a déclaré que ce genre de questions et de préoccupations étaient permanentes. Le Comité permanent R estimait qu'après Forest/Molenbeek, la VSSE avait été absorbée par le travail opérationnel. Le Comité a rappelé l'importance d'une hypothèse/d'un scénario formel(le) et de renseignements 'prédictifs'. Il convient évidemment de disposer d'effectifs suffisants, d'allouer les moyens nécessaires, d'établir une méthodologie et d'échanger des informations. Et le Comité d'insister sur le fait que d'autres services ont un rôle à jouer à cet égard, en particulier à l'OCAM, dont la tâche est de rédiger des évaluations de la menace et des analyses stratégiques.

---

[73] Comme cela a déjà mentionné au point II.4.3.3, les observations de l'OVG n'ont pas été partagées avec la VSSE.

II.4.8. CONCLUSIONS

Comme c'était le cas pour les attentats de Paris en novembre 2015, les activités des services de renseignement n'ont pas permis de détecter à temps les projets d'attentats qui ont été perpétrés à Zaventem et à Bruxelles. L'examen des informations collectées n'a pas non plus permis de constater que les services précités disposaient d'informations qui auraient permis d'éviter ces attentats.

Le Comité permanent R n'a pas décelé de dysfonctionnements dans la manière dont la VSSE, qui est le service de renseignement explicitement désigné dans la loi pour lutter contre le terrorisme, a accompli ses missions avant la commission de ces attentats. Plusieurs des (co-)auteurs impliqués étaient connus depuis les attentats de Paris et faisaient partie des *targets* prioritaires de la VSSE, mais ils ont pu échapper pendant plus de quatre mois à la vigilance de ce service, tout comme à la vigilance du SGRS, des services de renseignement étrangers et des services de police. La VSSE a utilisé les moyens disponibles (HUMINT, SOCMINT, MRD) et a adapté son fonctionnement dans les mois qui ont précédé les attentats, mais peu d'informations utiles en ont découlé. Le même constat peut être dressé en ce qui concerne les informations recueillies via les canaux internationaux et les nombreuses réunions organisées avec des services partenaires avant le 22 mars 2016. En résumé, malgré des efforts soutenus, la position d'information de la VSSE n'était, dans le cas présent, pas suffisamment solide pour contrer la menace. Cela n'enlève rien aux mérites ni à la contribution concrète qui a été fournie dans l'identification ultérieure et la mise sous les verrous des membres du réseau terroriste.

Selon le Comité, la position d'information des services de renseignement pouvait être renforcée, en particulier au niveau du travail avec les informateurs et par un meilleur accès aux canaux de communication des terroristes (potentiels).

En ce qui concerne le SGRS, on a pu constater que le service avait tenté d'activer ses sources HUMINT et SIGINT après les attentats de Paris afin d'en savoir plus sur ses auteurs. Cela a donné certains résultats, en termes de compréhension du fonctionnement de l'EI et de l'interconnectivité entre *targets*, mais n'a pas fourni de données pertinentes sur une menace concrète en Belgique. Le service n'a toutefois pas employé de MRD ni de SOCMINT à l'égard de quatre des (co-)auteurs connus du service, ni à l'égard d'autres (co-)auteurs. En raison de l'utilisation très limitée de ses propres moyens de collecte, le SGRS ne disposait que de très peu d'informations et, partant, d'une mauvaise position d'information sur la menace en Belgique. Le Comité permanent R a constaté, dans son enquête, que le flux d'informations émanant de l'opération OVG (*Operation Vigilant Guardian*) aurait certainement pu être meilleur. Dans le cadre de cette opération, des détachements militaires déployés sur le territoire belge ont fourni des éléments d'information, qui ont ensuite été portés à la connaissance des services de police qu'appuyaient ces détachements. Le Comité permanent R n'a pas vérifié

la suite donnée par les services de police, mais a constaté que les mêmes informations étaient arrivées simultanément au SGRS, via la chaîne de commandement militaire, informations que le service n'avait pas traitées. Le Comité estime que cela aurait dû être le cas, certainement dans le cadre de la mission incombant au SGRS, qui est de fournir tous les renseignements utiles aux militaires déployés (le concept de *force protection*). On peut néanmoins signaler que le SGRS a mis une partie de sa capacité CI au service de la VSSE, ce qui illustre parfaitement la bonne coopération de ces services.

Le Comité a constaté que l'échange de données entre services compétents, tant au niveau national qu'au niveau international, a, de manière générale, fortement progressé depuis les attentats de Paris. Mais cet échange restait, somme toute, assez limité en chiffres nominaux et, comme l'ont montré des enquêtes précédentes, il devait encore être amélioré. Le Comité a pu constater que la coopération, surtout entre services de renseignement européens, avait pris une nouvelle dimension dans le courant de l'année 2016. L'échange devait être encore approfondi au niveau belge et international pour renforcer la position d'information.

Le rapport du Comité permanent R à propos de l'enquête sur les attentats de Paris a montré que juste avant ces attentats, le SGRS avait sérieusement averti ses contacts belges et étrangers des projets de l'EI à l'encontre de cibles européennes. Ces informations n'étaient, il est vrai, pas suffisamment concrètes pour pouvoir mener une contre-attaque ciblée. Avant les attentats de Bruxelles, aucun nouvel élément inquiétant de ce genre n'a été découvert. Dans ses bulletins hebdomadaires, le SGRS ne pouvait donc que signaler la menace générale visant des cibles en Europe.

Les deux services étaient activement impliqués dans la concertation au sein du Conseil national de sécurité. Des briefings ont été donnés par les services dans ce cadre, et des informations ont été communiquées. En ce qui concerne la VSSE, il s'est avéré que les renseignements que le service envoyait aux autorités belges étaient surtout ponctuels ; il ne s'estimait pas en mesure de réaliser des analyses plus générales. Le Comité permanent R a néanmoins rappelé que l'essence même d'un service de renseignement est de préparer des renseignements prédictifs et stratégiques à l'intention des autorités.

Le Comité permanent R a déjà constaté à maintes reprises que lorsque les services de renseignement sont désignés comme experts judiciaires pour les Parquets, la logique judiciaire risque de 'phagocyter' la logique de renseignement, alors que justement, un équilibre est nécessaire entre l'action judiciaire et l'action administrative. Aussi convient-il effectivement de veiller à ce que les autorités administratives guident au mieux les services de renseignement pour que ceux-ci n'engagent pas leurs capacités limitées dans des missions purement judiciaires, telles que la collecte de preuves. C'est la raison pour laquelle le Comité estime que le risque de 'judiciairisation' des services de renseignement est un point d'attention important.

Pour le reste, le Comité permanent R a fait référence aux différents points d'attention et d'amélioration repris dans le rapport final établi dans le cadre de l'enquête de contrôle sur les attentats de Paris (voir II.2.4).

II.5. LA PROTECTION DU POTENTIEL ÉCONOMIQUE ET SCIENTIFIQUE ET LES RÉVÉLATIONS D'EDWARD SNOWDEN

II.5.1. INTRODUCTION

Le 6 juin 2013, *The Guardian*[74] et *The Washington Post*[75] publiaient pour la première fois des informations issues des dizaines de milliers de documents (classifiés) divulgués par Edward Snowden, qui a rempli diverses fonctions dans ou pour des services de renseignement américains. À compter de ce moment-là, les révélations se sont succédé.

Les informations donnaient un aperçu des programmes secrets, principalement de la *National Security Agency* (NSA) américaine et du *General Communication Headquarters* (GCHQ) britannique. Elles révélaient notamment l'existence du programme PRISM, au travers duquel la NSA récoltait massivement des données et métadonnées de télécommunications, et dévoilaient que les services américains, mais aussi britanniques, avaient monté des opérations de renseignement visant certaines institutions internationales et structures de coopération (ONU, UE et G20), et où des 'pays amis' étaient également ciblés.

Ces révélations ont constitué le point de départ de nombreuses enquêtes parlementaires, judiciaires et de renseignement à travers le monde, y compris en Belgique. Le 1er juillet 2013, la Commission de suivi du Sénat a demandé au Comité permanent R *« […] een update van de bestaande informatie over de praktijken op het vlak van datamining. Niet alleen de Amerikaanse inlichtingendienst NSA zou dit doen, maar ook het Verenigd Koninkrijk zou massaal gegevens onderscheppen en analyseren. In de tweede plaats wil de begeleidingscommissie dat het Comité I onderzoekt welke de gevolgen zijn voor de bescherming van het economisch en wetenschappelijk potentieel van ons land, en van de wettelijke opdrachten van onze inlichtingendiensten. Ten slotte wenst de begeleidingscommissie dat het Comité I onderzoekt hoe dergelijke praktijken worden getoetst aan de nationale en internationale rechtsregels die de privacy van burgers beschermen »*.[76]

---

74 G. GREENWALD et E. MACASKILL, *The Guardian*, 6 juin 2013 (NSA Taps in to Internet Giant's Systems to Mine User Data, Secret files Reveals).

75 B. GELLMAN et L. POITRAS, *The Washington Post*, 6 juin 2013 (US Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program).

76 *« Une mise à jour des informations existantes sur les pratiques en matière de datamining* [exploration de données]. *Le service de renseignement américain ne serait pas le seul à le*

Le Comité permanent R a alors ouvert plusieurs enquêtes de contrôle, qui étaient étroitement liées.[77] Trois d'entre elles ont été bouclées en 2014.[78]

La dernière enquête de contrôle[79], qui fait l'objet du présent rapport, traite des implications éventuelles des programmes étrangers précités pour la protection du potentiel économique et scientifique du pays.[80] Par cette enquête, le Comité entendait vérifier si les services de renseignement belges :

- s'étaient intéressés à ce phénomène ;
- avaient détecté une menace réelle ou éventuelle sur le potentiel économique et scientifique belge ;
- en avaient informé les autorités compétentes et avaient proposé des mesures de protection ; et
- disposaient de moyens suffisants et adéquats pour suivre cette problématique.

Par ailleurs, toujours à la demande de la Commission de suivi, les conséquences du programme PRISM et/ou d'autres systèmes analogues sur le potentiel économique et scientifique du pays ont été examinées. Le rapport a été clôturé début 2016.[81]

---

pratiquer, la Grande-Bretagne intercepterait et analyserait aussi massivement des données. En second lieu, la commission de suivi veut que le Comité examine quelles sont les conséquences pour la protection du potentiel économique et scientifique de notre pays, une des missions légales de nos services de renseignement. Enfin, la commission de suivi souhaite que le Comité R étudie comment de telles pratiques sont évaluées au regard des règles de droit nationales et internationales qui protègent la vie privée des citoyens » (traduction libre).

77 Une autre enquête a été initiée à la suite d'une plainte introduite par le président de l'Ordre néerlandais des Avocats du Barreau du Bruxelles ('Enquête contrôle suite à une plainte d'un bâtonnier sur l'utilisation d'informations issues de récolte massive de méta-data d'origine étranger dans des affaires pénales belges'). Voir à ce propos COMITÉ PERMANENT R, *Rapport d'activités 2014*, 38-43 (Chapitre II.3 'L'utilisation dans des affaires pénales d'informations issues d'une captation massive de données par des services étrangers').

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

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

80 Par exemple, Edward Snowden affirmait que l'Union européenne était une cible prioritaire de la NSA et du GCHQ britannique, surtout sur les sujets de politique étrangère, de commerce international et de stabilité économique. *'That a major goal of the US Intelligence Community is to produce economic intelligence is the worst kept secret in Washington.'* (http://www.europarl.europa.eu:document/activites/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf).

81 Les actes d'enquête ont été interrompus à diverses reprises en raison du plus haut degré d'urgence d'autres enquêtes de contrôle qui ont été confiées au Comité permanent R.
La version classifiée 'CONFIDENTIEL (Loi 11.12.1998)' du rapport final a été envoyée aux ministres compétents le 11 février 2016.

II.5.2. CONSTATATIONS

II.5.2.1. Systèmes de communications-interceptions massives et le PES

Le Comité permanent R a pu constater que la réalité des programmes d'interceptions de communications et de données pratiquées par les services de renseignement américains et britanniques avait été démontrée à suffisance par les révélations d'Edward Snowden. Ces interceptions étaient à la fois massives et ciblées. Les explications fournies par les gouvernements des pays concernés invoquaient toutefois la légitimité des objectifs poursuivis au regard de leur droit national, à savoir la lutte contre le terrorisme, le crime organisé et la corruption, mais ils niaient toute intention d'espionnage économique ou de collecte d'informations au bénéfice de leurs entreprises.

À l'issue de son enquête de contrôle, le Comité permanent R n'a pas eu connaissance de cas d'espionnage avérés d'entreprises belges ou d'organismes scientifiques belges par le biais de systèmes d'interception massive de communications, comme le programme PRISM de la NSA.

Il existe néanmoins de fortes présomptions permettant d'affirmer que des entreprises étrangères, tant en Europe qu'ailleurs dans le monde, ont fait l'objet d'interceptions de la part des services des pays susnommés. On peut tirer la même conclusion concernant l'espionnage visant des personnalités politiques de premier plan (cf. le '*Merkelgate*'[82]), ainsi que des pouvoirs publics et organismes internationaux tels que les institutions européennes en charge de la politique économique et financière. Les éléments susmentionnés étaient suffisamment cohérents et documentés pour attribuer le *hacking*[83] constaté chez Belgacom/BICS à ces mêmes services.

Le Comité affirmait pouvoir partir du principe que des entreprises, établissements scientifiques et autorités politiques belges, responsables de la politique financière et économique du pays, pouvaient faire l'objet d'espionnage économique. Peu importe ici que les techniques d'espionnage utilisées soient ciblées ou non, surtout lorsqu'elles sont mises en œuvre par des pays qui ne peuvent pas exactement être qualifiés d'alliés.[84]

Malgré l'émotion suscitée par les révélations d'Edward Snowden, force est de constater que, loin d'avoir mis un terme à leurs programmes d'interceptions, les

---

82 Edward SNOWDEN a révélé que la NSA avait mis sur écoute les entretiens téléphoniques de la Chancelière allemande, Angela Merkel.

83 À la mi-septembre 2013, l'opérateur de téléphonie BELGACOM a publié un communiqué de presse indiquant que des traces d'une intrusion digitale dans le système informatique interne de l'entreprise avaient été découvertes à l'occasion d'un contrôle de sécurité. Une plainte a alors été déposée auprès du Parquet fédéral (www.belgacom.com/be-fr/newsdetail/ND). Il s'agirait d'une affaire d'espionnage cybernétique visant les communications téléphoniques internationales gérées par la société Belgacom International Carrier Services (BICS).

84 Pour être complet, il ne faut pas non plus négliger l'espionnage industriel et concurrentiel entre acteurs privés, même si ce sujet ne fait pas l'objet de la présente enquête.

États concernés les ont, tout au plus, mieux étayées sur le plan juridique. Rien n'indique donc que les interceptions de communications ou que le (cyber) espionnage diminueront à l'avenir, bien au contraire. On peut même raisonnablement douter que des conventions politiques ou de droit international puissent apporter des solutions ou des garanties, au vu du caractère intrinsèquement secret de ces activités d'espionnage. Il convient dès lors de concentrer les efforts sur une amélioration de la protection des systèmes de communication et d'ICT.

Toujours en raison du caractère secret des opérations d'interception, qui fait que très peu d'informations sont disponibles sur l'ampleur de l'espionnage de nature économique et encore moins sur l'usage final ou l'impact des renseignements collectés, il est illusoire de pouvoir donner une estimation brute des dommages consécutifs à l'usage de ces systèmes d'espionnage sur le potentiel économique et scientifique belge. Ces dommages n'apparaissent souvent que de manière exceptionnelle ou indirecte, comme dans le cas du *hacking* de BELGACOM/BICS. Ce cas concret prouve que les dommages peuvent être considérables.

II.5.2.2. Le rôle des services de renseignement belges et de l'OCAM

Comme l'ont montré les enquêtes antérieures[85] du Comité permanent R, les services de renseignement belges ne sont pratiquement pas intervenus dans cette problématique, ni de manière préventive ni en prêtant leur concours aux opérations de ces services étrangers.

En ce qui concerne spécifiquement le potentiel économique et scientifique, les services ont fait preuve de peu d'initiative pour le protéger contre la menace d'interceptions (massives ou non), alors qu'ils étaient ou auraient dû être informés des risques, surtout après les révélations antérieures concernant le réseau ECHELON et l'affaire SWIFT.

Force a été de constater qu'aucune analyse de phénomène n'a jamais été faite dans cette matière, pas même après les révélations concernant les interceptions massives et leurs conséquences pour la Belgique ou pour son potentiel économique et scientifique.

D'autre part, les services de renseignement belges n'ont pas non plus été sollicités sur cette problématique, après les révélations, par les secteurs économiques ou par les autorités, excepté dans ce dernier cas sur leur éventuelle complicité dans le *hacking* de BELGACOM/BICS.

La présente enquête a également mis en évidence l'insuffisance et l'inadéquation du cadre légal qui était en vigueur à ce moment-là face aux

---

85 Voir par exemple 'L'affaire SWIFT', dans COMITÉ PERMANENT R, *Rapport d'activités 2006*, 39-48 ou 'ECHELON', dans COMITÉ PERMANENT R, *Rapport complémentaire d'activités 1999*, 11-55.

menaces complexes pesant sur les infrastructures critiques.[86] Or, l'inventaire de l'infrastructure critique n'a pas encore été dressé pour le secteur des communications électroniques dans le cadre de la loi relative à la protection des infrastructures critiques[87] et qui attribue un rôle à l'OCAM (ainsi qu'à ses services d'appui et au Centre de crise).

Alors qu'une analyse de risques en la matière devrait être une analyse *'all risk'*, les missions (et donc l'expertise) de l'OCAM sont limitées à l'extrémisme et au terrorisme. En outre, au sens de la Loi du 1er juillet 2011, l'infrastructure est une « *installation, un système ou une partie de celui-ci, d'intérêt fédéral, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, et dont l'interruption du fonctionnement ou la destruction aurait une incidence significative du fait de la défaillance de ces fonctions* » ; tout le monde ne s'accordait pas à dire que l'espionnage ou le cyberespionnage constituent des risques de cette nature. Le Comité permanent R estimait pourtant que la probabilité d'interceptions ou de *hacking* représente une menace pour l'intégrité des systèmes de communication critiques, qu'il intervienne pour des raisons d'espionnage ou pour d'autres raisons, plus destructives.

Une fois encore, il convient de souligner que l'exercice des missions des services de renseignement, et en particulier de la VSSE, concernant la protection du PES, s'avère ardu dans la pratique. Cette difficulté était déjà apparue lorsque la compétence légale a dû être opérationnalisée, et il aura fallu attendre un certain temps avant que le PES soit défini.[88]

Selon le Comité, ceci s'explique probablement par un manque de compréhension de la contribution qu'un service de renseignement peut apporter aux partenaires concernés. Il en résulte une incapacité des différents pouvoirs publics (fédéraux mais aussi régionaux) en charge de la politique économique et financière de définir leurs attentes en la matière, d'où un manque d'analyses et une méconnaissance des phénomènes par les secteurs à protéger. De plus, les interventions des services de renseignement en matière de protection du PES sont souvent perçues de manière négative lorsqu'ils rendent, par exemple, des avis négatifs pour l'exportation de certaines denrées à l'étranger ou pour l'acceptation d'investissements étrangers dans certains secteurs de l'économie. Toutefois, protéger le PES n'est pas seulement une question de coûts et de limitations, mais aussi et surtout d'opportunités de croissance économique. Mais il manque surtout un point de contact entre les services de renseignement et les acteurs publics et privés du potentiel économique et scientifique.

---

86 Cette législation pourrait être rendue plus opérationnelle si les infrastructures critiques du secteur des télécommunications en Belgique étaient désignées par l'autorité sectorielle compétente en la matière. L'exploitant de l'infrastructure pourrait alors être légalement tenu d'assurer une protection d'un niveau adéquat.

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

88 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 130.

Le Comité permanent R fait par ailleurs référence au plan d'action de la VSSE qui, au moment de la rédaction du rapport, accordait la priorité à la protection du PES, mais dont les résultats n'avaient pas encore pu être vérifiés. Le SGRS disait vouloir lui aussi s'investir davantage dans cette matière. Par ailleurs, des groupes de travail s'attelaient, sous l'égide du Conseil national de sécurité, à améliorer la protection du PES d'une part, et de la cybersécurité d'autre part. L'opérationnalisation du Centre pour la cybersécurité constitue en tout cas, aux yeux du Comité permanent R, un tournant extrêmement prometteur à cet égard.

II.6. LA VSSE ET LE PROTOCOLE DE COOPÉRATION AVEC LES ÉTABLISSEMENTS PÉNITENTIAIRES

Le 1er octobre 2014, une enquête de contrôle a été ouverte sur la manière dont la VSSE met en application le « protocole d'accord réglant la coopération entre la Sûreté de l'État et la Direction générale Exécution des Peines et des Mesures (DGEPM) ».[89] Cet accord a été conclu le 20 novembre 2006 dans le cadre du Plan Radicalisme, qui avait été approuvé le 28 avril 2006 par le Comité ministériel du renseignement et de la sécurité de l'époque. Cet accord de coopération a été conclu (surtout) à la demande de la VSSE, qui, au début des années 2000, avait prôné à plusieurs reprises un meilleur échange d'informations avec les prisons. Par exemple, en 2001, « *le prosélytisme de certaines organisations islamistes dans les prisons* » était une source de préoccupation pour la VSSE. Le service déplorait que « *l'administration pénitentiaire n'avait pas encore pris le pli de lui communiquer de manière spontanée des informations sur ce problème* ».[90]

L'objectif de l'enquête était d'examiner si le Protocole de coopération entre la VSSE et la DG EPI était appliqué de manière efficace, si la VSSE en retirait des informations utiles à ses missions et, accessoirement, de vérifier si l'échange de données sur les détenus visés par cet accord se déroulait conformément aux droits que la Constitution et les lois confèrent aux personnes.[91] La présente enquête de contrôle découle directement de deux enquêtes clôturées précédemment.[92]

---

89 La DGEPM a changé de nom pour devenir la Direction générale des Établissements Pénitentiaires (DG EPI). Le Comité permanent R avait appelé à une application rigoureuse de ce Protocole d'accord entre la VSSE et la DG EPI, voir COMITÉ PERMANENT R, *Rapport d'activités 2012*, 99.

90 COMITÉ PERMANENT R, *Rapport d'activités 2001*, 95.

91 L'enquête a été clôturée à la mi-mars 2016.

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

II.6.1. ÉCHANGE D'INFORMATIONS AVEC L'ADMINISTRATION PÉNITENTIAIRE

L'article 13 L.R&S dispose que les services de renseignement et de sécurité peuvent, dans le cadre de leurs missions, rechercher, collecter, recevoir et traiter des informations et des données à caractère personnel qui peuvent être utiles à l'exécution de ces missions. L'administration pénitentiaire constitue à cet égard une source d'informations notable. La compétence des membres de cette administration à transmettre des informations à la Sûreté de l'État est inscrite à l'article 14 L.R&S : les fonctionnaires et agents des services publics peuvent, « *sur la base des accords éventuellement conclus ainsi que des modalités déterminées par leurs autorités compétentes* », communiquer des renseignements aux services de renseignement de leur propre initiative ou à la demande de ces derniers.

Le dernier alinéa de l'article 14 L.R&S, qui a été inséré en 2010, stipule que la VSSE « *[peut] avoir accès aux banques de données du secteur public utiles à l'exécution de leurs missions* ». Dans ce cadre, il convient de souligner que la VSSE a directement accès à SIDIS Suite, la base de données du greffe de la DG EPI.

En marge de la collecte d'informations, la VSSE doit, conformément à l'article 20 § 1er L.R&S, veiller à assurer la coopération mutuelle la plus efficace possible avec, entre autres, les autorités administratives. La VSSE peut également, par le biais de protocoles d'accord, collaborer avec ces mêmes autorités et leur prêter une assistance technique (article 20 § 2 L.R&S).

II.6.2. L'APPLICATION DU PROTOCOLE AU FIL DES ANS

La finalité de l'accord conclu était de « *faciliter l'échange d'informations et de l'encourager, de définir les règles pratiques de la collaboration, d'intensifier l'échange d'idées et les analyses ou, en d'autres termes, d'axer davantage sur la pratique la collaboration concernant les missions et activités des services susmentionnés* ».

Le Comité permanent R a pu constater que la mise en œuvre du Protocole d'accord a pris beaucoup de temps. Deux périodes se distinguent : d'une part, entre 2006 et la mi-2014 (où les mécanismes définis dans le Protocole d'accord aux fins de la collaboration et de l'échange d'informations n'ont été appliqués que dans une certaine mesure) et d'autre part, à partir de la mi-2014 (où l'échange d'informations entre la VSSE et les établissements pénitentiaires s'est accéléré, sans qu'il y ait forcément un lien avec les mécanismes du Protocole d'accord).

Le Comité permanent R a dû constater que la manière dont le Protocole a été mis en œuvre sur le terrain jusqu'à la mi-2014 contraste nettement avec l'importance que le service lui avait accordée avant son élaboration, mais aussi par la suite. Ainsi, il est apparu que le nombre de documents échangés sur le terrorisme ou sur des détenus radicalisés pendant la période 2006-2014 était

limité.[93] Cependant, la quantité de renseignements échangés aurait augmenté au fil des ans. Mais la majorité des échanges d'informations reposait sur des contacts personnels/informels. Le Protocole d'accord aurait été, à cet égard, un élément facilitateur, en ce sens que les membres du personnel de l'administration pénitentiaire (par exemple les directeurs de prison) faisaient preuve de moins de réserve dans leurs contacts avec les membres de la VSSE, car ils se savaient couverts sur les plans juridique et administratif par le Protocole d'accord.[94] Pourtant, pendant cette période, les listes de détenus radicaux et de personnes liées au terrorisme prévues par le Protocole n'ont jamais été établies. Il aura fallu attendre jusqu'à la mi-2014.

Le fait que, dans les premières années, le Protocole n'ait pas véritablement été utilisé comme instrument pour la collecte d'informations pouvait éventuellement s'expliquer par la manière dont la VSSE percevait la menace.[95] Au cours des années suivantes, la problématique semble avoir gagné en importance. Dans les Plans d'action de 2011, 2012 et 2013, 'l'extrémisme – le terrorisme – l'islamisme (dans) les prisons' a fait l'objet d'un 'suivi prioritaire actif'.

Le Comité permanent R a considéré que l'amélioration de l'échange d'informations et de la collaboration entre la VSSE et la DG EPI trouvait sa véritable origine dans les éléments suivants : d'une part, à partir de 2012-2013, nombre d'individus partis combattre en Syrie (ou de candidats au départ) et de recruteurs ont été incarcérés et, d'autre part, la nouvelle direction de la VSSE a particulièrement mis l'accent sur l'échange d'informations en général, et sur l'échange d'informations avec les établissements pénitentiaires en particulier.

II.6.3. UNE ÉVALUATION PONCTUELLE DU PROTOCOLE : CONSTATATIONS

Dans le cadre de son enquête, le Comité a pu dresser les constats repris ci-après :

– si le Protocole mettait avant tout l'accent sur la radicalisation et le terrorisme, il est apparu que des informations étaient également échangées sur d'autres phénomènes tels que les organisations sectaires nuisibles, l'ingérence, l'anarchisme, l'extrême droite et l'extrême gauche[96] ;

---

93 La VSSE prétend qu'aucun chiffre n'a pu être fourni.

94 En outre, le fait qu'en 2006, la VSSE ait confié le suivi de la question à une personne disposant de solides connaissances pratiques en la matière, a réduit le fossé entre les deux administrations. Cette personne a rempli de manière plutôt pragmatique les obligations découlant du Protocole d'accord, ce qui a notamment permis d'accroître l'échange d'informations, même de manière informelle.

95 Dans son 'Analyse des phénomènes islamistes-extrémistes' de 2009, le service consacre un chapitre à l'extrémisme dans les prisons. Le service en conclut que « *les activités prosélytes islamiques-extrémistes dans les prisons belges semblent pour l'instant plutôt limitées* ».

96 Vu que la plupart des contacts étaient informels, il n'a pas été possible de communiquer des chiffres à ce propos.

- il était stipulé dans le Protocole que les deux parties utiliseraient des listes : la VSSE, une liste d'éléments radicaux et une liste de personnes liées au terrorisme ; la DG EPI, une liste de détenus condamnés pour terrorisme. La DG EPI mettait le 'Registre Terrorisme EPI' à la disposition de la VSSE.[97] La VSSE n'a quant à elle établi aucune liste. Le service ne l'estimait ni pratique, ni souhaitable. Pour remplir sa part du contrat, la VSSE a choisi, depuis août 2014, de travailler avec des fiches pour tout détenu dont le nom figurait dans le 'Registre Terrorisme EPI'. Cette fiche reprenait des informations pertinentes pour l'administration pénitentiaire : le risque d'évasion, le risque de radicalisation de tiers, les antécédents dans le domaine de l'usage d'armes… Ces fiches étaient remises aux directeurs de prison concernés, qui prenaient ensuite les mesures nécessaires ;
- la DG EPI, qui pouvait demander un complément d'informations à la VSSE, recourait de plus en plus à cette possibilité, surtout depuis l'éclatement de la crise en Syrie, qui a donné lieu à une augmentation du nombre de détenus liés au terrorisme ;
- il importait de constater que la VSSE avait activé son accès à la base de données.[98] Auparavant, le VSSE utilisait des ordinateurs spécialement dédiés à cet effet et des codes d'accès distincts, mais en 2016, un accès global a donné. La base de données SIDIS a subi un profond remaniement en septembre 2014 ; le nouveau système (SIDIS Suite) a été étendu à toute une série de données (comme les visiteurs, les numéros de téléphone…) ;
- la VSSE et la DG EPI, dans le cadre du Plan Radicalisme et de la liste JIB qui en découle, participaient toutes deux à certaines réunions de travail, où des informations étaient également échangées. Les deux formes d'échange d'informations coexistaient. La liste du 'Registre Terrorisme EPI' (concernant les détenus condamnés pour terrorisme) et la liste Plan R/JIB (énumération d'éléments 'radicalisants') étaient des listes bien distinctes, ayant chacune une finalité différente ;
- le Comité permanent R a en outre remarqué qu'une pratique s'était développée en dehors du Protocole, c'est-à-dire que des informations étaient directement échangées avec la prison concernée, et non avec le *point of contact* (POC) au niveau national. Le Comité permanent R en a souligné le

97 Cette liste a été discutée pour la première fois en février 2014 au sein du Groupe de travail Prisons (Plan R). Elle a ensuite été diffusée et régulièrement mise à jour.

98 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 oblige un service à obtenir l'autorisation préalable du Comité sectoriel pour l'autorité fédérale pour « *toute communication électronique de données personnelles par un service public fédéral* ». Le Comité a constaté qu'une telle autorisation n'avait pas été demandée dans ce cas-ci. Le Comité estimait que cette demande n'était pas sans importance, étant donné que la Commission vie privée dans son avis 08/2016 du 24 février 2016 établissait que SIDIS/SIDIS Suite « *ne réussit pas le test de la LVP* ». En 2013 déjà, la Commission vie privée sommait l'administration concernée d'« *établir une base légale pour cette banque de données* ».

danger : dans la mesure où, par exemple, cet échange ne fait pas l'objet d'un rapport formel ni d'un procès-verbal – et ne vient donc pas alimenter la base de données centrale de la VSSE (VESTA) – le POC pourrait perdre la vue d'ensemble ;
- selon la VSSE, la DG EPI signalait de plus en plus de personnes présentant des signes de radicalisation, ce qui pouvait éventuellement s'expliquer par la formation (dispensée par la VSSE) sur la radicalisation au sein de l'administration pénitentiaire. Toutefois, la VSSE elle-même remarquait que l'actualité et l'attention répétée des médias avaient également accru la vigilance dans le chef du personnel pénitentiaire ;
- dans le Protocole, on a tenté de distinguer le terrorisme et le radicalisme, mais cette distinction était artificielle. Il aurait dû être question de deux régimes distincts, alors qu'en réalité, l'approche différait peu dans la pratique ;
- le Comité permanent R a attiré l'attention sur deux évolutions qui avaient toute leur importance au moment de l'enquête. D'une part, la VSSE et la DG EPI ont dû accorder une attention accrue au phénomène de l'anarchisme. En effet, un mouvement particulier s'est révélé très actif dans l'approche de détenus et dans la lutte contre l'existence des prisons. Des informations relatives aux 'sympathisants' du mouvement anarchiste en question étaient régulièrement échangées depuis quelques années. Tant pour la DG EPI que pour la VSSE, l'échange de données est une source d'informations pertinentes. D'autre part, il a été constaté que des groupements islamistes extrémistes ne tentaient pas d'influencer les détenus musulmans par le biais de visites, mais plutôt par la correspondance ;
- la VSSE a indiqué que la DG EPI mentionnait de plus en plus souvent des signes flagrants de radicalisation parmi les détenus. Mais aucun chiffre n'était disponible ici non plus ;
- la VSSE était très satisfaite du respect de la réglementation en matière d'informations classifiées. La DG EPI n'a pas non plus observé d'infractions concernant les pièces classifiées ;
- le Protocole d'accord insistait également, comme souligné précédemment, sur l'importance de la formation des fonctionnaires pénitentiaires.[99] Le Comité a toutefois constaté que cet aspect n'avait été pris au sérieux qu'en 2011. C'est alors qu'une formation avait été organisée à l'intention des directeurs, des membres du Service psychosocial et de quelques fonctionnaires pénitentiaires. Cette formation était axée sur l'identification du radicalisme. Les personnes formées allaient ensuite être en mesure de dispenser à leur tour des formations au sein des établissements pénitentiaires.

[99] Il a notamment été envisagé d'intégrer la formation dans la formation COPPRA (*Community Policing and Prevention of Radicalisation*), d'apporter son concours au projet de déradicalisation de l'OCAM (*Internal Security Fund* - 'ISF'), et de créer, pour les fonctionnaires pénitentiaires, un outil en ligne qui leur permettrait d'acquérir certaines aptitudes par auto-apprentissage. Mais ces pistes n'en sont qu'à un stade précoce et ne sont pas encore très concrètes.

Mais cette procédure n'a pas produit ses pleins effets, notamment en raison de la rotation du personnel. Dans toutes les prisons, un cours général de sensibilisation a été donné en 2012 et 2013 à la direction et aux cadres de surveillance supérieurs. En définitive, seule une minorité des fonctionnaires pénitentiaires a été formée ;

– enfin, la réunion semestrielle convenue dans le Protocole entre les responsables de la VSSE et la DG EPI n'a pour ainsi dire jamais eu lieu, ce qui ne signifie pas qu'il n'y avait aucune communication. En effet, les collaborateurs des deux services partageaient leurs expériences et étaient facilement joignables, mais là où le bât blesse, c'est au niveau de la concertation à un niveau supérieur.

II.6.4. INITIATIVES PRISES PAR LA VSSE EN DEHORS DU PROTOCOLE[100]

Il va de soi que la VSSE ne dépendait pas exclusivement du Protocole conclu avec la DG EPI pour élaborer sa position d'information sur les détenus (radicalisés). Le service a pris diverses initiatives, comme par exemple la collaboration développée en 2013 avec plusieurs services de renseignement européens pour échanger des expériences. Elle a donné lieu au rapport intitulé '*After the Prison*'.[101]

En outre, un *point of contact* (POC) a été désigné à la VSSE, une cellule 'Radicalisation dans les prisons' a été créée, chaque poste provincial de la VSSE a reçu une liste de personnes de contact de l'établissement pénitentiaire relevant de sa circonscription, et les éléments nécessaires à un suivi optimal de la problématique de la radicalisation dans les prisons ont été examinés.[102, 103]

II.6.5. CONCLUSION

Le Comité permanent R a conclu que le Protocole avait initié un mouvement. Une évolution certaine était perceptible. Toutefois, de nombreux aspects avaient

---

100 Ces initiatives ne faisaient pas l'objet de l'enquête du Comité permanent R.

101 Une note interne détaillée de la VSSE *('Intensifier les efforts de la VSSE dans les prisons')* souligne l'importance d'avoir un aperçu de la radicalisation au sein des établissements pénitentiaires.

102 Cette estimation est intervenue en décembre 2014 et a été intégrée dans la note interne susmentionnée de la VSSE *'Intensifier les efforts de la VSSE dans les prisons'* du 1er décembre 2014. Celle-ci comprend notamment une étude sur les besoins en personnel, les besoins en matière de HUMINT, la possibilité de s'adresser à un détenu en tant que source humaine, la fréquence à laquelle les pouvoirs publics sont informés et la désignation des collaborateurs pouvant bénéficier d'un accès exclusif au système SIDIS.

103 À la mi-mars 2016, le Comité a reçu une étude approfondie intitulée 'Analyse de phénomène Radicalisation et Terrorisme dans les prisons belges – Mars 2016' (traduction libre).

été négligés pendant assez longtemps. Certains aspects du Protocole n'ont même jamais été mis en œuvre. Cependant, les deux services se disaient très satisfaits. Tant la DG EPI que la VSSE indiquaient n'avoir constaté aucun manquement notable ni manifestation d'insatisfaction concernant le fonctionnement du Protocole, qu'elles considéraient comme positif. Le Comité permanent R a cependant signalé que le Protocole n'avait jamais fait l'objet d'une évaluation.

II.7. LE SUIVI D'UNE MENACE POTENTIELLE À L'ENCONTRE D'UN VISITEUR ÉTRANGER

En mars 2015, un agent des services extérieurs de la VSSE s'est adressé au service d'Enquêtes du Comité permanent R. Il se plaignait de la manière dont les services d'analyse avaient travaillé dans le dossier relatif à la visite imminente en Belgique du médecin congolais, M. Mukwege. Selon le plaignant – qui est aussi une connaissance du Docteur Mukwege et le co-organisateur de la visite – l'OCAM n'avait pas reçu la totalité des informations pertinentes lui permettant d'établir une évaluation correcte de la menace qui pesait sur l'intéressé.[104]

II.7.1. CONTEXTUALISATION

Le gynécologue congolais est connu comme militant des droits de l'homme. Il avait attiré l'attention de la VSSE pour la première fois dans le cadre des élections organisées en 2011 en République Démocratique du Congo. Le service a commencé à suivre ses activités surtout dans le contexte de ses visites en Belgique. Ces visites pouvaient avoir des répercussions au sein de la diaspora africaine ou sur les relations de la Belgique avec le Congo, ce qui pouvait présenter un danger pour la sécurité intérieure et extérieure de la Belgique ou pour ses relations extérieures.

Le Docteur Mukwege a effectué plusieurs visites en Belgique entre 2013 et 2015. Ces visites n'avaient jamais donné lieu à de quelconques mesures de sécurité de la part des autorités belges.

En décembre 2014, la VSSE a été informée de l'intention de l'intéressé de revenir dans notre pays en mars 2015. Étant donné que l'évaluation de la situation au Congo, tout comme les menaces visant le médecin, était une mission permanente, le service d'analyse concerné n'a pas établi d'apostille particulière à ce propos. L'initiative a donc été laissée aux services extérieurs d'organiser la collecte d'informations de manière autonome.

104 L'enquête de contrôle a été clôturée en mai 2016.

Fin février 2015, le service d'analyse concerné a rédigé une note pour l'OCAM et le Centre de Crise, en se basant sur des éléments collectés par des sources humaines et sur des informations provenant des médias sociaux. Au cours du mois de mars 2015, des rapports émanant d'autres sources sont encore parvenus à ce service d'analyse, mais n'ont pas apporté plus de détails quant à une éventuelle menace pesant sur le médecin. Ces rapports n'ont pas donné lieu à la rédaction d'une nouvelle note.

Sur l'insistance de l'agent des services extérieurs (c'est-à-dire l'agent qui allait introduire la plainte au Comité permanent R) et du chef hiérarchique, le service d'analyse a malgré tout établi une note complémentaire. Cette nouvelle note n'a pas amené l'OCAM à revoir son évaluation de la menace, qui est restée au 'niveau 2'.[105]

II.7.2. CONSTATATIONS

Le Comité permanent R a constaté que les éléments collectés avaient été évalués, analysés et transmis à l'OCAM et au Centre de Crise dans des délais raisonnables pour leur permettre de prendre les mesures adéquates.

Le Comité s'est interrogé sur le double rôle joué par le plaignant et sur sa fonction : il intervient d'une part en sa qualité d'agent de la VSSE, et d'autre part à titre privé.[106] Le Comité permanent R a attiré l'attention sur le fait que cette 'confusion des rôles' pouvait être préjudiciable au travail d'analyse final.

Le Comité n'a pas pu constater de dysfonctionnement dans manière dont le service d'analyse a géré la visite du Docteur Mukwege en Belgique. Le fait que la majorité des informations collectées proviennent d'un seul agent de collecte, à savoir le plaignant lui-même, aurait pu fausser l'objectivité de l'analyse qui en a résulté, ce qui n'a pas été le cas.

La 'liberté d'action' dont l'inspecteur traitant bénéficiait dans cette affaire s'explique notamment par l'absence de directives, aussi bien de la part des services d'analyse envers les services extérieurs qu'au sein des sections concernées des services extérieurs. Il n'y avait pas de plan de collecte en tant que tel. Le chef hiérarchique de l'agent avait bien donné un signal en refusant deux rapports établis par cet agent, mais pour le reste, aucune mesure fondamentale n'a été prise pour l'amener à changer d'attitude. En pareil cas, la direction de la VSSE pourrait intervenir de manière proactive.

105 L'agent concerné a été averti du maintien du niveau par l'OCAM.
106 Il n'a d'ailleurs pas caché sa proximité avec le Docteur Mukwege.

II.8. UNE PLAINTE CONTRE UN COLLÈGUE INDISCRET

En juillet 2015, un officier supérieur du SGRS a introduit une plainte auprès du Comité permanent R. Un collaborateur du SGRS aurait, en effet, divulgué des données sur sa vie privée et professionnelle dans un espace public, là où les deux protagonistes résident. L'officier craignait pour sa sécurité et celle de sa famille.

Le plaignant s'était déjà adressé à deux reprises à la direction du SGRS, mais avait estimé que la réaction manquait de fermeté. Il a finalement déposé plainte auprès du Comité permanent R. La plainte portait tant sur les indiscrétions présumées que sur la réaction du SGRS. Le rapport final a été approuvé en mai 2016.

II.8.1. CONSTATATIONS

Le collaborateur a admis avoir parlé du plaignant lors du drink, mais a nié avoir communiqué des données classifiées relatives au plaignant. Il n'aurait d'ailleurs jamais eu accès à de telles données. Le Chef du SGRS a déclaré s'être entretenu avec les deux protagonistes. Il estimait que les indiscrétions de son collaborateur étaient déplacées d'un point de vue professionnel. Il a demandé à ses services de rappeler le collaborateur administratif à l'ordre – ce qui a été fait – mais il n'a reçu aucun retour à ce sujet, en raison d'une erreur de communication.

Au départ, la plainte était considérée par le SGRS comme une problématique d'importance relative. Le Chef du SGRS avait jugé inadmissible le comportement du collaborateur administratif, mais avait constaté qu'il n'avait pas exploité d'informations confidentielles. Il avait dès lors estimé qu'une sanction disciplinaire n'était pas indiquée. Le collaborateur a néanmoins été muté dans un autre service du SGRS. La plainte a fini par être traitée par la section habilitations de sécurité du SGRS, et le collaborateur administratif s'est vu infliger un blâme.

II.8.2. CONCLUSIONS

Le Comité permanent R n'a trouvé aucune indication de violation du secret auquel le collaborateur administratif est pourtant tenu. Par ailleurs, aucun accès illicite à l'enquête de sécurité du plaignant ou à des informations classifiées n'a été noté.

Quant au devoir de discrétion, le Comité a néanmoins constaté que le collaborateur administratif n'avait pas fait preuve de la réserve et de la prudence professionnelles requises en abordant des questions d'ordre professionnel ou privé relatives au plaignant lors d'un drink. En ce sens, la plainte était fondée.

Dans son enquête, le Comité n'a trouvé aucun élément indiquant un problème de sécurité dans le chef du plaignant ou de sa famille. De manière générale, le Comité estime que la plainte aurait pu être traitée de manière plus adéquate en interne.

II.9. UNE PLAINTE RELATIVE À UN PAIEMENT DÛ (OU NON)

En avril 2015, un ancien inspecteur de la VSSE avait adressé une plainte au Comité permanent R. En effet, il avait été contraint de rembourser une somme (modeste) qu'il aurait perçue à tort et qui provenait de la caisse des fonds spéciaux. Après avoir tenté, en vain, de défendre son point de vue auprès de la VSSE, il avait décidé de se tourner vers le Comité permanent R. Il avait en outre indiqué que les problèmes qu'il avait rencontrés avec sa hiérarchie directe l'avaient incité à quitter la VSSE.[107]

Aussi le Comité a-t-il décidé d'ouvrir une *« enquête de contrôle suite à la plainte d'un ancien agent de la VSSE relative à la gestion de la caisse de service d'un poste de province »*.[108]

Au cours de la période où il a été demandé au plaignant de restituer une somme (2012-2013), un système comptable inadéquat et non conforme aux instructions de l'administration centrale était utilisé.[109] Le Comité permanent R n'a d'ailleurs pas pu trouver de preuve qui aurait étayé ou contredit l'assertion du plaignant. Le système comptable utilisé à ce moment-là ne permettait d'effectuer aucun contrôle *post factum*, si bien qu'il n'était pas possible de déterminer, sur le plan comptable, si la somme contestée était due ou non. Lors du traitement de la plainte au niveau de la VSSE, aucun responsable n'a été mandaté pour résoudre le différend. Dès lors, de nombreuses personnes sont intervenues dans cette affaire, sans qu'une solution acceptable pour tous les intéressés puisse être trouvée. Ce procédé a contribué à générer une insatisfaction et des tensions inutiles.

II.10. UNE PLAINTE RELATIVE À UNE INTERVENTION CONTROVERSÉE DE DEUX ASSISTANTS DE PROTECTION

En juin 2015, un incident impliquant deux membres du Service Protection des personnes de la VSSE (de l'époque[110]) s'est produit lors d'une mission sur la voie publique. Les assistants de protection étaient chargés d'assurer la sécurité d'un

---

107 Le plaignant a travaillé plus de trois ans comme membre des services extérieurs de la Sûreté de l'État.

108 L'enquête a été clôturée en mai 2016.

109 D'une précédente enquête de contrôle sur l'utilisation de ce que l'on appelle les 'fonds secrets' de la VSSE, il est ressorti que pendant la période citée, la gestion des comptes au niveau local ou le traitement comptable sur place n'ont été que peu contrôlés. Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2013*, 58-59 et *Rapport d'activités 2014*, 65.

110 Cette compétence a été transférée de la VSSE à la Police fédérale (l'article 7, 3° L.R&S a été abrogé par l'article 20 Loi du 21 avril 2016, *M.B.* 29 avril 2016).

diplomate étranger, lorsque la voiture d'un particulier les a brièvement suivis et a ignoré à plusieurs reprises leurs ordres de se tenir à distance. Lorsque le véhicule de l'intéressé s'est immobilisé à un feu de signalisation, les assistants de protection sont intervenus. Ils auraient fait preuve d'agressivité, l'un d'eux ayant même sorti son arme. Le conducteur de ce véhicule a rapporté ces faits au Comité.[111]

Le Comité permanent R a entendu tous les protagonistes. Tous les rapports internes dressés à ce sujet au sein de la VSSE ont été examinés. Le Comité a également pris connaissance des dispositions légales et réglementaires ainsi que des directives et consignes internes qui s'appliquaient à l'exécution des missions de protection rapprochée de la VSSE.

La personne escortée le jour des faits bénéficiait d'une protection permanente et faisait l'objet d'une menace évaluée au niveau 3.[112] Le Comité permanent R a estimé qu'en l'occurrence, les rapprochements successifs opérés par la plaignante avec le véhicule d'escorte ont donné aux agents de la VSSE des motifs raisonnables de croire que la vie ou l'intégrité physique de la personne qu'ils étaient chargés de protéger était gravement mise en danger. Cette inquiétude justifiait donc le contrôle du véhicule et de sa conductrice. L'incident était sans nul doute le résultat d'un manque de prudence et de conscience de la part de la plaignante, qui n'a pas suffisamment pris ses distances par rapport au véhicule banalisé de la VSSE.

Le Comité était néanmoins convaincu que l'incident aurait pu être évité si l'équipe de protection n'avait pas rencontré des problèmes de communication. L'équipe ne pouvait pas communiquer de manière appropriée avec l'intéressée (pas de panneau de communication) et ne disposait pas de moyens de communication adéquats[113] qui leur auraient permis d'évaluer la situation. Le Comité a également constaté à la VSSE l'absence de possibilités d'entraînement en situations réalistes de stress.

Le Comité permanent R a jugé que le recours à la violence était 'raisonnable' dans les circonstances du moment, même si la plaignante ne l'a pas perçu comme tel et même si, rétrospectivement, il est apparu qu'il n'y avait aucune menace réelle.

---

111 Le Comité permanent R a décidé d'ouvrir une enquête de contrôle le 24 juin 2015. Les travaux ont dû être suspendus à plusieurs reprises en raison d'autres enquêtes confiées au Comité et jugées plus urgentes. Le rapport final a été approuvé le 11 mai 2016.

112 Le niveau 3 est attribué lorsque la menace est considérée comme possible et vraisemblable, ce qui requiert par conséquent une attention soutenue de la part des agents de protection.

113 Lors des missions, la communication entre les équipes de protection et les services de police passe par le réseau ASTRID. L'enquête de contrôle effectuée en 2014 avait déjà permis de constater que le réseau de communication était inopérant dans certaines zones du pays. Voir COMITÉ PERMANENT R, *Rapport d'activités 2014*, 45-52 ('II. 4. La VSSE et sa mission légale de protection des personnes').

II.11. UNE PLAINTE RELATIVE À UNE INTERVENTION DE L'OCAM

En mai 2015, le Comité permanent R, conjointement au Comité permanent P, a ouvert une enquête sur la manière dont l'OCAM avait joué un rôle dans le retrait de la licence d'un pilote de ligne.[114] L'intéressé s'interrogeait sur l'intervention et la compétence de l'OCAM. Les Comités ont estimé ne pas avoir la compétence légale d'apprécier le bien-fondé du motif ayant justifié la suspension de la licence. L'enquête s'est limitée à évaluer le rôle de l'OCAM. L'enquête a été finalisée en décembre 2016.

II.11.1. LES NOTES D'ÉVALUATION DE L'OCAM

Début 2010, la Direction générale Transport aérien (DGTA) du SPF Mobilité et Transports a informé l'OCAM qu'un citoyen belge aurait menacé par téléphone de commettre un attentat dans le pays où il avait exercé la profession de pilote jusqu'en 1999. Ses menaces viseraient à forcer les autorités compétentes de lui restituer la licence de vol qui lui avait été retirée pour des raisons d'ordre psychique.

La DGTA a demandé une évaluation de la menace à l'OCAM, qui a réagi rapidement en ces termes : « *Het OCAD kan niet evalueren of (betrokkene) de vermelde bedreigingen daadwerkelijk geuit heeft. Wel zijn de aard van de bedreigingen van die aard dat de grootste omzichtigheid aan de dag moet worden gelegd, ook al wordt het uiten van de dreiging door de betrokkene tegengesproken. Er zijn – op dit ogenblik – ten andere geen elementen aanwezig om te twijfelen aan de versie van de politie* ».[115] Et ensuite : « *een onderzoek van de psychische toestand van betrokkene lijkt meer dan aangewezen. Als dit onderzoek aantoont dat er wel degelijk sprake is van psychische labiliteit, dan kan het OCAD niet anders concluderen dat de ernst van de dreiging als ernstig moet worden ingeschat en de waarschijnlijkheid tot het plegen van een aanslag als mogelijk. Rekening houdend met de bovenstaande elementen stelt het OCAD het niveau van de terroristische of extremistische dreiging uitgaande van betrokkene in deze hypothese vast op ERNSTIG (niveau 3)* ».[116]

---

114 Sur base de l'article 63 L.Contrôle, un conseiller s'est abstenu de participer à l'enquête de contrôle.

115 « *L'OCAM n'est pas en mesure d'évaluer si* (l'intéressé) *a effectivement proféré les menaces dont il est fait mention. Néanmoins, des menaces de ce genre doivent appeler à la plus grande prudence, même si l'intéressé a nié avoir proféré la menace. Il n'y a d'ailleurs – pour le moment – aucun élément permettant de mettre en doute la version de la police* » (traduction libre).

116 « *Un examen de l'état psychique de l'intéressé semble plus qu'indiqué. Si cet examen démontre qu'il est effectivement question d'instabilité psychique, l'OCAM ne peut que conclure que la menace doit être considérée comme grave, et la commission d'un attentat comme possible.*

La DGTA a alors suspendu la licence de pilote du plaignant en Belgique. Vu les doutes sur sa capacité à conserver sa licence de pilote, le plaignant a dû se soumettre à un examen médical. Cet examen a eu lieu en avril 2010 et a conclu à la capacité du plaignant de disposer de sa licence de vol, sous réserve qu'il se soumette annuellement à un examen psychiatrique.

En mai 2010, l'OCAM a établi une nouvelle évaluation. Tenant compte du rapport médical, l'OCAM a ramené l'évaluation de la menace au niveau 2. La note d'évaluation mentionnait que « *de ernst van de dreiging, uitgaande van de heer X blijft, gelet op de concrete geuite bedreigingen in het verleden, door het OCAD ingeschat op ernstig. Evenwel wordt op heden de waarschijnlijkheid van de uitvoering van de dreiging, gelet op het vermeld psychiatrisch verslag, ingeschat als weinig waarschijnlijk* ».[117] Et plus loin que « *het komt in deze context evenwel wettelijk gezien niet aan het OCAD toe om advies te geven over de wenselijkheid om aan de Heer X opnieuw een vliegbrevet uit te reiken* ».[118]

II.11.2. UNE COMPÉTENCE DE L'OCAM ?

Les compétences *rationae materiae* de l'OCAM sont décrites à l'article 3 de la Loi du 10 juillet 2006 relative à l'analyse de la menace (L.OCAM) et sont précisées dans l'Arrêté royal du 28 novembre 2006 portant exécution de la L.OCAM (AR OCAM). Sont visées les menaces énumérées à l'article 8, 1°, *b)* et *c)* L.R&S, soit le terrorisme[119] et l'extrémisme.[120] De plus, ces menaces doivent être dirigées contre l'intégrité des personnes en Belgique et des ressortissants belges à l'étranger, l'infrastructure critique du pays sous certaines conditions, les événements ou les groupements définis et les institutions et les intérêts belges à l'étranger.

Compte tenu des éléments repris ci-dessus, l'OCAM établit, dans cette hypothèse, le niveau de la menace terroriste ou extrémiste émanant de l'intéressé à GRAVE (niveau 3) » (traduction libre).

117 « *Eu égard aux menaces concrètes qui ont été proférées dans le passé, la menace émanant de Monsieur X. est toujours considérée comme grave par l'OCAM. Toutefois, un passage à l'acte est à présent considéré comme peu probable au vu du rapport psychiatrique mentionné* » (traduction libre).

118 « *Dans ce contexte, il n'appartient cependant pas à l'OCAM, d'un point de vue légal, de donner un avis sur l'opportunité de délivrer à nouveau un brevet de pilote à Monsieur X.* » (traduction libre).

119 L'article 8, 1°, *b)* L.R&S définit le terrorisme comme étant « *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* ».

120 L'article 8, 1°, *c)* L.R&S définit l'extrémisme comme étant « *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* ».

Dans sa première note d'évaluation, l'OCAM estimait qu'il s'agissait d'une menace terroriste et extrémiste. Selon informations initiales, cette menace visait à forcer les autorités compétentes à restituer à l'intéressé sa licence de vol.

Se sentant tenu de statuer dans l'urgence, l'OCAM a réalisé son évaluation sur base des seuls éléments d'information qui ont été portés à sa connaissance, en tenant compte des quatre critères suivants :

- la gravité de la menace ;
- la fiabilité de la source d'informations, tenue d'emblée pour acquise s'agissant d'un service de police étranger ;
- la capacité du plaignant à mettre cette menace à exécution, elle aussi tenue pour acquise vu sa profession de pilote ;
- la probabilité qu'il la mette à exécution, tenue pour vraisemblable vu l'état psychique allégué de l'intéressé.

Cependant, aucune confrontation de ces éléments n'a été établie avec le point de vue exposé par le plaignant à la DGTA.

Les Comités étaient d'avis que selon les informations disponibles, l'objectif des menaces proférées par le plaignant relevait d'un intérêt personnel et non d'une quelconque motivation idéologique ou politique. Il n'était donc pas question ici d'une menace terroriste ou extrémiste. Dès lors, la compétence légale de l'OCAM d'effectuer une analyse en la matière n'était pas établie. Les deux Comités étaient conscients de la situation difficile dans laquelle se trouvait l'OCAM par rapport à cette demande de la Direction générale du trafic aérien.

II.12. ÉVALUATIONS INDIVIDUELLES DE LA MENACE PAR L'OCAM

II.12.1. OBJECTIF DE L'ENQUÊTE

La mission de l'OCAM est de déterminer le niveau de la menace en matière de terrorisme et d'extrémisme. Ce niveau de la menace peut, entre autres, être établi par rapport à des événements, des lieux, ou encore par rapport à des individus. En mars 2015, les Comités permanents R et P ont ouvert une enquête de contrôle commune sur *« la manière dont l'OCAM détermine le niveau de la menace que représente un individu ou de celle qui le vise, sur les conséquences que la détermination de ce niveau de la menace entraîne sur la répartition des tâches, les mesures à prendre et l'échange d'information entre services concernés, ainsi que sur les conséquences pratiques pour la personne concernée et son suivi ».* Cette enquête a été initiée à la demande de la Commission de suivi de la Chambre, qui souhaitait obtenir des réponses aux questions suivantes :

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

Un rapport intermédiaire a été envoyé à la Commission de suivi en février 2016. Dans le prolongement des activités menées pour la Commission parlementaire 'attentats terroristes', les deux Comités ont décidé que l'enquête n'était plus d'actualité, et ils y ont mis fin. Par conséquent, seuls les résultats intermédiaires de l'enquête sont repris ci-après.

II.12.2. CADRE JURIDIQUE

Aux termes de la Loi du 10 juillet 2006 relative à l'analyse de la menace (L.OCAM), l'organe de coordination s'est vu confier trois missions, dont une consiste à « *effectuer ponctuellement une évaluation commune qui doit permettre d'apprécier si des menaces visées à l'article 3 se manifestent et, le cas échéant, quelles mesures s'avèrent nécessaires* » (art. 8, 2 L.OCAM). L'OCAM n'est donc pas compétent pour procéder à des évaluations concernant d'autres types de menaces que le terrorisme et l'extrémisme.[121]

L'Arrêté royal portant exécution de la Loi du 10 juillet 2006 relative à l'analyse de la menace (AR OCAM) stipule que les évaluations de l'OCAM doivent, d'une part, porter sur les personnes, groupements, objets ou événements susceptibles de représenter une menace terroriste ou extrémiste, et d'autre part, sur les personnes, groupements ou objets susceptibles d'être les cibles ou les victimes d'une telle menace. Pour être complet, il convient encore de mentionner que l'OCAM est également compétent pour effectuer une évaluation de la menace en ce qui concerne les infrastructures critiques.

Le Roi fixe les modalités relatives aux évaluations. L'article 11 § 6 AR OCAM répertorie deux critères d'évaluation du niveau de la menace : d'une part, la gravité du danger ou de la menace, et d'autre part la vraisemblance de ce danger

[121] Ainsi, par d'exemple, les menaces liées à l'espionnage sont de la compétence des services de renseignement. Les menaces d'atteinte à l'ordre public ou celles liées au crime organisé sont, quant à elles, de la compétence de la Police fédérale.

ou de cette menace. Pour déterminer la gravité de chaque menace (et donc également en ce qui concerne les personnes), l'OCAM doit déterminer un 'niveau', allant de 1 (faible) à 4 (très grave) (art. 11 § 6 AR OCAM).

II.12.3. LES ÉVALUATIONS DE LA MENACE DE L'OCAM (2011-2015)

Une note interne de l'OCAM, datant de 2011, indique que «*l'évaluation ponctuelle […] [comprend] toujours [les points suivants] : l'exposé de l'événement, la description du contexte (situation politique, précédent historique…), la fixation du niveau de menace et s'il échet la suggestion de certaines mesures*». La note impose également que l'évaluation fasse l'objet d'un contrôle de qualité sur la base d'un '*peer counseling*' informel.

Il est ressorti d'une enquête précédente que ces évaluations ne se fondaient sur aucun processus ou critère d'analyse formalisé.[122] Arguant de la spécificité de chaque cas et de l'application des 'principes généraux en matière d'analyse', l'OCAM estimait même inutile de disposer d'une procédure d'évaluation formalisée, la seule garantie de qualité étant la vérification, par la direction, de la conformité de l'évaluation avec la ligne générale de l'OCAM.

Entre 2013 et 2015, la situation n'a que très peu évolué. Les Comités ont constaté que l'OCAM ne voyait pas la nécessité d'adapter sa méthode de travail.

Dans le cadre de la présente enquête de contrôle, les Comités permanents R et P ont examiné une trentaine d'évaluations tirées, de sept dossiers individuels[123], et ont dressé les constats suivants :

– jusqu'à la fin de l'année 2015, aucune méthodologie formelle, ni critère précis, n'était employé(e) pour déterminer la gravité, la vraisemblance, et donc le niveau de la menace, à l'égard ou émanant de personnes. La méthodologie telle que définie à l'article 11 § 6 AR OCAM, qui établit deux critères d'évaluation du niveau de la menace (*supra*), plus précisément la gravité du danger ou de la menace et la vraisemblance de ce danger ou de cette menace, n'était presque jamais explicitement appliquée ;
– l'OCAM a rarement respecté ses propres règles en matière d'évaluation. Les évaluations réalisées entre 2012 et 2015 étaient souvent sommaires et n'accordaient que peu d'attention à la contextualisation. On ne pouvait pas véritablement parler d'analyses ;

122 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 35-39 ('II.5. Enquête commune sur les évaluations de la menace effectuées par l'OCAM concernant des personnalités étrangères en visite en Belgique').

123 Ces dossiers ont été sélectionnés sur une période de trois ans suivant l'enquête commune effectuée par des deux Comités en 2012. L'OCAM a réalisé, au cours de cette période, environ 1000 évaluations par an, et en 2015 jusqu'à plus de 1500.

– des problèmes ont été signalés dans les flux d'informations entre les services de police, les autorités judiciaires et l'OCAM. Par ailleurs, la classification de certaines informations par les services de renseignement empêchait leur diffusion et leur utilisation par les autorités chargées de mettre en œuvre les mesures de sécurité ;
– une fois reçues par le Centre de crise du gouvernement, les évaluations de la menace étaient discutées avec les représentants des différents services et autorités. La plupart des mesures faisaient l'objet d'une discussion collégiale avant d'être décidées par le Centre de crise du gouvernement. Là où l'OCAM formulait des propositions, celles-ci étaient floues.

II.12.4. UNE NOUVELLE MÉTHODOLOGIE

En 2015, le Conseil national de sécurité et le Comité stratégique du renseignement et de la sécurité ont chargé l'OCAM et le Centre de crise de développer une méthodologie d'évaluation ponctuelle *« qui puisse déterminer avec le plus de précision possible le niveau de la menace »*. La méthodologie proposée par les deux services distinguait trois types d'analyses :
– la menace envers des personnes, des événements ou des intérêts ;
– la menace émanant d'individus et/ou de groupes ;
– la menace générale en Belgique.

Il était proposé que la méthodologie d'évaluation de la menace pour la première catégorie (des personnes, des événements ou des intérêts) repose sur l'analyse de trois facteurs :
– l'information de base donnant lieu à évaluation (quelle en est la source ? Est-elle fiable et crédible ?) ;
– la vraisemblance de l'information (l'information doit être évaluée comme 'très improbable', 'improbable', 'possible', 'vraisemblable' ou 'certaine') ;
– le degré de gravité ('très basse', 'basse', 'moyenne', 'haute', 'très haute', 'critique') de l'impact sur la sécurité, l'ordre public, les infrastructures, la vie des citoyens.

Chacun de ces facteurs doit se voir attribuer un score, et la combinaison de ces scores sur une matrice d'évaluation permettra de déterminer un niveau de menace (entre 1 et 4). Un niveau de contrôle interne et externe est également prévu.

Cette nouvelle méthodologie, proposée en octobre 2015, a été soumise à l'appréciation des deux ministres de tutelle. Étant donné que la méthodologie n'a pas été mise en œuvre au cours de la présente enquête, les Comités n'ont pas été en mesure d'en évaluer l'application.

II.13. DYSFONCTIONNEMENTS SPÉCIFIQUES AU SEIN DE L'OCAM

Au second semestre de 2015, les Comités permanents R et P ont reçu deux lettres anonymes, qui faisaient référence à des « *irrégularités* » et à des « *problèmes structurels graves* » au sein de l'organe de coordination. Peu après, les Comités ont encore reçu une plainte portant sur le fonctionnement interne de l'OCAM. En octobre 2015, les Comités permanents R et P ont regroupé toutes les questions dans une « *enquête de contrôle commune sur des dysfonctionnements internes dénoncés au sein de l'OCAM* ».[124]

La première dénonciation concernait la rédaction de fiches individuelles relatives aux *foreign terrorist fighters*.[125] Le plaignant estimait que l'exécution de cette mission était incompatible avec sa fonction d'expert. L'article 3 AR OCAM stipule que l'OCAM peut disposer d'analystes (statutaires) et d'experts (détachés), dotés d'un profil spécifique à leur fonction.[126] Les Comités étaient d'avis que la rédaction de fiches individuelles suggérait une évaluation ponctuelle de la menace que représente chaque FTF. L'attribution de cette tâche aux experts n'était donc pas incompatible avec leur profil. En outre, il va de soi que les analystes étaient eux aussi investis d'une responsabilité en la matière, ce qui ne présentait pas, ici non plus, d'incompatibilité avec leur profil. Au cours de l'enquête, les Comités ont pu constater que la répartition de la tâche de rédaction des fiches FTF entre les experts et les analystes avait été adaptée pour tendre vers un meilleur équilibre.

---

124 Le rapport final a été approuvé en septembre 2016.

125 La Circulaire du 21 août 2015 relative à l'échange d'informations et au suivi des FTF attribue à l'OCAM la mission de créer une fiche individuelle de renseignement dès qu'un individu peut se révéler être un FTF. Le service est tenu de prendre les mesures nécessaires à cet égard afin d'assurer un éventuel suivi dans les plus brefs délais.

126 L'annexe 3 de l'AR OCAM définit les profils.
« *L'analyste est responsable, sous l'autorité du directeur de l'OCAM ou de celui qui a été délégué par lui comme chef de département, de la récolte et de la recherche d'informations et des renseignements concernant le phénomène du terrorisme selon une répartition en sphères d'intérêt, entre autres, géographique, ethnique et religieuse. En outre il doit analyser avec minutie la situation géopolitique liée à ces sphères d'intérêt selon sa spécialité. Il est également responsable de l'introduction des données traitées dans les fichiers de la documentation spécialisée de l'OCAM. Il est chargé de l'analyse des données récoltées et de leur traitement et d'en assurer des évaluations périodiques et stratégiques en collaboration avec les experts détachés des services d'appui* ». L'intéressé participe également à des réunions en Belgique et à l'étranger axées sur le terrorisme et l'extrémisme. Il assure une permanence à tour de rôle.
« *L'expert est responsable de la collecte et de la recherche d'informations et de renseignements concernant la situation géopolitique et le phénomène du terrorisme […]. Il est chargé de l'analyse permanente des données entrantes et est responsable de leur traduction en évaluations ponctuelles, utilisables concernant la menace terroriste potentielle et ceci en étroite collaboration avec les autres experts et analystes de l'OCAM* ». Il assure également la fonction d'officier de liaison pour son service d'origine. Il est responsable de l'introduction et de l'actualisation des données traitées dans les fichiers de la documentation spécialisée de l'OCAM.

Le second volet de la dénonciation concernait l'irrégularité du détachement à l'OCAM d'un agent contractuel d'un service d'appui. En effet, le détachement d'un agent contractuel n'était pas conforme à l'article 83 de l'Arrêté royal du 23 janvier 2007 relatif au personnel de l'Organe de coordination pour l'analyse de la menace.[127, 128] Seule une modification de la réglementation permettrait de régulariser le détachement de contractuels.[129]

Le plaignant anonyme évoquait par ailleurs le traitement de faveur dont aurait bénéficié un expert de la part de la direction. Il aurait été avantagé au niveau de la formation. Les Comités permanents R et P n'ont trouvé aucun indice en ce sens.

Un autre plaignant citait la décision – injustifiée selon lui – de mettre fin à son détachement. Les Comités permanents R et P se sont abstenus de juger le bien-fondé de cette décision. Ils ont cependant dû constater que plusieurs incidents survenus précédemment avaient déjà détérioré la relation professionnelle et personnelle entre la direction et le plaignant. Ils étaient néanmoins d'avis que la manière dont la décision formelle avait été prise reflétait une méconnaissance du principe général de bonne gestion. Mais censurer ou réformer la décision n'entrait pas dans les compétences des Comités.[130]

La dénonciation mentionnait également des voyages inutiles et des contacts internationaux inappropriés établis par l'OCAM. Les Comités avaient déjà enquêté sur ces dénonciations.[131] La plainte ne comportait aucun nouvel élément à ce niveau.

S'agissant de la remarque sur 'les problèmes d'alcoolisme latents' chez certains membres du personnel, une évaluation objective de l'ampleur du problème a été demandée à la direction, ainsi que des informations sur les mesures (préventives ou disciplinaires) qui avaient été prises. Les Comités ont pris acte des mesures prises.

Enfin, le plaignant a fait état de pressions qu'il aurait subies pour qu'il s'abstienne d'évoquer les dysfonctionnements précités. Faute d'éléments tangibles, les Comités n'étaient pas en mesure de vérifier cette allégation.

---

127 « *Les emplois d'expert et les emplois de personnel administratif auprès de l'OCAM sont occupés, par voie de détachement, par des agents nommés à titre définitif dans les services d'appui selon une répartition fixée par le Conseil National de Sécurité, sur la proposition du directeur et du directeur adjoint* ».

128 La direction de l'OCAM a insisté sur le fait que le détachement n'avait jamais fait l'objet d'un quelconque recours et qu'elle se félicitait du travail accompli par l'intéressé. Mais cela ne changeait rien à l'irrégularité.

129 La direction de l'OCAM a pris une initiative à cet égard, mais les ministres de tutelle n'y ont pas réagi.

130 Les Comités ont pris acte du fait que le plaignant n'a pas introduit de recours au Conseil d'État ou devant les tribunaux compétents.

131 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 33-37 ('II.7. Les contacts internationaux de l'OCAM').

II.14. UNE PLAINTE DANS LE CADRE D'UNE ENQUÊTE DE SÉCURITÉ AU SGRS

II.14.1. CONTEXTUALISATION

En avril 2015, le Comité permanent R a reçu une plainte relative à une enquête de sécurité effectuée par le SGRS. De manière plus spécifique, la plaignante indiquait que dans le cadre de l'enquête de sécurité visant son conjoint, le SGRS avait recueilli des informations erronées la concernant. Elle prétendait qu'il lui avait été reproché d'avoir obtenu, par voie illicite, des informations reprises dans la base de données de l'Office des étrangers (OE) à propos d'un membre de la Défense avec lequel son conjoint était entré en contact. La plaignante a fermement démenti ces allégations. Elle a précisé que le SGRS n'aurait pas correctement répertorié des informations à caractère personnel dans ses fichiers, ce qui aurait mis en cause son intégrité professionnelle.[132]

II.14.2. CONSTATATIONS

Pour son enquête de contrôle, le SGRS ne prend en considération que des données recueillies conformément aux dispositions légales.[133] Il s'agit, d'une part, de données à caractère personnel complétées par le demandeur lui-même et, par extension, son partenaire, dans le questionnaire de base en vue de l'obtention d'une habilitation de sécurité, et d'autre part, de renseignements complémentaires (données administratives, policières et judiciaires) recueillies par le service de renseignement.[134] Lors de la consultation du dossier de sécurité, le Comité a pu constater que le nom de la plaignante ne figurait pas dans la décision relative à l'enquête de sécurité et que le SGRS n'avait jamais porté atteinte à l'intégrité de l'intéressée.

---

132 Son conjoint n'était pas d'accord avec l'abaissement du niveau de sa nouvelle habilitation de sécurité et a fait appel (avec succès) de cette décision auprès de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. La procédure d'appel a entraîné la suspension de l'enquête de contrôle, qui a finalement été clôturée en mars 2016.

133 La Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Le SGRS se base également sur la Directive du 16 février 2000 de ce qui était encore le Comité ministériel du renseignement et de la sécurité concernant l'ampleur des enquêtes de sécurité.

134 Ces données sont accessibles aux seuls agents du SGRS spécialement mandatés à cet effet, pour autant qu'ils aient besoin d'en prendre connaissance et d'y avoir accès dans l'exercice de leur fonction ou de leur mission afin de traiter ces données dans le cadre d'une demande d'habilitation de sécurité.

II.15. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ EFFECTUÉS EN 2016 ET QUI ONT DÉBUTÉ EN 2016

II.15.1. LA POSITION D'INFORMATION DE L'OCAM AVANT LES ATTENTATS DE PARIS

Presque immédiatement après les attentats de Paris de novembre 2015, le Comité permanent R a ouvert une enquête de contrôle sur la position d'information des deux services de renseignement belges (voir II.3). 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 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 deux 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 ensuite été entendu à plusieurs reprises par la commission d'enquête, qui a *de facto* repris les questions de l'enquête, les Comités n'ont pas jugé pertinent de reprendre les devoirs d'enquête.[135]

II.15.2. L'ÉCHANGE DE DONNÉES SUR LES *FOREIGN TERRORIST FIGHTERS* AU NIVEAU INTERNATIONAL

Lors d'une réunion internationale à laquelle participaient plusieurs organes de contrôle européens[136], il a été décidé d'initier, dans tous les pays participants,

---

135 Lors de leur réunion commune du 13 juin 2017, les deux Comités ont décidé de clôturer l'enquête et de ne pas rédiger de rapport final. Le président de la Commission de suivi en a été informé le 15 juin 2017 et n'a émis aucune objection.

136 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.

une enquête de contrôle similaire 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[137] consiste à obtenir la vue la plus claire et la plus 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 en vue d'améliorer la position d'information des services concernés, sans pour autant éroder les droits du citoyen.

Diverses missions d'enquête ont été effectuées au second semestre de 2016, tant au niveau national qu'international. Les résultats de l'enquête de contrôle seront utilisés – là où c'est possible vu les restrictions en matière de classification – pour étoffer l'enquête internationale.

[137] L'enquête a démarré fin août 2016, après que la Commission de d'accompagnement de la Chambre des Représentants eut approuvé l'initiative qui lui avait été soumise.

CHAPITRE III
LE CONTRÔLE DES MÉTHODES PARTICULIÈRES DE RENSEIGNEMENT

Ce chapitre offre un aperçu de l'utilisation 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 en 2016.[138] Le rapport portant sur l'utilisation des méthodes particulières par les services de renseignement, qui a été établi en exécution de l'article 35 § 2 L.Contrôle, constitue la base de ce chapitre.[139]

La première partie est néanmoins consacrée à un examen plus approfondi des quatre lois qui sont entrées en vigueur en 2016 et qui ont induit des modifications pour les MRD. En raison de ces modifications, il n'a pas toujours été possible de comparer les chiffres de l'année d'activités 2016 avec ceux des années précédentes.

Pour des raisons évidentes, il n'a pas été possible non plus, dans ce chapitre, de prendre en considération deux autres modifications de loi. La première est la 'Loi PNR' du 25 décembre 2016.[140] Certes, cette loi a été votée au cours de l'année de référence, mais elle n'est pas entrée en vigueur cette année-là. La seconde modification concerne la réglementation MRD qui a été discutée au Parlement en 2016, mais qui n'est entrée en vigueur que le 8 mai 2017.

---

138 La Commission BIM assure le contrôle *a priori* de la mise en œuvre des méthodes particulières de renseignement. Voir à ce propos: COMITÉ PERMANENT R, *Rapport d'activités 2010*, 53-55 ('III.1.2. Le contrôle par la Commission BIM') et P. DE SMET, 'Check and balances. A priori en a posteriori controle', VAN LATEHM, W., VAN DAELE, D. et VANGEEBERGEN, B. (eds.), *De wet op de bijzondere inlichtingenmethoden*, Intersentia, Antwerpen, 2010, 93-118.

139 Conformément à 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), qui a modifié l'article 35 § 2, alinéa 1er, L. Contrôle, le Comité ne fera plus rapport « *tous les six mois* » sur l'application des méthodes MRD, mais bien « *annuellement* ».

140 Loi du 25 décembre 2016 relative au traitement des données des passagers, *M.B.* 25 janvier 2017. PNR est l'acronyme de *Passenger Name Record*.

III.1. LES QUATRE MODIFICATIONS DE LOI INTERVENUES EN 2016

III.1.1. UNE NOUVELLE MISSION POUR LES SERVICES DE RENSEIGNEMENT

La loi du 29 janvier 2016[141] a explicitement octroyé aux deux services de renseignement la mission de «*rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge*» (articles 7, 3°/1 ; et 11 § 1er, 5° L.R&S). Conformément à l'article 18/1, alinéa 1er, 1° et 2° L.R&S, la VSSE et le SGRS peuvent mettre en œuvre des méthodes spécifiques et exceptionnelles dans ce cadre. Dans de nombreux cas, cette nouvelle compétence est étroitement liée à la possibilité de suivre des services de renseignement étrangers qui pratiquent l'espionnage ou l'ingérence en Belgique. Aussi le Comité a-t-il fait remarquer que dans ces cas, les services de renseignement faisaient référence à ces menaces, et non à la nouvelle compétence. Le Comité permanent R a attiré l'attention de la VSSE et du SGRS à ce sujet, afin qu'il soit possible, à l'avenir, d'avoir une vue précise sur la mise en œuvre de cette nouvelle compétence.

III.1.2. L'IDENTIFICATION DE L'UTILISATEUR DE TÉLÉCOMMUNICATIONS OU D'UN MOYEN DE COMMUNICATION UTILISÉE COMME UNE MÉTHODE ORDINAIRE

Depuis la Loi du 5 février 2016 modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice[142], l'identification de l'utilisateur de télécommunications ou d'un moyen de communication utilisé est considérée – suite aux recommandations du Comité permanent R[143] – 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 organique des services de renseignement et de sécurité du 30 novembre 1998.

Lorsque l'identification (et la localisation) est réalisée à l'aide d'un moyen technique (et donc pas via une réquisition adressée à un opérateur), la collecte reste une méthode spécifique. Les articles 18/2 § 1er et 18/7 § 1er L.R&S ont été adaptés à cette fin. Une nouvelle méthode spécifique a également été inscrite dans ces dispositions : l'obtention des données relatives à la méthode de paiement,

141 *M.B.* 24 février 2016.
142 *M.B.* 19 février 2016.
143 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 71.

l'identification du moyen de paiement de l'abonnement ou de l'utilisation du service de communication électronique via la réquisition d'un opérateur de communications électroniques ou d'un fournisseur d'un service de communications électroniques ou par accès direct aux fichiers concernés.

La nouvelle 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.

Cette modification de la loi est entrée en vigueur le 29 février 2016. Il n'était donc pas évident pour le Comité de produire des chiffres permettant une comparaison complète avec les années précédentes (voir le point III.2 ci-après).

III.1.3. UNE NOUVELLE LOI SUR LA RÉTENTION DE DONNÉES AVEC DES IMPLICATIONS POUR LES SERVICES DE RENSEIGNEMENT

La Loi du 29 mai 2016[144] a modifié l'obligation pour les opérateurs de conserver certaines métadonnées pendant douze mois. Cette modification de la loi résultait d'une décision de la Cour européenne de Luxembourg et d'un arrêt de la Cour constitutionnelle.

La modification de la loi a aussi impacté la mise en œuvre de certaines méthodes spécifiques par les services de renseignement. Ainsi, la réquisition de certaines données via des opérateurs était limitée dans le temps. L'article 18/8 L.R&S permet aux deux services de renseignement « *au besoin en requérant à cette fin le concours technique de l'opérateur d'un réseau de communication électronique ou du fournisseur d'un service de communication électronique,* [de] *procéder ou faire procéder 1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées; 2° à la localisation de l'origine ou de la destination de communications électroniques* ». Si la VSSE ou le SGRS souhaite obtenir ces données via un opérateur, la loi pose des limites. Ainsi, pour une menace potentielle qui se rapporte à une activité pouvant être liée à des organisations criminelles ou à des organisations sectaires nuisibles, le dirigeant du service ne peut, dans sa décision, requérir les données que pour une période de six mois préalable à la décision. Lorsque la menace se rapporte à l'espionnage, à l'ingérence ou à la prolifération, cette période peut aller jusqu'à neuf mois. Pour des activités liées au terrorisme ou à l'extrémisme, le délai est porté à douze mois avant la décision.

Cette nouvelle réglementation implique que le SGRS est lui aussi légalement tenu d'indiquer dans le cadre de quelle menace concrète, parmi les menaces

144 *M.B.* 18 juillet 2016.

susmentionnées, se situe sa collecte. Ceci est nouveau, en ce sens que le SGRS n'est en principe pas lié à ces sept menaces dans le cadre de son action. Toutefois, il y aura peu de changement dans la pratique, puisque le SGRS a toujours fait référence à l'une des sept menaces dans ses décisions MRD.

Enfin, il convient de signaler que lors de l'élaboration de cette réglementation, la nouvelle compétence de la VSSE et du SGRS, qui est de suivre les activités de services de renseignement étrangers sur notre territoire, n'a pas été prise en considération. Ici aussi, un délai maximum pour la prise de connaissance de métadonnées devrait être spécifié.

III.1.4. L'IDENTIFICATION D'UN DÉTENTEUR D'UNE CARTE PRÉPAYÉE

Une nouvelle méthode ordinaire a été insérée à l'article 16/2 L.R&S par la Loi du 1er septembre 2016[145] : *« § 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 prépayées 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 »*. La VSSE et le SGRS doivent – comme lors de l'identification de l'utilisateur de télécommunications ou d'un moyen de communication utilisé (voir III.1.2) – tenir un registre de toutes les identifications requises.

Cette réglementation n'est entrée en vigueur qu'à la mi-décembre 2016. Elle n'a donné lieu à aucun cas d'application concret.

III.2. LES CHIFFRES RELATIFS AUX MÉTHODES SPÉCIFIQUES ET EXCEPTIONNELLES

Entre le 1er janvier et le 31 décembre 2016, 1868 autorisations ont été accordées par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement, 1747 pour la VSSE (1558 spécifiques et 189 exceptionnelles) et 121 par le SGRS (88 spécifiques et 33 exceptionnelles). Le tableau ci-dessous établit une comparaison avec les chiffres des années précédentes.

145 *M.B.* 7 décembre 2016.

	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

Ces chiffres indiquent, d'une part un *statu quo* pour le SGRS, et d'autre part, une augmentation très sensible (de pas moins de 34 %) pour la VSSE. Mais pour véritablement établir une comparaison avec les chiffres de l'année dernière, il convient aussi de tenir compte des 'identifications ordinaires via l'opérateur', qui ne sont plus considérées comme des méthodes spécifiques depuis le 29 février 2016 (voir III.1.2).

À partir de mars 2016, pas moins de 2203 réquisitions ont été adressées à des opérateurs par la VSSE, et 216 par le SGRS. Il ressort d'une comparaison avec les chiffres de 2015 que cela équivaudrait à plus de 1700 méthodes d' 'identifications via des opérateurs' pour la VSSE, et environ 60 pour le SGRS.[146] En 2015, la VSSE n'a mis en œuvre qu'un nombre limité de ces méthodes. À peine 663 'identifications' ont été autorisées.[147] On ne peut certainement pas déduire de cette augmentation constatée pour l'année 2016 que l'assouplissement de la procédure a donné lieu à une utilisation inconsidérée de cette méthode. Les chiffres mensuels des réquisitions adressées aux opérateurs pour la période 2015-2016 démontrent, en effet, que la forte augmentation du nombre d'identifications concernait les attentats de Paris et ceux de Zaventem et de Maelbeek.

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

146 En effet, la mise en œuvre d'une méthode d'identification implique généralement plusieurs réquisitions adressées à différents opérateurs belges.

147 Le SGRS a utilisé cette méthode à 55 reprises en 2015.

III.2.1. LES AUTORISATIONS RELATIVES AU SGRS

III.2.1.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	14	7	4	2
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	0	0	0	0
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	0	0	0	0
Prise de connaissance des données d'identification de moyens de communication électroniques ; réquisition du concours d'un opérateur ; ou accès direct à des fichiers de données	66 méthodes	67 méthodes	55 méthodes	–[148]
Prise de connaissance des données d'identification d'un trafic de communications électroniques à l'aide d'un moyen technique ; ou réquisition d'un opérateur concernant le moyen ou le mode de paiement d'un utilisateur	–	–	–	12 méthodes
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	15	12	12	42
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	36	28	16	32
TOTAL	**131**[149]	**114**	**87**	**88**

148 Depuis le 29 février 2016, cette méthode est d'une part ramenée à « *l'identification ou la localisation, à l'aide d'un moyen technique, des services et des moyens de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée* », et d'autre part élargie à « *la réquisition de l'opérateur d'un réseau de communications électroniques ou d'un fournisseur d'un service de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, l'identification du moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques* » (voir à ce propos III.1.2).

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

Le nombre plus élevé de 'prises de connaissance de données d'identification' les années précédentes tient exclusivement au fait que les identifications via des opérateurs sont considérées, depuis février 2016, comme une méthode ordinaire (voir III.1.2). Une comparaison approximative avec l'année dernière révèle une légère augmentation. Mais le nombre de 'prises de connaissance de données d'appel' et le nombre de 'localisations' ont connu une croissance beaucoup plus forte : ils ont respectivement triplé et doublé ! La durée moyenne des localisations a elle aussi sensiblement augmenté (de 164 à 201 jours).

Ces chiffres montrent que la tendance observée en 2014 et 2015, à savoir une utilisation moins fréquente d'identifications et de localisations, ne s'est pas poursuivie.

III.2.1.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	1	1	3	1
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	0	1	0	0
Création ou recours à une personne morale fictive	0	0	0	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	0	0	0	1
Collecte de données concernant des comptes bancaires et des transactions bancaires	5	5	3	11
Intrusion dans un système informatique	0	03	3	4
Écoute, prise de connaissance et enregistrement de communications	17	26	25	16
TOTAL	**23**[150]	**36**	**34**	**33**

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

En ce qui concerne les méthodes exceptionnelles, force est de constater que le nombre de mesures d'écoute a chuté, tandis que les données bancaires ont fait l'objet de nombreuses demandes.

III.2.1.3. Les intérêts et les menaces justifiant le recours aux méthodes particulières[151]

Depuis l'entrée en vigueur de la Loi du 29 janvier 2016 concernant le contrôle des activités des services de renseignement étrangers en Belgique (voir III.1.1), le SGRS est autorisé à utiliser les méthodes spécifiques et exceptionnelles dans le cadre de quatre (et non plus trois) missions :

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

NATURE DE LA MISSION	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
Mission de renseignement	111	109	112	64
Sécurité militaire	15	5	6	1
Protection de secrets	28	36	4	1
Suivi des activités des services étrangers en Belgique	–	–	–	chiffre non connu

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

NATURE DE LA MENACE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
Espionnage	94	123	101	55
Terrorisme (et processus de radicalisation)	6	7	4	5
Extrémisme	24	15	13	6
Ingérence	1	0	4	0
Organisations criminelles	16	2	0	0
Autre	13	0	0	0

Bien que le nombre de méthodes soit resté identique, les chiffres relatifs à la 'nature de la mission' et à la 'nature de la menace' connaissent une baisse sensible. Ce phénomène s'explique uniquement par l'utilisation d'une autre méthode d'enregistrement. Les chiffres absolus baissent considérablement, mais les proportions sont pratiquement restées les mêmes. En ce qui concerne la mise en œuvre de méthodes particulières, l'espionnage demeure la principale menace pour le SGRS.

III.2.2. LES AUTORISATIONS RELATIVES À LA VSSE

III.2.2.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	109	86	86	125
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	0	0	0	0
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	0	0	0	0
Prise de connaissance des données d'identification de moyens de communication électroniques ; réquisition du concours d'un opérateur ; ou accès direct à des fichiers de données	613 méthodes	554 méthodes	663	–[152]

[152] Depuis le 29 février 2016, cette méthode est d'une part ramenée à « *l'identification ou la localisation, à l'aide d'un moyen technique, des services et des moyens de communication électronique auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée* », et d'autre part élargie à « *la réquisition de l'opérateur d'un réseau de communications électroniques ou d'un fournisseur d'un service de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, l'identification du moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques* » (voir à ce propos III.1.2).

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
Prise de connaissance des données d'identification d'un trafic de communications électroniques à l'aide d'un moyen technique ; ou réquisition d'un opérateur concernant le moyen ou le mode de paiement d'un utilisateur	–	–	–	215 méthodes
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	136	88	33	622
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	244	248	361	596
TOTAL	**1102**	**976**	**1143**	**1558**

Il avait déjà été signalé que le nombre global d'autorisations relatives à la mise en œuvre de méthodes spécifiques par la VSSE avait connu une hausse fulgurante. Le tableau ci-dessus montre clairement que la 'prise de connaissance de données d'appel' explique presqu'à elle seule cette tendance (on est passé de seulement 33 cas en 2015 à 622 cas en 2016). Mais le nombre d''observations' et de 'localisations' a lui aussi augmenté. Enfin, les 'identifications', qui, depuis février 2016, sont considérées comme des méthodes ordinaires si elles se font via un opérateur, ont connu une forte croissance. Sur base des données disponibles, le Comité estime le nombre d'identifications mises en œuvre à plus de 1700.

L'augmentation considérable du nombre de méthodes spécifiques mises en œuvre coïncide évidemment avec la vague d'attentats terroristes.

III.2.2.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	6	9	6	7
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	6	21	8	18
Création ou recours à une personne morale fictive	0	0	0	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	6	18	5	8

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
Collecte de données concernant des comptes bancaires et des transactions bancaires	11	8	6	6
Intrusion dans un système informatique	12	18	16	27
Écoute, prise de connaissance et enregistrement de communications	81	86	87	123
TOTAL	**122**[151]	**156**	**128**	

Les multiples attentats qui ont été commis en Belgique et à l'étranger ont inversé la tendance en matière d'utilisation des méthodes exceptionnelles. Ainsi, le nombre de ces méthodes, qui avait diminué en 2015, a connu une forte augmentation en 2016. Cette tendance s'observe surtout au niveau des 'inspections' (de 9 à 22), des 'intrusions dans des systèmes informatiques' (de 16 à 27) et des 'mesures d'écoute' (de 87 à 123). Non seulement il y a eu davantage de méthodes, mais leur durée moyenne a elle aussi considérablement augmenté.

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

Le tableau suivant reprend les menaces (potentielles) dans le cadre desquelles la VSSE a accordé des autorisations spécifiques et exceptionnelles. Une méthode 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). En 2016, les méthodes exceptionnelles ne pouvaient pas être mises en œuvre dans le cadre de l'extrémisme ni de l'ingérence (mais c'est possible depuis 2017). Elles sont toutefois autorisées dans le cadre du processus de radicalisation menant au terrorisme (art. 3, 15° L.R&S). La loi définit les diverses notions comme suit :

1. l'espionnage : le recueil ou la livraison d'informations non accessibles au public, et le fait d'entretenir des intelligences de nature à les préparer ou à les faciliter ;
2. le terrorisme : le recours à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d'atteindre ses objectifs par la terreur, l'intimidation ou les menaces.
   Processus de radicalisation : un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes ;

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

3. le 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 ;
4. 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 ;
5. 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 ;
6. 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 ;
7. l'ingérence : la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins ;
8. les organisations criminelles, c'est-à-dire toute association structurée de plus de deux personnes, établie dans le temps, en vue de commettre de façon concertée des crimes et délits, pour obtenir, directement ou indirectement, des avantages patrimoniaux, en utilisant l'intimidation, la menace, la violence, des manœuvres frauduleuses ou la corruption ou en recourant à des structures commerciales ou autres pour dissimuler ou faciliter la réalisation des infractions. Sont visées dans ce cadre les formes et structures des organisations criminelles qui se rapportent intrinsèquement aux activités visées dans des menaces précédentes ou qui peuvent avoir des conséquences déstabilisantes sur le plan politique ou socio-économique.

Depuis l'entrée en vigueur de la Loi du 29 janvier 2016 concernant le contrôle des activités des services de renseignement étrangers en Belgique (voir III.1.1), la VSSE peut également mettre en œuvre les méthodes spécifiques et exceptionnelles pour « *rechercher, analyser et traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge* » (art. 7, 3/1° L.R&S).

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

NATURE DE LA MENACE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
Espionnage	359	319	253	209
Terrorisme (et processus de radicalisation)	580	499	812	684
Extrémisme	246	267	171	67
Proliferation	15	33	30	6
Organisations sectaires nuisibles	9	0	0	0
Ingérence	8	10	10	15
Organisations criminelles	9	8	0	0
Suivi des activités des services étrangers en Belgique[154]	–	–	–	chiffre non connu

Les chiffres repris ci-dessus montrent que le 'terrorisme', en ce qui concerne la mise en œuvre de méthodes 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 :

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

En considérant que plusieurs menaces peuvent figurer dans une même autorisation, les chiffres sont les suivants pour l'année 2016 :

154 Cette compétence a été insérée par la Loi du 29 janvier 2016 (voir III.1.1).

INTÉRÊTS PROTÉGÉS	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel	1177	1100	1258	968
La sûreté extérieure de l'État et les relations internationales	1160	1075	1150	927
La sauvegarde des éléments essentiels du potentiel économique et scientifique	11	10	4	13

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

III.3.1. LES CHIFFRES

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

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

- d'initiative ;
- à la demande de la Commission de la protection de la vie privée ;
- par le dépôt d'une plainte d'un citoyen ;
- de plein droit, chaque fois que la Commission BIM a suspendu une méthode spécifique ou exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données ;
- de plein droit, quand le ministre compétent a donné son autorisation sur base de l'article 18/10, § 3 L.R&S.

Par ailleurs, le Comité peut aussi être saisi en sa qualité d''auteur d'avis préjudiciels' (articles 131*bis*, 189*quater* et 279*bis* CIC). Le Comité rend, le cas échéant, un avis sur la légalité des méthodes spécifiques ou exceptionnelles ayant fourni des renseignements qui sont utilisés dans le cadre d'une affaire pénale. Les demandes d'avis sont introduites par les juridictions d'instruction ou par les juridictions de fond. Le Comité n'intervient pas alors *stricto sensu* comme un organe juridictionnel.

TYPE DE SAISINE	NOMBRE 2013	NOMBRE 2014	NOMBRE 2015	NOMBRE 2016
1. D'initiative	16	13[155]	16	3
2. Commission Vie Privée	0	0	0	0
3. Plainte	0	0	0	1
4. Suspension par la Commission BIM	5	5	11[156]	[19]
5. Autorisation du ministre	2	1	0	0
6. Auteur d'avis préjudiciel	0	0	0	0
TOTAL	**23**	**19**	**27**	**23**

Une évolution singulière ressort de ce tableau : le Comité permanent R s'est saisi dans nettement moins de cas, certainement compte tenu de l'augmentation du nombre de méthodes particulières de renseignement. Ainsi, en 2015, le Comité se saisissait encore de 1,1 % des dossiers MRD, alors que le pourcentage est resté limité à 0,15 % en 2016. Une des raisons expliquant cette diminution est que le contrôle *prima facie*, qui est effectué au sein du Comité pour chaque dossier MRD, montre que les deux services de renseignement prennent en considération, comme il se doit, les limites de la loi, les décisions de la Commission BIM et la jurisprudence du Comité. L'autre raison est le fait que la Commission BIM a suspendu plus souvent les méthodes problématiques (19 cas). Comme le montre le tableau ci-après, le Comité a néanmoins annulé (partiellement), dans 11 des 19 cas, la suspension prononcée par la Commission.

Il est en outre intéressant de mentionner la plainte déposée par un citoyen. Pour la première fois depuis l'introduction de cette possibilité en 2010, une plainte a donné lieu à une décision du Comité. Vu l'intérêt qu'il présente, ce cas sera développé (voir ci-après).

Une fois saisi, le Comité peut prendre plusieurs types de décisions (intermédiaires). Les décisions intermédiaires sont reprises aux points 3 à 10, et les décisions finales, des 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. décider de ne pas donner suite à une plainte qui est manifestement non fondée (art. 43/4, alinéa 1er, L.R&S) ;
3. suspendre la méthode contestée dans l'attente d'une décision définitive (art. 43/4, dernier alinéa, L.R&S) ;
4. demander des informations complémentaires à la Commission BIM (43/5 § 1er, alinéa 1er et alinéa 3, L.R&S) ;

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

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

5. demander des informations complémentaires au service de renseignement concerné (43/5 § 1er, alinéa 3, L.R&S) ;
6. ordonner une mission d'enquête pour le service d'Enquêtes R (art.43/5 § 2, L.R&S). Dans cette rubrique, il n'y a aucune référence aux multiples informations complémentaires recueillies par le service d'Enquêtes R avant la saisine proprement dite et donc d'une manière plutôt informelle ;
7. procéder à l'audition des membres de la Commission BIM (art. 43/5 § 4, alinéa 1er, L.R&S) ;
8. procéder à l'audition du dirigeant du service de renseignement ou des membres du service de renseignement concerné (art. 43/5 § 4, alinéa 1er, L.R&S) ;
9. statuer sur les secrets relatifs à une information ou instruction judiciaire en cours dont les membres des services de renseignement sont dépositaires, après concertation avec le magistrat compétent (art. 43/5 § 4, alinéa 2, L.R&S) ;
10. pour le président du Comité permanent R, statuer sur la demande du dirigeant du service ou le membre du service de renseignement qui estime devoir garder le secret dont il est dépositaire parce que sa divulgation est de nature à porter préjudice à la protection des sources, à la protection de la vie privée de tiers ou à l'accomplissement des missions du service de renseignement (art. 43/5 § 4, alinéa 3, L.R&S) ;
11. mettre fin à la méthode concernée si celle-ci est toujours en cours ou si elle a été suspendue par la Commission BIM, et interdire l'exploitation des données recueillies grâce à cette méthode et leur destruction (art. 43/6 § 1er, alinéa 1er, L.R&S) ;
12. mettre fin partiellement à une méthode autorisée. Il est question ici, par exemple, d'une situation où une méthode est limitée dans le temps, pas d'une situation où une seule autorisation d'un dirigeant du service autorise plusieurs méthodes et où le Comité ne met fin qu'à une seule d'entre elles ;
13. lever totalement ou partiellement la suspension et l'interdiction qui ont été décidées par la Commission BIM (art. 43/6 § 1er, alinéa 1er, L.R&S), ce qui implique que la méthode autorisée par le dirigeant du service a bien été considérée par le Comité comme (partiellement) légale, proportionnelle et subsidiaire ;
14. constater la non-compétence du Comité permanent R ;
15. déclarer le caractère infondé de l'affaire pendante et permettre la poursuite de la méthode ;
16. délivrer un avis préjudiciel (articles 131*bis*, 189*quater* et 279*bis* CIC).

Le Comité permanent R doit statuer définitivement dans un délai d'un mois suivant la date à laquelle il a été saisi (art. 43/4 L.R&S). À l'exception du dossier de plainte (l'affaire a dû être ajournée), ce délai a toujours été respecté.

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

III.3.2. LA JURISPRUDENCE

La substance des décisions finales prises par le Comité permanent R en 2016 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 ici de la prudence requise, puisque de nombreuses décisions ont été classifiées (seize au niveau CONFIDENTIEL et quatre au niveau SECRET).

Les décisions ont été regroupées en cinq rubriques :

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

Certaines décisions ont été reprises dans plusieurs rubriques lorsque cela s'avérait pertinent.

III.3.2.1. Motivation de l'autorisation

Dans quatre dossiers distincts, le Comité a dû décider si une autorisation d'exécution d'une méthode était suffisamment motivée, et ce aussi bien en fait qu'en droit.

Dans le premier dossier, un service de renseignement voulait procéder à la prise de connaissance des « *données de connexion du passé (dont notamment des adresses IP) sur des comptes [d'un réseau social] utilisés par un target et que la période était limitée à 90 jours précédents la notification à la Commission BIM* » (dossier 2016/4542). La qualification retenue par le service de renseignement était une prise de connaissance de données d'appel. Le Comité a fait remarquer que « *les méthodes s'apparentent plus à une localisation de l'origine ou de la destination de communications électroniques qu'à une identification et un repérage (…) ; que cependant la localisation est également une méthode spécifique dont les conditions sont identiques à celles applicables à l'identification et au repérage et qu'en conséquence le changement (éventuel) de « qualification » n'a pas d'incidence en terme de légalité* ». La méthode n'était donc pas illégale.

Dans le deuxième dossier, la 'motivation en fait' a été évaluée. Un service de renseignement étranger avait demandé à son service partenaire belge d'effectuer une prise de connaissance et une localisation sur des numéros de téléphone belges à partir desquels des menaces de mort auraient été proférées à deux reprises contre des dignitaires. La Commission BIM a suspendu la méthode parce que le texte et l'esprit de la Loi MRD imposent que des indications plus précises soient reprises dans la décision sur le lien avec le 'terrorisme' comme l'une des menaces à suivre (dossier 2016/4707). Le Comité a demandé un complément d'informations à ce sujet au service belge. Le lien avec le terrorisme n'en est pas directement ressorti. Mais le Comité a établi que « *dans les circonstances actuelles, des menaces de mort adressées par deux fois à des*

personnes proches du gouvernement […] d'un pays européen, même si à ce stade, celles-ci ne sont pas très caractérisées, peuvent être considérées comme relevant du « terrorisme » au sens de l'article 8-1° al 2 – b ».

Dans un autre dossier, l'intention précise du service de renseignement n'était pas claire. Se référant à l'article 18/16 L.R&S, un service de renseignement voulait placer un logiciel dans un appareil de communication pour se faire une idée de la nature des communications et pour écouter des conversations (dossier 2016/5365). Étant donné que l'écoute de conversations relève de l'article 18/17 L.R&S, des explications complémentaires ont été demandées au service concerné. Il est apparu que l'intention n'était *pas* de procéder effectivement à des écoutes. Par conséquent, le Comité a décidé que la méthode *« wettig is, VOOR ZOVER de beoogde methode niet het afluisteren, kennisnemen of registreren van communicaties op het oog heeft ».*[157]

Le dernier cas concernait la demande d'un service belge de pouvoir suivre un groupe d'étrangers qui séjournaient en Belgique (dossiers 2016/4875 et 2016/4877). Ces personnes, qui occupaient ou avaient occupé une fonction importante dans leur pays d'origine, étaient supposées être membres d'un mouvement déterminé. Dans sa décision, le service de renseignement se fondait sur la menace 'ingérence' et exposait les motifs qui montraient l'intérêt pour le service de les suivre. Insuffisant pour la Commission BIM et le Comité : *« Attendu qu'il échet de constater que, aussi bien la menace identifiée que les motifs sont loin d'être exposés d'une manière optimale puisque, par exemple [l'organisation dont dépend le groupe] est décrite comme une organisation sectaire en faisant simplement référence à une étude réalisée à l'étranger et que l'ingérence (réelle ou potentielle) n'est pas caractérisée à suffisance à défaut d'identifier les moyens illicites trompeurs ou clandestins ».* C'est pourquoi le Comité a demandé un complément d'informations. *« Attendu qu'à l'issue d'une enquête complémentaire, le Comité permanent R n'a, en principe, pas à substituer une motivation plus adéquate de la méthode sollicitée à la motivation insuffisamment étayée du service ; que cependant dans le cas d'espèce, et vu notamment que [l'organisation] constitue un mouvement […] qui tente de s'installer en Europe occidentale et entre autres en Belgique et qui est relativement récent et donc moins connu que d'autres mouvements [similaires], le Comité permanent R a décidé de demander des informations complémentaires. Celles-ci l'amènent à considérer que la méthode spécifique peut-être autorisée ».* En effet, il y avait suffisamment d'éléments disponibles pointant non seulement l''ingérence' mais aussi l''extrémisme'. *« Attendu en conséquence que la méthode est légale pour les motifs tels que requalifiés ».*

157 *« est légale, POUR AUTANT que la méthode visée n'ait pas pour objectif l'écoute, la prise de connaissance ou l'enregistrement de communications »* (traduction libre).

III.3.2.2. L'exigence de proportionnalité et de subsidiarité

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

L'analyse de ces exigences de proportionnalité et de subsidiarité était traitée dans le dossier 2016/4707 susmentionné. Un service de renseignement étranger avait demandé à son service partenaire belge d'effectuer une prise de connaissance et une localisation sur des numéros de téléphone belges à partir desquels des menaces de mort auraient été proférées à deux reprises contre des membres d'un gouvernement étranger. Le Comité a établi que « *la méthode projetée devrait permettre d'objectiver les menaces puisque les méthodes ordinaires ne sont pas suffisantes et que la méthode en question a un caractère limité d'intrusion dans la vie privée de personnes; Attendu que l'éventuelle décision de recours à d'autres méthodes concernant ces numéros de GSM ou leurs utilisateurs devra préciser plus amplement en quoi les menaces ont un caractère terroriste; Attendu en conséquence que la méthode spécifique visée est légale en ce compris le principe de proportionnalité et de subsidiarité* ».

La question de la proportionnalité a également été abordée dans le dossier 2016/4785. Un service de renseignement entendait repérer des données d'appel d'un moyen de communication de son *target*, mais aussi de plusieurs membres de sa famille. Vu les motivations données et les informations fournies, la méthode s'avérait justifiée à l'égard du *target*. « *Dat evenwel het opsporen van de oproepgegevens van de […] familieleden gemotiveerd wordt door de mogelijkheid dat de target een telefoontoestel van één van zijn familieleden kan gebruiken* ».[158] Le service concerné, interrogé à ce propos, a indiqué ne pas disposer d'indications concrètes selon lesquelles le *target* utiliserait les appareils téléphoniques des membres de sa famille. Par conséquent, le Comité a estimé que l'usage de la méthode visée à l'égard de l'entourage familial n'était pas proportionnel.

III.3.2.3. Légalité de la méthode concernant les techniques utilisées, les données recueillies, la durée de la mesure et la nature de la menace

Les services de renseignement ne peuvent évidemment pas employer n'importe quelle technique en vue de recueillir des informations auprès de quiconque. La loi pose des limites claires à différents niveaux : pour quelle menace et pour la protection de quel intérêt une méthode peut-elle être utilisée ? Quels actes peuvent être posés et quels actes ne le peuvent pas ? Par qui, pour quelles données ? Combien de temps une technique peut-elle être utilisée ? Les mesures

158 « *Que, toutefois, le repérage des données d'appel des membres de la famille […] est motivé par l'éventualité que le target puisse utiliser l'appareil téléphonique d'un membre de sa famille* » (traduction libre).

peuvent-elles être appliquées en dehors de la Belgique ?… Le Comité permanent R a précisé ces limites dans quelques décisions.

III.3.2.3.1. Une finalité de renseignement mais pas une finalité judiciaire

La Commission BIM avait suspendu une méthode parce que le service de renseignement avait fait remarquer dans sa décision que les résultats des méthodes *« dienen om het inlichtingendossier (…) af te ronden zodat deze kunnen toegevoegd worden aan een ander lopende gerechtelijk onderzoek (…) waarbij de VSSE technisch assistent is »*[159] (dossier 2016/4414). La Commission BIM a établi, à juste titre, qu'il n'incombe pas à un service de renseignement de récolter des renseignements devant servir à étoffer un dossier judiciaire. Le Comité a toutefois demandé des explications au service concerné, mais a jugé la motivation trop sommaire. Il est ressorti des informations fournies que l'objectif était d'avoir une vue sur un réseau défini. La méthode a été considérée comme légale, vu que le service avait bien à l'esprit une finalité de renseignement.

III.3.2.3.2. Les limites des missions des services de renseignement

Le service de renseignement souhaitait retracer le moyen de communication utilisé par un groupe pour pouvoir ensuite localiser les personnes (dossier 2016/4633) et les observer (dossier 2016/4634). Il s'agissait de personnes qui faisaient partie d'un mouvement politique d'opposition et qui avaient demandé le statut de réfugié en Belgique. Le service était d'avis que ce mouvement politique *« de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, alsook de uitwendige veiligheid van de staat en de internationale betrekkingen bedreigt of zou kunnen bedreigen »*.[160] Le Comité a fait remarquer que le service se référait bien à un intérêt devant être protégé, mais que nulle part dans la décision une activité menaçante (espionnage, ingérence, terrorisme, extrémisme, prolifération, organisations sectaires nuisibles, organisations criminelles) n'était suffisamment établie, à l'exception d'une seule mention selon laquelle le groupement concerné usait de 'pratiques sectaires'. La décision mentionnait toutefois que l'organisation était soupçonnée *« van te pogen het […] staatsapparaat [van hun land van herkomst] binnen te dringen »*[161], et d'autre part, que l'organisation tentait d'exercer une influence tant sur la diaspora que sur les responsables politiques belges. Le Comité a jugé

159 *« servent à (…) clôturer le dossier de renseignement de telle sorte qu'ils puissent être annexés à une autre enquête judiciaire en cours (…,) dans laquelle la VSSE prête une assistance technique »* (traduction libre).

160 *« menace ou pourrait menacer la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel ainsi que la sûreté extérieure de l'État et les relations internationales »* (traduction libre).

161 *« de tenter de s'introduire dans l'appareil d'État […] [de leur pays d'origine] »* (traduction libre).

« dat deze motivering geenszins voldoet aan de definitie van inmenging, nu volgens de wet inmenging het volgende inhoudt : « de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden ».[162] Le service n'était donc pas compétent pour récolter des renseignements dans cette affaire.

III.3.2.3.3. Les limites de la méthode visant à réclamer des données bancaires

Le service de renseignement concerné souhaitait retrouver le titulaire d'un numéro de compte bancaire (dossier 2016/4688). Quand le service a appris que cette personne avait effectué un versement sur le compte d'une société, il a voulu vérifier, pendant une période déterminée, tous les versements effectués sur le compte bancaire de la société. Il se fonde pour cela sur l'article 18/15 § 1er L.R&S : *« Dans l'intérêt de l'exercice de leurs missions, les services de renseignement et de sécurité peuvent être autorisés à solliciter les renseignements suivants : 1° la liste des comptes bancaires (…) dont la personne visée est le titulaire, le mandataire ou le véritable bénéficiaire, et, le cas échéant, toutes les données à ce sujet ; 2° les transactions bancaires qui ont été réalisées, pendant une période déterminée, sur un ou plusieurs de ces comptes bancaires ou instruments financiers, y compris les informations concernant tout compte émetteur ou récepteur »*. Le Comité a attiré l'attention sur le fait que cette disposition ne permet pas de réclamer des données bancaires d'un tiers. Ce n'est autorisé qu'à l'égard de *« la personne visée »*. Le Comité a donc décidé que *« aldus de wet niet toelaat dat een bankrekening van een derde (in casu de firma) wordt onderzocht, om uiteindelijk de geviseerde persoon te identificeren »*.[163]

III.3.2.3.4. Imprécision sur la durée de la méthode

Dans la décision d'utiliser une méthode spécifique, il était d'une part mentionné qu'elle pouvait être mise en œuvre *« voor de periode vanaf [welbepaalde datum] tot en met [welbepaalde datum] »*[164], et d'autre part, qu'elle *« kan worden uitgevoerd gedurende drie maanden vanaf de beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie »*.[165] En d'autres termes, les dates de début et de fin n'étaient pas précisées. Le Comité a conclu que la date de début coïncidait avec le jour où la Commission a été informée. En outre, le

---

162 *« que cette motivation ne répond aucunement à la définition de l'ingérence, or la loi définit l'ingérence comme suit : « la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins »* (traduction libre).

163 *« la loi ne permet pas qu'un compte bancaire d'un tiers (en l'occurrence la société) soit examiné pour, in fine, identifier la personne visée »* (traduction libre).

164 *« pour la période à compter du [date déterminée] à [date déterminée] incluse »* (traduction libre).

165 *« peut être exécutée durant trois mois à compter de la décision du dirigeant du service et après la communication de cette décision à la commission »* (traduction libre).

Comité a établi qu'en cas de « *tegenstrijdigheid van data voor de kortste periode dient te worden gekozen* »[166] (dossier 2016/4515).

III.3.2.3.5. L'estimation du nouveau délai visé à l'article 18/8 L.R&S

Dans le cadre d'une éventuelle affaire d'espionnage, un service de renseignement a décidé à un moment donné de procéder, via un opérateur, à la prise de connaissance de données d'appel pour une période de neuf mois entièrement préalable à la demande (dossier 2016/5266). À ce moment-là, l'article 18/8 L.R&S en question était modifié dans le sens où pour cette menace « *le dirigeant du service peut dans sa décision requérir les données pour une période de neuf mois préalable à la décision* » [nous soulignons]. Le Comité a dès lors établi que « *sous peine de vider le texte de sa portée, le terme 'préalable' ['voorafgaand' dans la version néerlandaise, ndlr] doit être compris comme instituant la date de décision […] comme un point de départ non inclus dans le calcul du délai légal visé* ». Cela signifiait dans le cas présent que la méthode portait sur une période excédant d'un jour la période autorisée.

III.3.2.3.6. Une réquisition incomplète

Le Comité a dû intervenir dans deux dossiers car la réquisition adressée aux opérateurs s'avérait incomplète.

Ainsi, un service de renseignement souhaitait obtenir des données d'appel pour une période de 90 jours (dossier 2016/4542). Cette limitation n'était pas mentionnée dans la réquisition envoyée au fournisseur. Le service de renseignement estimait, en effet, que le fournisseur concerné ne conservait ces données que 90 jours. Il est apparu que ce n'était pas le cas : le service a reçu les données pour une année entière. Même si le service a fait savoir qu'il n'utiliserait pas ces données, la Commission BIM a suspendu la méthode, et le Comité a décidé que la méthode était en partie illégale.

Dans une autre affaire, un service de renseignement disposait de numéros de téléphone étrangers appartenant à des personnes qui étaient liées à un groupement terroriste (dossier 2016/4838). En procédant à une prise de connaissance de données et à une localisation de données d'appel, il souhaitait découvrir si ces personnes, au cours d'un mois déterminé, avaient eu des contacts en Belgique. Mais la réquisition de l'opérateur ne mentionnait pas que la méthode était limitée à des 'contacts belges'. La Commission a donc suspendu la méthode. Le Comité a examiné le cas et a constaté que l'opérateur avait transmis toutes les informations en sa possession. Aucune de ces données ne concernait un numéro belge ou un contact qui pouvait être situé en Belgique. Aussi le Comité a-t-il pris la décision suivante : « *Attendu que les*

166 « *contradiction de dates, il convient de choisir la période la plus courte* » (traduction libre).

méthodes sont légales dans la mesure où elles visent les contacts en Belgique de numéros étrangers utilisés à l'étranger; Attendu que cependant l'exécution des méthodes est illégale dans la mesure où le réquisitoire transmis à l'opérateur n'est pas conforme à la décision […] puisqu'il n'est pas limité aux contacts belges ».

III.3.2.3.7. La Loi MRD et la Convention de Vienne du 18 avril 1961 sur les relations diplomatiques

Un service de renseignement voulait mettre en œuvre plusieurs méthodes portant sur des intérêts qui tombaient dans le champ d'application de la Convention de Vienne de 1961 (dossier 2016/4458). La Commission BIM a suspendu les méthodes, une décision confirmée par le Comité.

Le Comité permanent R s'est saisi dans deux autres cas (2016/5147 et 2016/5259) pour vérifier si la méthode utilisée était conforme au principe de légalité, et plus précisément à la Convention de Vienne. L'examen a montré que les méthodes (ou une partie de celles-ci) portaient sur des données qui entraient dans les 'périmètres inviolables' explicités par le Comité dans sa jurisprudence (dossier 2014/3148). De plus, le Comité a rappelé qu'il avait signalé à ce moment-là une absence de directives en la matière du Comité ministériel du renseignement et de la sécurité (qui est devenu le Conseil national de sécurité). Par ailleurs, dans le dossier 2016/5259, le Comité a constaté que de telles directives n'étaient pas encore disponibles. Il a ajouté ici le motif suivant: « *Overwegende dat het Vast Comité I, en deze keer met aandrang, herhaalt dat in dergelijke omstandigheden geen methode ten aanzien van [bepaalde aspecten] die vallen onder de Conventie van Wenen van 1961 kunnen worden toegelaten* ».[167, 168]

III.3.2.4. Les conséquences d'une méthode (mise en œuvre) illégale(ment)

En raison de l'extrême urgence, le dirigeant d'un service a autorisé oralement une méthode spécifique dans sept cas similaires (dossiers 2016/4490 à 2016/4496 inclus). La confirmation écrite n'a suivi que plus d'un mois et demi plus tard. Vu que l'article 18/7 § 2 impose que « *cette décision verbale est confirmée dans les plus brefs délais par une décision écrite motivée du dirigeant du service* », la Commission BIM a suspendu la méthode. Le Comité n'a pas suivi cette décision pour les raisons suivantes: « *Attendu qu'il échet de constater que la loi n'a pas prévu explicitement de sanctions en cas du non-respect de cette exigence; Attendu*

---

167 *'Attendu que le Comité permanent R rappelle, cette fois avec insistance, que dans de telles circonstances aucune méthode ne peut être autorisée au regard de [certains aspects] qui relèvent de la Convention de Vienne de 1961'* (traduction libre).

168 Le Comité a invité les Cabinets du Premier ministre, de la Justice et de la Défense pour mener une discussion approfondie sur la problématique. Chaque partie a pu développer son point de vue et exprimer ses préoccupations lors de cette réunion de travail.

que le Comité permanent R a déjà antérieurement émis un avis selon lequel la procédure d'extrême urgence devait être améliorée; Attendu qu'il ne fait pas de doute que la loi n'a pas été respectée en ce qui concerne la confirmation écrite de la réquisition qui doit être faite dans les plus brefs délais, selon les termes de la loi, mais que, par ailleurs, le Comité permanent R doit prendre attitude sur les conséquences du non-respect de cette condition formelle; Attendu que le retard mis par [le service de renseignement] à confirmer, par écrit, la réquisition verbale trouve son explication dans les circonstances de faits, dans lesquels la méthode a été mise en œuvre; Attendu que l'irrégularité formelle constatée n'affecte pas la fiabilité des informations recueillies et qu'elle n'a pas de plus entraîné de violation des droits fondamentaux des personnes faisant l'objet de la méthode; Que le comité se réfère dans sa décision à la jurisprudence « Antigone » qui a amené le législateur à insérer un art. 32 dans le titre préliminaire du Code de Procédure pénale ainsi que la jurisprudence en droit administratif dans certains cas de non-respect des formes et des procédures ».

III.3.2.5. La décision juridictionnelle relative à la plainte

Le plaignant était poursuivi pour des faits de terrorisme. Dans le dossier pénal, il a découvert des éléments indiquant qu'il était suivi à l'époque par la VSSE. Ainsi, le dossier contenait notamment des photos du requérant. Il souhaitait savoir si la VSSE avait agi dans la légalité en utilisant, selon lui, des méthodes spécifiques de renseignement.

Diverses questions préjudicielles ont été abordées dans cette affaire. Vu que ces questions peuvent constituer un précédent, elles sont détaillées ci-dessous.

III.3.2.5.1. Demande d'introduction de questions préjudicielles

Le requérant souhaitait en premier lieu que le Comité permanent R, en sa qualité d'organe juridictionnel, pose une série de questions préjudicielles à la Cour constitutionnelle sur base de l'article 26 § 2, alinéa 2, Loi spéciale sur la Cour constitutionnelle[169] ou – si le Comité n'y donnait pas suite – à la Cour de Justice

[169] *« Schenden de bepalingen van hoofdstuk IV/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen-en veiligheidsdienst de artikelen 10 en 11 van de grondwet in die zin dat de a posteriori controle van de inlichtingendiensten, zoals in casu de observatie met een technisch hulpmiddel, enkel gebeurt op verzoek van de rechtsonderhorige en niet op automatische wijze en dat hiervoor een aparte klacht ingediend moet worden, terwijl de controle door de kamer van inbeschuldigingstelling van de bijzondere opsporingsmethoden, zoals een observatie met een technisch hulpmiddel, overeenkomstig artikel 235 ter van het Wetboek van strafvordering steeds gebeurt wanneer de onderzoeksrechter zijn dossier aan de Procureur des Konings overzendt krachtens artikel 127 § 1, lid 1 van het Wetboek van strafvordering ». « Viole les dispositions du chapitre IV/2 de la loi du 30 novembre organique des services de renseignement et de sécurité, les articles 10 et 11 de la Constitution, en ce sens que le contrôle a posteriori des services de renseignement, comme dans ce cas-ci l'observation à l'aide d'un moyen technique, ne peut être exercé qu'à la demande du justiciable et n'est pas automatique, et qu'à*

de l'Union européenne établie au Luxembourg.[170] Le Comité, qui intervient en la matière comme une juridiction et est donc, en principe, en mesure de soumettre des questions préjudicielles à la Cour constitutionnelle, a estimé qu'il ne devait pas accéder à cette demande.

En ce qui concerne la première question, le Comité se réfère aux éléments suivants :

– contrairement à ce qu'affirmait le plaignant, le contrôle est exercé sur *chaque* méthode particulière de renseignement, de matière automatique et sans exception, d'abord par la Commission BIM et ensuite par le Comité permanent R ;
– en 2010, une demande d'annulation partielle ou totale des dispositions également avancées par le plaignant avait déjà été rejetée la Cour

---

cet effet, une plainte distincte doit être introduite, alors que le contrôle des méthodes particulières de recherche par la chambre des mises en accusation, comme une observation à l'aide d'un moyen technique, conformément à l'article 235ter du Code d'instruction criminelle, est toujours exercé lorsque le juge d'instruction transmet son dossier au Procureur du Roi en vertu de l'article 127 § 1er, alinéa 1er du Code d'instruction criminelle » (traduction libre). Et « *Schendt artikel 43/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen-en veiligheidsdienst de artikelen 10 en 11 van de grondwet in die zin dat het niet mogelijk is voor de klager die overeenkomstig artikel 43/4 van de wet van 30 november 1998 houdende regeling van de inlichtingen-en veiligheidsdienst een klacht indiende, beroep in te stellen tegen de beslissing van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten omtrent de controle op de inlichtingenmethoden, terwijl het voor een beklaagde of inverdenkinggestelde wel mogelijk is om cassatieberoep in te stellen tegen de beslissing van de kamer van inbeschuldigingstelling omtrent de controle op de bijzondere opsporingsmethoden?* » « *Viole l'article 43/8 de la 30 novembre organique des services de renseignement et de sécurité, les articles 10 et 11 de la Constitution, en ce sens qu'il n'est pas possible pour le plaignant qui, conformément à l'article 43/4 de la loi du 30 novembre organique des services de renseignement et de sécurité, a introduit une plainte, d'introduire un recours contre la décision du Comité permanent de Contrôle des services de renseignement et de sécurité concernant le contrôle des méthodes particulières de renseignement, alors que pour un prévenu ou un inculpé, il est possible de se pourvoir en cassation contre la décision de la chambre des mises en accusation concernant le contrôle des méthodes particulières de recherche?* » (traduction libre).

170 « *Schendt artikel 26 van de bijzondere wet op het Grondwettelijk Hof de Verdragen en meer bepaald de artikelen 47 en 48 van het Handvest van de grondrechten van de Europese Unie in samenhang met artikel 20 van het Handvest van de grondrechten van de Europese Unie in die zin dat het een rechtsonderhorige niet mogelijk is om een prejudiciële vraag te stellen aan het Grondwettelijk Hof aangaande de schending van zijn grondrechten doordat het Vast Comité van Toezicht op de Inlichtingen- en veiligheidsdiensten geen rechtscollege zou betreffen in de zin van artikel 26 van de Bijzondere Wet op het Grondwettelijk Hof, terwijl het Vast Comité van Toezicht op de Inlichtingen- en veiligheidsdiensten wel uitspraak in enige en laatste aanleg doet over de regelmatigheid van de aangewende inlichtingen-methoden?* » « *Viole l'article 26 de la Loi spéciale sur la Cour constitutionnelle, les Conventions et plus particulièrement les articles 47 et 48 de la Charte des droits fondamentaux de l'Union européenne dans le prolongement de l'article 20 de la Charte des droits fondamentaux de l'Union européenne, en ce sens qu'il n'est pas possible pour un justiciable de poser une question à la Cour constitutionnelle concernant la violation de ses droits fondamentaux puisque le Comité permanent de Contrôle des services de renseignement et de sécurité ne constituerait pas une juridiction au sens de l'article 26 de la Loi spéciale sur la Cour constitutionnelle, alors que le Comité permanent de Contrôle des services de renseignement et de sécurité se prononce en premier et dernier ressort sur la régularité des méthodes de renseignement employées?* » (traduction libre).

constitutionnelle qui, dans son arrêt n° 145/2011 du 22 septembre 2011, établissait qu'il n'y avait, en la matière, aucune incompatibilité entre la loi de renseignement du 30 novembre 1998 et la Constitution ;
– les méthodes particulières de recherche de la police suivent une autre méthodologie et un autre parcours que ceux des méthodes particulières de renseignement. Pour chacune des méthodes, le législateur a prévu une procédure adaptée visant à protéger le justiciable. Le double contrôle pour les MRD (à savoir un contrôle *a priori* par la Commission suivi d'un contrôle *a posteriori* par le Comité) offre des garanties plus que suffisantes contre une éventuelle utilisation illégale de méthodes particulières de renseignement.

En ce qui concerne la deuxième question préjudicielle, le Comité attire notamment l'attention sur les aspects suivants :
– l'article 43/8 L.R&S stipule que les décisions du Comité ne sont susceptibles d'aucun recours. Comme indiqué ci-dessus, une demande d'annulation partielle ou totale de la Loi MRD a déjà été traitée en 2010 par la Cour constitutionnelle. C'est la raison pour laquelle, dans son arrêt, la Cour constitutionnelle se prononçait déjà dans le sens où il ne voyait pas, en la matière, d'incompatibilité entre la loi du 30 novembre 1998 et la Constitution ;
– le Comité a en outre rappelé qu'il est une juridiction *sui generis* qui ne fait pas partie du pouvoir judiciaire et qui a été instituée pour prévenir toute infraction aux droits fondamentaux des justiciables en imposant un contrôle visant à empêcher la commission d'actes illégaux par les services de renseignement. Le Comité est un organe indépendant qui offre de solides garanties d'impartialité, ce qui était d'ailleurs clairement reconnu par la Cour constitutionnelle.

Concernant la question de savoir si le Comité était obligé de poser les questions préjudicielles formulées par le plaignant à la Cour de Justice de l'Union européenne, les arguments suivants ont été développés :
– dans la question soumise au départ, le plaignant affirmait que le Comité permanent R n'était pas une juridiction. Il convenait de contredire cette affirmation, comme cela a déjà été mentionné ci-dessus. La demande du requérant qu'une question préjudicielle soit posée à la Cour européenne de Justice reposait donc sur des prémisses erronées ;
– de toute façon, il n'incombait pas non plus au Comité de se prononcer sur l'application de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle en général, et en particulier, de contrôler celle-ci en regard des dispositions conventionnelles européennes ;
– poser une question préjudicielle en la matière ne présentait absolument pas de lien avec le pouvoir juridictionnel du Comité permanent R et ne pouvait pas non plus contribuer à résoudre le différend qui se présentait, si bien qu'il n'y avait pas d'objet à la question ;

– les articles 46 et 47 mentionnés dans la Charte font d'ailleurs partie du domaine pénal et sont d'application dans les cours pénales. Cette matière n'est pas non plus du ressort du Comité permanent R et ne présente pas le moindre lien avec le pouvoir juridictionnel du Comité.

III.3.2.5.2. Effet suspensif

Le requérant demandait au Comité de conférer un effet suspensif à son contrôle, et ce à l'égard de l'utilisation de renseignements contestés dans l'affaire pénale. Le Comité a rejeté cette demande comme étant 'sans objet'. Dans la Loi sur les services de renseignement du 30 novembre 1998, il n'est question que d'une 'suspension' de la méthode, ce qui signifie la suspension de l'exécution de la méthode. Étant donné que la méthode concernée avait déjà été exécutée et clôturée en 2013, elle ne pouvait plus être suspendue.

III.3.2.5.3. Consultation des pièces du dossier

Le plaignant demandait à consulter toutes les informations sur les observations, les autorisations du dirigeant du service et la décision de la Commission BIM en la matière. Cela devait lui permettre de vérifier la légalité des méthodes de renseignement.

Le Comité a attiré l'attention sur le fait que de telles pièces, conformément à la Loi Classification du 11 décembre 1998, ne pouvaient jamais être portées à la connaissance de personnes qui ne sont pas titulaires d'une habilitation de sécurité, vu qu'il s'agit chaque fois de documents classifiés. D'ailleurs, il n'appartient pas au plaignant de demander la présentation de certains documents, alors que la loi a prévu une procédure très spécifique quant à la prise de connaissance de tous les éléments pertinents. Cette procédure est inscrite à l'article 43/5 § 3 L.R&S, où il est stipulé que le dossier « *contient tous les éléments et renseignements pertinents en la matière, à l'exception de ceux qui portent atteinte à la protection des sources, à la protection de la vie privée de tiers, aux règles de classification énoncées par la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, ou à l'accomplissement des missions des services de renseignement et de sécurité définies aux articles 7, 8 et 11* ».

Le plaignant estimait cependant qu'il ne disposait pas de suffisamment d'éléments pour être en mesure d'évaluer la proportionnalité et la subsidiarité. Il prétendait qu'il devait pouvoir consulter des informations dont la VSSE disposait avant de procéder aux observations afin de vérifier si des méthodes de renseignement ordinaires n'auraient pas pu être employées. Le Comité a signalé que l'évaluation de la proportionnalité et de la subsidiarité incombait à la Commission BIM et au Comité permanent R, qui sont les deux instances compétentes pour s'assurer du respect de ces principes.

III.3.2.5.4. Appréciation sur le fond

Le Comité estimait que les méthodes dont il était question répondaient aux principes de proportionnalité et de subsidiarité. Dans ce cas-ci, l'objectif était de constater avec certitude et objectivité que l'intéressé était en contact avec des personnes connues pour leurs idées islamistes extrémistes et/ou un lien éventuel avec la problématique syrienne. Des méthodes ordinaires étaient ici « *ontoereikend […] en het opstellen van een camera die beelden opneemt de gepaste mogelijkheid […] om de inlichtingen te verzamelen en de contacten tussen de klager en anderen vast te stellen, en dit zonder afbreuk te doen aan het tweede principe dat moet worden in acht genomen, met name de proportionaliteit* ».[171] Dans le cas présent, les menaces potentielles (c'est-à-dire le terrorisme et l'extrémisme) étaient suffisamment graves pour justifier une méthode de renseignement particulière. De plus, toutes les conditions de forme et de procédure étaient remplies.

III.3.2.5.5. Le principe de l'*ultra petita*

Si le plaignant faisait initialement référence à deux observations dans sa plainte, il l'a élargie après avoir constaté qu'il avait fait l'objet de plusieurs observations.

Le Comité permanent R a pointé le principe de l'*ultra petita*, en vertu duquel une juridiction ne peut accorder plus que ce qui était exigé. Le Comité n'a dès lors pas vu la nécessité « *buiten de controle op de inlichtingenmethoden van 3 juni 2013 en van 13 december 2013, andere mogelijke bijzondere inlichtingenmethoden aan een controle te onderwerpen. Bij de beoordeling van onderhavige klacht werd aldus een wettigheidscontrole uitgevoerd op alle inlichtingenmethoden die van toepassing waren op de klager* ».[172]

III.3.2.5.6. Destruction de données et interdiction d'exploitation

Enfin, le plaignant demandait que cesse l'exploitation des données recueillies illégalement et que celles-ci soient immédiatement détruites.

L'arrêt de l'exploitation des informations et leur destruction sont des possibilités que le législateur a offertes au Comité permanent R pour chaque méthode particulière de renseignement qui lui est soumise dans le cadre de son contrôle *a posteriori*.

---

171 « *insuffisantes […] et l'installation d'une caméra qui enregistre des images constitue le moyen adéquat pour recueillir les renseignements et constater les contacts qu'entretiennent le plaignant et d'autres personnes, et ce sans enfreindre le second principe qui doit être pris en considération, à savoir la proportionnalité* » (traduction libre).

172 « *De soumettre à un contrôle d'autres méthodes de renseignement éventuelles, en plus de celles du 3 juin 2013 et du 13 décembre 2013. Ainsi, lors de l'évaluation de la présente plainte, un contrôle de légalité de toutes les méthodes de renseignement qui s'appliquaient au plaignant a été effectué* » (traduction libre).

Le Comité permanent R a chaque fois décidé, pour chaque méthode particulière, qu'un arrêt de l'exploitation de données ou leur destruction ne s'imposait pas. Le Comité permanent R a déjà pris une décision définitive à ce propos lors de son contrôle systématique.

III.4. CONCLUSIONS ET RECOMMANDATIONS

Le Comité permanent R a formulé les conclusions et recommandations générales suivantes concernant le contrôle des méthodes particulières de renseignement :

- le nombre de méthodes particulières mises en œuvre par la VSSE a connu une croissance exponentielle, ce qui s'explique par l'augmentation des activités de renseignement à la suite des attentats de Paris et de Zaventem/Maelbeek. Ce phénomène reposait quasi exclusivement sur l'augmentation des 'prises de connaissance de données d'appel', qui sont passées de seulement 33 à 622 cas. Les méthodes exceptionnelles ont elles aussi connu une croissance considérable. Non seulement il y a eu davantage de mesures exceptionnelles, mais leur durée moyenne était aussi nettement plus longue ;
- malgré les attentats, le nombre de méthodes spécifiques et exceptionnelles mises en œuvre par le SGRS est resté assez stable ;
- le nombre de réquisitions auprès d'opérateurs pour identifier l'utilisateur d'un moyen de télécommunication (nouvel article 16/2 L.R&S) était très élevé. Mais c'était ici aussi la conséquence directe des attentats ;
- si, dans le cadre de la mise en œuvre des MRD, le SGRS se concentrait traditionnellement sur la menace 'espionnage', la VSSE a continué de se concentrer sur le 'terrorisme' ;
- alors qu'en 2015, le Comité se saisissait encore de 1,1 % des dossiers MRD, le pourcentage est resté limité à 0,15 % en 2016. Une des raisons expliquant cette diminution était que le contrôle *prima facie*, qui est effectué au sein du Comité pour chaque dossier MRD, a montré que les deux services de renseignement prennent en considération, comme il se doit, les limites de la loi, les décisions de la Commission BIM et la jurisprudence du Comité ;
- le Comité a insisté pour que, dans leurs décisions MRD, la VSSE et le SGRS puissent se référer explicitement, le cas échéant, à la nouvelle compétence pour suivre les activités de services de renseignement étrangers sur le territoire belge (voir III.1.1) ;
- lors de l'élaboration de la réglementation portant sur la réquisition d'opérateurs (voir III.1.3), la nouvelle compétence de la VSSE et du SGRS qui consiste à suivre les activités de services de renseignement étrangers sur le territoire belge n'a pas été prise en considération. Le Comité a recommandé que le législateur fixe ici aussi un délai maximum pour la prise de connaissance de métadonnées.

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

Depuis le début de l'année 2011, la VSSE et le SGRS peuvent tous deux, dans des conditions très strictes, écouter des communications, en prendre connaissance et les enregistrer (art. 18/17, § 1er L.R&S).

Les 'interceptions MRD'[173] doivent cependant être clairement distinguées de *« la recherche, la captation, l'écoute, la prise de connaissance ou l'enregistrement, par le Service Général du Renseignement et de la Sécurité des Forces armées de toute forme de communications émises à l'étranger »*. Cette seconde forme d'interception est possible depuis longtemps déjà, et peut être mise en œuvre tant à des fins militaires dans le cadre des missions définies à l'article 11 § 2, 1° et 2° L.R&S, que pour des motifs de sécurité et de protection des troupes belges et alliées lors de missions à l'étranger ainsi que des ressortissants belges établis à l'étranger (art. 11, § 2, 3° et 4°, L.R&S). Ces 'interceptions' sont soumises à un tout autre cadre de contrôle.[174]

Le contrôle externe est, en effet, exclusivement confié au Comité permanent R, à la fois avant, pendant et après les interceptions (art. 44*bis* L.R&S). Le Comité est compétent pour faire cesser les interceptions en cours, lorsqu'il apparaît que les conditions dans lesquelles elles sont réalisées ne respectent pas les dispositions légales et/ou l'autorisation ministérielle (art. 44*ter* L.R&S). Chaque année, au début du mois de décembre, le SGRS doit, en effet, présenter au ministre de la Défense sa liste motivée d'organisations ou d'institutions dont les communications pourront faire l'objet d'interceptions dans le courant de l'année suivante, et ce dans le but d'octroyer à ces interceptions l'autorisation ministérielle. Le ministre doit prendre sa décision dans les dix jours ouvrables et doit la communiquer au SGRS. Ensuite, le SGRS est tenu d'envoyer la liste et l'autorisation ministérielle au Comité permanent R. Mais cette liste est souvent

173 Voir à ce propos 'Chapitre III. Le contrôle des méthodes particulières de renseignement'.

174 La Loi du 30 mars 2017 (*M.B.* 28 avril 2017) a sensiblement élargi les possibilités d'interception. La loi prévoit aussi que le Comité permanent R effectue un contrôle renforcé, notamment en se basant sur une liste d'interceptions mensuelle. Le présent rapport d'activités ne tient compte que de la réglementation qui était d'application en 2016.

transmise avec retard.[175] L'année 2016 n'a pas fait exception, le Comité n'ayant reçu le plan d'interceptions qu'au mois de juin.

Par ailleurs, vu les constats qu'il a dressés dans la foulée des révélations d'Edward Snowden[176] et vu l'intention déclarée du SGRS d'utiliser la possibilité de mettre des câbles de télécommunication sur écoute, le Comité a actualisé et approfondi ses connaissances sur les activités SIGINT[177] du SGRS. Le Comité a ainsi effectué des visites de travail dans les sites belges où se déroulent ces activités. Par exemple, le travail des opérateurs a été observé en temps réel et a ensuite été comparé aux mentions reprises dans le journal de bord (art. 44*bis* 2° et 3° L.R&S). Des interceptions mentionnées dans le journal de bord ont été sélectionnées de manière ponctuelle afin de vérifier leur traçabilité et de vérifier si elles devaient être reprises dans le 'Plan d'interceptions 2016'. Enfin, des discussions ont été menées avec des membres du département technique de la section SIGINT, ce qui a permis d'avoir une vue d'ensemble sur le matériel utilisé. Les accords de coopération avec d'autres partenaires SIGINT ont également été discutés.

Ces enquêtes, inspections et discussions ont donné lieu à une étude qui a été transmise, en juillet 2016, au ministre de la Défense et au SGRS. Le Comité a notamment établi les constatations et formulé les remarques suivantes :

- les priorités assignées aux opérateurs étaient conformes au 'Plan d'interceptions 2016' ;
- en 2016, la section SIGINT du SGRS était active dans une nouvelle région. La section était essentiellement chargée de rechercher et d'identifier des sélecteurs pertinents ;
- le journal de bord répondait aux exigences telles que formulées par le Comité dans de précédentes recommandations ;
- les interceptions sélectionnées ponctuellement, et qui ont ensuite fait l'objet d'une vérification approfondie, se sont révélées traçables et compatibles avec le 'Plan d'interceptions 2016' ;
- le SGRS s'est montré disposé à mieux identifier les personnes et les organisations qui figurent dans les plans d'interceptions plutôt que de se référer à des typologies. Le Comité a néanmoins souligné que cette intention devait être effectivement concrétisée ;
- certains besoins matériels ont déjà été comblés ou sont programmés. Un élargissement du cadre du personnel n'était toutefois pas prévu, ce qui a suscité l'inquiétude du Comité, plus particulièrement en ce qui concerne les

175 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 103 ('IX3.2. L'envoi à temps des interceptions de sécurité visées') et *Rapport d'activités 2015*, 71. Le Comité n'a reçu le Plan d'écoutes 2017 qu'en juillet 2017.

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

177 SIGINT est l'abréviation de *Signals Intelligence* et fait référence aux renseignements recueillis via l'interception de signaux électroniques.

traducteurs qualifiés, en plus des analystes, des opérateurs et des collaborateurs nécessaires ;
- le Comité a été informé de nouvelles initiatives développées en matière de coopération SIGINT avec des pays tiers et de l'intention d'acquérir du nouveau matériel. Le Comité a salué cette ouverture du SGRS. Il a néanmoins fait remarquer que de telles d'initiatives seraient suivies avec attention, exactement comme l'ont été de précédents projets du SGRS[178] ;
- le Comité permanent R n'a fait aucun constat ayant entraîné l'arrêt d'interceptions.

Dans l'ensemble, le Comité a constaté que le SGRS avait fait preuve de transparence quant à ses activités d'interception, ses processus de travail et ses projets. Le Comité a l'intention de continuer à renforcer son contrôle spécifique en la matière.

178 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 73-75 (V.1. 'Avis concernant la coopération internationale en matière de SIGINT').

CHAPITRE V
MISSIONS POUR LES COMMISSIONS D'ENQUÊTE PARLEMENTAIRES

Le Comité permanent R a été créé par la Loi du 18 juillet 1991 comme l'organe de contrôle spécifique des services de renseignement et de sécurité. En 1996[179], le Comité s'est vu confier, pour la première fois, une nouvelle mission : une commission d'enquête parlementaire peut désormais faire appel à l'organe de contrôle dans ses enquêtes. Cette évolution s'inscrivait dans le cadre d'une réforme globale (en l'occurrence une extension[180]) des possibilités d'enquêtes parlementaires. Ce n'est qu'en 2016 que la possibilité de faire appel au Comité a été utilisée pour la première fois : le Comité permanent R s'est vu assigner différentes missions par deux commissions d'enquête distinctes.

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

Le 22 mars 2016, la Belgique a été la cible d'attentats terroristes graves. 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[181], et ce « *afin d'analyser si la Belgique s'est*

---

179 La 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 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.), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, Antwerpen, Intersentia, 2013, 55.

180 La loi énonce à présent 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.

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

dotée de moyens pour lutter efficacement contre le radicalisme et le terrorisme, d'examiner si elle dispose de services aptes à assurer la sécurité des citoyens et de faire des recommandations qui permettraient de les améliorer».[182]

En juillet 2016, le Comité permanent R a pris l'initiative d'ouvrir une enquête de contrôle relative à «*la position d'information des deux services de renseignement sur les individus ou groupes ayant perpétré des attentats ou liés aux attentats de Bruxelles-Zaventem, avant le 22 mars 2016 ainsi que les individus ou groupes qui ont permis à Salah Abdeslam de vivre dans la clandestinité, jusqu'à son arrestation le 18 mars 2016*».[183] Mais la Commission a fait appel au Comité permanent R et au Comité permanent P, à diverses reprises.

Les activités menées par le Comité permanent R pour cette Commission d'enquêtes peuvent se résumer comme suit: l'envoi de rapports d'enquête, la rédaction d'un rapport reprenant les recommandations formulées précédemment dans le cadre de la lutte contre le terrorisme et l'extrémisme, l'utilisation du Comité comme 'passerelle' pour les informations classifiées, l'audition comme témoin et l'exécution de missions d'enquête.

V.1.1. L'ENVOI DE RAPPORTS D'ENQUÊTE

Dans le passé, le Comité permanent R a mené de nombreuses enquêtes[184] susceptibles de présenter un intérêt direct ou indirect pour la Commission d'enquête parlementaire.[185] Il s'agissait des enquêtes suivantes:

- enquête de contrôle sur la manière dont les services de renseignement s'intéressent aux activités islamistes extrémistes et terroristes (2001);
- enquête de contrôle sur le suivi de l'islamisme radical par les services de renseignement (2007);
- enquête de contrôle sur la manière dont la VSSE et le SGRS suivent les activités que des services de renseignement étrangers déploient sur le territoire belge à l'égard de la diaspora (2011);
- enquête de contrôle sur la détection et le suivi par le SGRS d'éléments extrémistes au sein du personnel de la Défense (2012);
- enquête commune de contrôle sur la manière dont l'OCAM entretient des relations internationales avec des services étrangers ou internationaux

182 *Doc. parl.*, Chambre 2016-17, 54-1752/8, 25.

183 Pour plus de détails, voir: 'Chapitre II.4. La position d'information des deux services de renseignement avant les attentats de Zaventem et de Maelbeek'.

184 Début juin 2016, une liste reprenant toutes les enquêtes de contrôle effectuées par le Comité permanent R entre 2000 et 2016 a été transmise au président de la Commission d'enquête parlementaire.

185 En marge des activités de la Commission, le Comité a été informé que «*la commission d'accompagnement a décidé que dorénavant, elle n'examinerait plus les dossiers des Comités P et R concernant le terrorisme tant que la commission d'enquête parlementaire sur les attentats terroristes n'aurait pas terminé ses travaux*».

homologues en application de l'art. 8, 3° de la L. OCAM du 10 juillet 2006 (2013) ;
- enquête de contrôle suite à une plainte d'un bâtonnier sur l'utilisation d'informations issues de la récolte massive de métadata d'origine étrangère dans des affaires pénales (2013) ;
- enquête de contrôle concernant la plainte d'un ressortissant tunisien résidant en Belgique qui pense être suivi par les services de renseignement (2014) ;
- enquête de contrôle relative à la position d'information des deux services de renseignement sur le recrutement, l'envoi, le séjour et le retour en Belgique de jeunes (belges et étrangers résidant en Belgique) qui partent ou sont partis combattre en Syrie ou en Irak et au transfert des renseignements aux diverses autorités (ainsi qu'un addendum sur l'attentat manqué dans le Thalys) (2016) ;
- enquête de contrôle sur la manière dont la VSSE a mis en application le protocole d'accord réglant la coopération entre la Sûreté de l'État (VSSE) et la Direction générale Exécution des Peines et des Mesures (DGEPM) (2016) ;
- enquête de contrôle sur la position d'information des deux services de renseignement sur les individus ou groupes ayant perpétré les attentats de Paris ou liés à ces attentats, avant le vendredi 13 novembre 2015 au soir (2016).

Le Comité permanent R a mis ces rapports d'enquête à la disposition de la Commission d'enquête parlementaire.

V.1.2. UN APERCU DES RECOMMANDATIONS RELATIVES À LA LUTTE CONTRE LE TERRORISME ET L'EXTRÉMISME

À la demande de la commission d'enquête parlementaire, le Comité a établi un rapport reprenant toutes les recommandations formulées depuis 2010 qui présentent un intérêt direct ou indirect dans le cadre de la lutte contre le terrorisme et l'extrémisme. Celles-ci ont été complétées par d'autres recommandations relatives à la protection des droits que la Constitution et la loi confèrent aux personnes. Pour autant que le Comité soit en possession des informations requises, il a été chaque fois brièvement indiqué si et dans quelle mesure la recommandation en question a déjà été mise en œuvre. Ce document est résumé ci-dessous.

Moyens techniques et effectifs suffisants – Possibilités légales

Le Comité a toujours plaidé en faveur de l'octroi de moyens suffisants aux deux services de renseignement, et ce pas seulement au niveau des effectifs et de la logistique, mais aussi au niveau législatif. Naturellement, ces recommandations ne visaient pas exclusivement à améliorer la lutte contre l'extrémisme et le

terrorisme ; l'octroi des moyens nécessaires doit permettre d'exécuter comme il se doit toutes les tâches énumérées dans la Loi organique du 30 novembre 1998.

Dans ce contexte, le Comité a fait remarquer que les effectifs de la VSSE suivaient complètement l'évolution budgétaire. L'année 2015 constituait un creux en termes d'effectifs : en 2010, la VSSE disposait encore de 15 % d'équivalents temps plein (ETP) en plus par rapport à début janvier 2015. Début 2016, une augmentation était à nouveau perceptible, vu le recrutement de nouveaux inspecteurs et analystes.

En ce qui concerne le SGRS, il n'était pas possible de dresser un tableau comparatif, étant donné que ce service ne dispose pas d'un budget propre, mais qu'il est géré comme une entité au sein de la Défense. Les chiffres disponibles concernant les effectifs du SGRS montrent que le nombre d'ETP est resté plutôt stable depuis 2007.

Enfin, le Comité a souligné l'importance d'un budget et d'un cadre adéquats à l'OCAM, qui depuis son instauration en 2006, a un rôle important à jouer dans la lutte contre le terrorisme et l'extrémisme.

En ce qui concerne les compétences légales, il a évidemment été fait mention de la Loi du 4 février 2010 qui a permis à la VSSE et au SGRS d'utiliser des méthodes spécifiques et exceptionnelles étendues. Ces moyens sont bien entendu fréquemment mis en œuvre pour contrer les menaces terroristes et extrémistes.

Enfin, le Comité a également souligné que le SGRS n'est pas exclusivement compétent pour le suivi de l'extrémisme et du terrorisme *per se*. Ce n'est que dans la mesure où un lien existe avec la sécurité militaire que ce service de renseignement est compétent. On peut par exemple mentionner le suivi de l'extrémisme au sein de l'armée. Un autre exemple est la situation où il y existe une menace militaire réelle émanant des *foreign terrorist fighters* (FTF), entre autres pour la population : le SGRS est clairement compétent pour intervenir. Le Comité a recommandé de réfléchir à une description plus précise des compétences du SGRS en la matière.[186]

Modifications de la Loi MRD

Ces dernières années, le Comité a formulé plusieurs recommandations en vue d'adapter la Loi MRD, d'une part pour permettre une intervention plus performante, et d'autre part, pour garder l'équilibre indispensable avec les libertés et les droits fondamentaux.

Ainsi, il a été signalé que le Loi MRD ne permettait pas la mise en œuvre de méthodes exceptionnelles en cas d'extrémisme. Le Comité a proposé d'abandonner cette interdiction. La Loi organique des services de renseignement

[186] La Loi du 30 mars 2017, qui a sensiblement modifié la loi organique des services de renseignement et de sécurité, a donné une définition plus large des compétences du SGRS, sans toutefois faire explicitement référence au terrorisme et à l'extrémisme.

et de sécurité a été modifiée en ce sens par la Loi du 30 mars 2017. Cette loi a introduit d'autres modifications liées à des recommandations émises précédemment par le Comité : la mise en œuvre de MRD à l'étranger, l'abandon de l'interdiction de détruire des données récoltées via des écoutes après un an et deux mois, l'utilisation de la procédure d'extrême urgence visée à l'article 13/1 § 2, alinéa 3, L.R&S pour la commission d'infractions… En ce qui concerne le respect des libertés et des droits fondamentaux, le Comité a souligné à plusieurs reprises que l'obligation de notification, qui a été annulée par l'arrêt de la Cour constitutionnelle du 22 septembre 2011, devait être remplacée. La modification de la loi de 2017 y a également répondu.

Enfin, le Comité a attiré l'attention sur de précédentes recommandations visant à revoir la réglementation pour les interceptions de communications étrangères par le SGRS. Des éléments qui doivent de toute manière être examinés dans le cadre d'une telle révision 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'écoutes annuel, la possibilité de faire du *datamining* en vrac, et la question de savoir si des opérations SIGINT étrangères doivent toujours s'inscrire dans le cadre plus large d'un 'mandat international'. Les modalités ont été précisées pour certains de ces aspects dans la Loi du 30 mars 2017.

Coordination en matière de renseignements et création de l'OCAM

Dans le cadre d'une enquête sur la gestion des informations dans une affaire liée au terrorisme, le Comité a réitéré sa proposition de nommer un coordinateur en matière de renseignements. Cette personne devrait avoir une vue sur la production des services opérationnels. Sa mission consisterait à recevoir les rapports des services de renseignement dans les domaines que l'ancien Comité ministériel (qui est devenu le Conseil national de sécurité) considère comme prioritaires et sur base desquels elle établirait des synthèses périodiques et thématiques destinées aux autorités compétentes. La nécessité d'une meilleure coordination et d'un l'échange d'informations entre les services de police et de renseignement est également apparue à la suite de l'enquête commune des Comités R et P relative à la coordination entre les différents services de renseignement et de police dans la lutte contre le terrorisme. Les résultats de ces enquêtes ont été concrétisés en grande partie via la création de l'Organe de coordination pour l'analyse de la menace par la Loi du 10 juillet 2006. Depuis l'instauration de l'OCAM, le Comité permanent R, de concert avec le Comité permanent P, a formulé plusieurs recommandations visant à améliorer le fonctionnement de l'organe de coordination. Il s'agissait notamment des thèmes suivants :

- un point de contact doit être clairement établi au sein de chaque service d'appui ;
- le point de contact central doit avoir une vue complète sur les informations échangées ;

- au sein de chaque service d'appui, la traçabilité des renseignements doit être garantie ;
- la notion de 'renseignements pertinents' doit être clarifiée ;
- la confusion autour des différentes procédures d'embargo doit être dissipée ;
- la portée de la procédure d'embargo sur le travail d'analyse de l'OCAM doit être précisée ;
- il convient de prévoir une procédure en cas de différend au sujet de l'utilisation et de la diffusion d'informations fournies sous embargo ;
- l'application de la procédure d'embargo doit pouvoir être contrôlée ;
- les évaluations ponctuelles de la menace doivent être standardisées ;
- un réseau de communication sécurisé doit être prévu ;
- la confusion autour de l'identité et des 'missions à l'étranger' de l'OCAM doit être levée par une directive du Conseil national de sécurité[187] ;
- la représentation des services de sécurité à des forums internationaux doit être coordonnée ;
- le fonctionnement de la *Joint Information Box* (qui est une liste de données sur des personnes et des organisations 'radicalisantes' dans notre société) doit être sensiblement revu.[188]

Le législateur ou le gouvernement a, ici aussi, concrétisé plusieurs points repris dans les recommandations.

Coopération entre la VSSE et le SGRS avec d'autres services de police et autorités belges

Pour lutter contre le terrorisme et l'extrémisme, il est évidemment essentiel que les différentes autorités compétentes coopèrent de manière optimale et coordonnent leurs actions. Diverses recommandations du Comité permanent R doivent y contribuer :

- les ministres compétents du Conseil national de sécurité doivent définir les conditions de la coopération, de l'échange d'informations et de l'assistance technique, et ce faisant, exécuter les obligations reprises aux articles 19 et 20 L.R&S[189] ;
- la coordination et la collaboration entre les deux services de renseignement doivent être améliorées, plus particulièrement par une exploitation rationnelle des moyens, l'échange d'informations et la production d'analyses communes, sans que les services ne perdent leur identité ni leurs spécificités ;

187 Le Conseil national de sécurité a entre-temps édicté une telle directive.

188 Cette recommandation a été prise en considération, entre autres par la création de la banque de données dynamique FTF (voir à ce propos le 'Chapitre VI. Le contrôle de banques de données communes') et par la transformation annoncée de la JIB.

189 Cette recommandation a déjà été (en partie) concrétisée dans différents protocoles et directives.

- des protocoles d'accord doivent être conclus avec l'Office des étrangers et le Commissariat général aux réfugiés et apatrides[190] ;
- le protocole d'accord entre la VSSE et la Direction générale des Établissements pénitentiaires est dépassé dans sa forme actuelle et doit être adapté et réécrit. Le SGRS devrait lui aussi conclure un tel accord ;
- une concertation doit être mise en place entre les services de renseignement, d'une part, et les services de police (fédérale et locale), d'autre part, afin d'échanger des données par le biais de procédures bien définies. L'absence d'accord de coopération entre ces services constitue sans aucun doute une défaillance dans le système de sécurité belge ;
- les différents participants à la *local task force* doivent s'informer mutuellement des besoins, des possibilités et des limites de chacun ;
- pour un suivi adéquat de l'extrémisme au sein de l'armée, le SGRS doit veiller à optimiser tous les canaux d'informations utiles. La qualité des contacts établis avec les différentes unités et les autres services de la Défense doit concentrer toute l'attention.

Collaboration avec les services étrangers

En ce qui concerne la collaboration avec les services étrangers aussi, le Comité a recommandé à plusieurs reprises de mettre en œuvre les dispositions des articles 19 et 20 L.R&S. En 2017, le Conseil national de sécurité a adopté une directive importante en la matière, qui précise à quelles conditions les services de renseignement belges doivent ou peuvent collaborer avec les services étrangers. Toutefois, la directive n'aborde pas encore suffisamment la transmission de données à caractère personnel aux services étrangers. Il s'agit naturellement d'un aspect essentiel dans le cadre de la lutte contre le terrorisme.

En outre, le Comité a souligné que le service de renseignement qui reçoit ces données de l'étranger doit au moins s'efforcer de découvrir de quelle manière les renseignements concernés ont été recueillis, et ce pour ne pas accepter, le cas échéant, des données de pays tiers qui ont été (manifestement) recueillies illégalement.

Enfin, le Comité a récemment émis une recommandation visant à instaurer des procédures plus structurées et standardisées au niveau international pour l'échange d'informations avec l'étranger.

La collecte et l'analyse : les produits du travail de renseignement

Le Comité a formulé six recommandations pour organiser la collecte et l'analyse en vue d'apporter une valeur ajoutée claire au niveau des produits du travail de renseignement :

190 Un tel accord existe depuis 2011 entre la VSSE et l'Office des étrangers.

- les processus de renseignement doivent bénéficier d'une approche méthodique, où sont déterminées au préalable les questions d'enquête portant sur les phénomènes à suivre et la manière dont les informations sont recueillies (méthodes de collecte) et analysées (méthodes d'analyse) (cf. II.1.3.3) ;
- les deux services de renseignement doivent demander explicitement à leurs 'clients' de préciser les renseignements dont ils veulent disposer et la manière dont ils évaluent ces renseignements (*feedback*) ;
- il convient d'utiliser des techniques d'analyse standardisées pour éviter de commettre des erreurs cognitives ou factuelles ;
- il convient de produire des renseignements prédictifs pour les différentes autorités, étant donné qu'ils constituent l'essence du travail de renseignement ;
- les services doivent établir des analyses stratégiques, en particulier sur l'islamisme radical et sur les stratégies utilisées par les extrémistes islamistes ;
- en vue d'assurer la continuité des activités, il convient de réaliser et d'actualiser des analyses de phénomène.

Flux d'informations et ICT

En ce qui concerne les flux d'informations et les applications ICT au sein du SGRS, le Comité a formulé, à l'époque, les recommandations concrètes suivantes :

- le système *Request for Information* (RFI) devrait améliorer (considérablement) le traitement, le suivi et la clôture des demandes d'informations ;
- il convient 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 être en mesure de 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. Il fallait en outre veiller à une bonne collaboration entre les services de collecte et les bureaux d'analyse. Enfin, il était impératif d'investir dans les moyens humains et l'ICT.
- de manière générale, le Comité recommandait d'investir suffisamment de moyens dans l'ICT, et ce plus rapidement que ce qui était prévu dans les plans d'investissement.

En 2016, le Comité a cependant constaté que le système de gestion des données du SGRS n'était pas encore au point. Il a une nouvelle fois recommandé d'y remédier de toute urgence.

En ce qui concerne la VSSE, le Comité a constaté que les concepts à la base de l'organisation de la banque de données représentaient une source de problèmes,

étant donné qu'ils n'étaient pas interprétés de manière univoque ou appliqués en tant que tels. Aussi le travail de renseignement risquait-il de perdre en efficacité et en efficience, puisque (tous) les rapports appropriés risquaient de ne pas 'remonter à la surface' lorsque cela s'avérait nécessaire pour le travail d'analyse. Il y avait aussi un risque de tirer des conclusions erronées. Le Comité permanent R a dès lors recommandé que la VSSE se penche sur les processus de travail, le flux d'informations et les moyens ICT qui supportent l'ensemble.

Conditions d'organisation pour un fonctionnement optimal

Dans le cadre de l'audit du SGRS[191], le Comité permanent R a émis de nombreuses recommandations concrètes concernant les conditions d'organisation nécessaires à une bonne affectation des moyens, à la gestion et la direction du personnel, aux flux d'informations et l'ICT (voir *supra*) et, enfin, à la gestion des risques.

Les recommandations du Comité permanent R découlant de l'audit de performance de la VSSE ont été subdivisées en quatre thèmes : leadership, gestion interne de l'information, processus de travail et satisfaction qualité. Certaines de ces recommandations ont été mises en œuvre complètement ou partiellement.

Une réglementation prévue pour les aspects liés au travail avec les informateurs

Au fil des années, le Comité permanent R a formulé de nombreuses recommandations concernant le travail avec les informateurs. Celles-ci gardent tout leur intérêt, étant donné que la possibilité de collecte demeure également essentielle dans le domaine de l'extrémisme et du terrorisme.

- une réglementation légale claire concernant le travail avec les informateurs doit être établie ;
- il faut ensuite qu'une directive générale soit édictée, où tous les aspects du travail avec les informateurs seront abordés ;
- il convient en particulier d'accorder plus d'attention à une analyse de risques formelle, qui énumère les différents risques, à laquelle participe une personne ou une section qui n'avait pas pris part à la rédaction de proposition initiale de recrutement ;
- pour être en mesure d'évaluer la pertinence et la fiabilité des informations à fournir ou des informations fournies, les services de renseignement doivent pouvoir disposer de la vue la plus précise possible de l'intéressé (*screening*). Il convient dès lors de prévoir une base légale fixant les grandes lignes de tels contrôles ;

191 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 7-14 ('Un audit au sein du service de renseignement militaire').

- il arrive qu'un informateur soit 'guidé' de manière à ce qu'il commence à opérer, à certains moments, comme un informateur civil qui se voit confier de véritables missions de renseignement. Cette forme de recueil de renseignements est, à divers égards, encore plus problématique que le travail 'ordinaire' avec des informateurs (sécurité de l'intéressé et possibilité qu'il soit 'tenté' de poser des actes illégaux). D'autres part, les possibilités de contrôle du service sur la manière dont ses 'missions' sont remplies, sont limitées. Aussi le Comité permanent R réitère-t-il sa recommandation relative à l'élaboration d'une réglementation légale en la matière ;
- il convient de mener une réflexion sur l'opportunité – dans des cas tout à fait exceptionnels et moyennant un contrôle démocratique approfondi – d'octroyer une 'contrepartie' bien définie (pécuniaire ou non) à des informateurs qui peuvent disposer d'informations cruciales pour la sécurité de l'État de droit ;
- les deux services de renseignement doivent réfléchir à l'instauration 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.

Une série de recommandations ponctuelles

- dans le cadre du suivi du terrorisme et de l'extrémisme, il est absolument nécessaire de garantir l'anonymat des enquêteurs afin de les protéger contre des menaces ;
- les membres du personnel des services de renseignement et de l'OCAM doivent faire preuve de la plus grande prudence dans leurs activités sur les réseaux sociaux, surtout dans le contexte actuel de menace accrue d'attentats terroristes ;
- les services doivent définir des critères pour informer les personnes qui font l'objet d'une menace (art. 19 L.R&S) ;
- le personnel d'entreprises ou d'institutions qui traitent des substances chimiques, radiologiques ou biologiques susceptibles d'être utilisées dans l'élaboration d'armes NRBC devraient être soumises à une enquête ou à une vérification de sécurité ;
- 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 ;
- la VSSE doit systématiquement tenir à jour ses informations, et ce dans le cadre de son rôle dans les demandes de reconnaissance de communautés religieuses (p. ex. la reconnaissance d'un mosquée) ;
- les services doivent (pouvoir) recruter suffisamment de collaborateurs maîtrisant des langues spécifiques.

V.1.3. 'PASSERELLE' POUR LA CONSULTATION DE DOCUMENTS SECRETS

En raison de l'étendue de sa mission et de ses pouvoirs, ainsi que de la tâche qui lui est confiée de formuler des recommandations, la Commission parlementaire a estimé utile d'avoir accès à ces enquêtes. Celles-ci comportent des rapports, des renseignements ou des document secrets, qu'il s'agisse d'informations classifiées, 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, l'OCAM, les Comités permanents R et P, la Cellule de traitement des informations financières …).[192]

Quant à la consultation d'informations classifiées, il convenait de trouver un *modus vivendi*, vu que les membres de la Commission n'étaient pas titulaires de l'habilitation de sécurité requise.[193] Plusieurs consultations ont eu lieu pour aboutir à la conclusion d'un protocole.[194] En ce qui concerne les services de renseignement spécifiquement, il a été décidé que les informations classifiées seraient disponibles à la consultation dans les locaux du Comité permanent R. La Commission pouvait compter sur le concours d'un de ses experts, qui est titulaire d'une habilitation de sécurité. Il a «*pu avoir des contacts avec ces organismes et prendre connaissance de documents dont il a pu déduire ce qu'il pouvait en dire à la commission sans trahir leur secret*».[195]

V.1.4. TÉMOIN(S) POUR LA COMMISSION D'ENQUÊTE

Le 21 décembre 2016, le président du Comité permanent R a été entendu à huis clos. Il a donné des explications à la commission concernant l'enquête de contrôle sur la position d'information des deux services de renseignement, préalablement au 22 mars 2016, relative individus ou groupes qui ont perpétré les attentats à Zaventem et à Maelbeek ou qui y étaient impliqués, et aux individus

192 *Doc. parl.*, Chambre 2016-17, 54-1752/8, 27.

193 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).

194 *Doc. parl.*, Chambre 2016-17, 54-1752/8, 27. «*Pour ce qui concerne les informations figurant dans des dossiers en cours ainsi que celles détenues par des services de police ou de renseignement, elle a établi, le 27 mai 2016, un protocole conclu entre un de ses experts ainsi que le procureur fédéral, le procureur général de Bruxelles et le magistrat désigné par le premier président de la cour d'appel de Bruxelles, conformément à l'article 4, § 2, de la Loi du 3 mai 1980. Ce protocole prévoit la mise sous enveloppe scellée des informations secrètes demandées et leur ouverture en présence de l'expert disposant de l'habilitation de sécurité ainsi que des chefs de corps*». Par chefs de corps, on n'entend pas seulement ici les responsables de police, mais aussi l'Administrateur général de la VSSE et le Chef du SGRS, qui utilisaient cette procédure.

195 *Doc. parl.*, Chambre 2016-17, 54-1752/8, 27.

ou groupes qui ont permis à Salah Abdelslam de rester dans la clandestinité jusqu'à son arrestation le 18 mars 2016.[196, 197]

V.1.5. L'EXÉCUTION DE DEVOIRS D'ENQUÊTE COMPLÉMENTAIRES

À la demande de la Commission parlementaire de suivi, le Comité permanent R a établi une ligne du temps reprenant les documents qui, entre le 13 novembre 2015 et le 22 mars 2016, ont été reçus ou envoyés par les services de renseignement belges de/à des services partenaires (étrangers) au sujet des protagonistes des attentats.[198] D'autres missions d'enquête ont été exécutées au cours de l'année 2017.

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

Le 1er décembre 2016, le texte visant à instaurer une seconde commission d'enquête parlementaire a été adopté en séance plénière de la Chambre.[199] 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. Le journal 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'.[200] Les autorités françaises auraient alors fait appel à Armand De Decker, qui était, à ce moment-là, sénateur 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

196 *Doc. parl.*, Chambre 2016-17, 54-1752/8, 49. Lors de la réunion du 11 janvier 2017, une nouvelle audition a eu lieu avec le président du Comité permanent R.

197 La Commission a refusé d'accéder à la demande des présidents des Comités permanents R et P de pouvoir être présents lors des auditions à huis clos de responsables des services placés sous leur contrôle.

198 La ligne du temps concernait Salah Abdelsam, Mohamed Abrini, Mohamed Belkaïd, Khalid et Ibrahim El Bakraoui, Osama Krayem et Najim Laachraoui.

199 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).

200 Il s'agit de Messieurs Chodiev, Ibragimov et Machkevitch, trois associés provenant d'Asie centrale qui se sont établis en Belgique au début des années 90 pour fonder des sociétés.

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, sur les pressions et l'influence qui ont mené à l'élaboration de cette 'loi sur la transaction financière'.

La Commission d'enquête était donc chargée de mener l'enquête sur les circonstances ayant mené à l'adoption et à l'application de la Loi du 14 avril 2011 portant disposition diverses, en ce qui concerne la transaction pénale. Elle devait en outre examiner comment le Ministère public avait fait application de l'article 216*bis* CIC. Enfin, la Commission d'enquête devait enquêter sur la manière dont Messieurs Patokh Chodiev et Alijan Ibragimov avaient acquis la nationalité belge.[201]

Le 15 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 de Patokh Chodiev et d'autres 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 naturalisation[202] – et étaient issus de l'enquête de contrôle Tractebel.[203]

En 2017, le Comité permanent R a été largement impliqué et s'est vu confier diverses missions d'enquête par la Commission d'enquête parlementaire : plusieurs rapports d'enquête ont été établis, et le président du Comité permanent R a été entendu à plusieurs reprises dans ce cadre. Le Comité y reviendra dans son Rapport d'activités 2017.

---

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

202 Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2012*, 5-14 *('Le rôle de la VSSE dans le cadre des procédures d'acquisition de la nationalité belge'*).

203 L'enquête de contrôle sur *'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), a fait l'objet de deux rapports succincts (COMITÉ PERMANENT R, *Rapport d'activités 2001*, 6-7 et *Rapport d'activités 2003*, 118). En raison d'autres priorités, cette enquête n'a jamais été finalisée.

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[204] 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.

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*', également appelée la banque de données dynamique FTF, via l'Arrêté royal du 21 juillet 2016 (AR FTF).[205]

L'article 44/6[206] 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 (COC) et au Comité permanent R. Les deux instances sont également chargées de rendre un avis conjoint préalable à la création d'une banque de données commune sur base d'une 'déclaration préalable'. Il s'agit de nouvelles missions pour le Comité permanent R.

Le présent chapitre étant le premier à être rédigé dans ce contexte, il est consacré à la description des banques de données communes (VI.1), avant d'aborder spécifiquement la banque de données FTF (VI.2) et de retracer les activités menées l'année écoulée, dans ce cadre, par le COC et le Comité permanent R (VI.3).

VI.1. QU'EST-CE QU'UNE BANQUE DE DONNÉES COMMUNE ?

VI.1.1. FINALITÉS ET RÈGLES

Différents services, organes ou autorités exercent des missions en matière de prévention et de suivi du terrorisme ou de l'extrémisme pouvant mener au terrorisme.

---

204 *M.B.* 9 mai 2016.

205 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 (AR FTF).

206 Également modifié par la Loi du 27 avril 2016 précitée.

L'article 44 § 2 LFP prévoit que, lorsqu'il est nécessaire pour ces instances, dans le cadre de l'exercice conjoint de leurs missions, de structurer les données à caractère personnel et les informations disponibles *« de sorte qu'elles puissent être directement retrouvées, ces données et informations sont traitées dans une ou plusieurs banques de données communes »*. Au niveau des finalités, la création d'une banque de données commune est motivée soit par une nécessité stratégique, tactique ou opérationnelle de traiter en commun des données, soit par l'aide à la prise de décisions des autorités administratives, de police administrative ou judiciaire (art. 44/11/3*bis* LFP).

Une telle banque de données ne peut être créée que conjointement par les ministres de l'Intérieur et de la Justice. Ils sont alors responsables du traitement, au sens 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.

Elle permet le traitement de différentes catégories de données à caractère personnel relatives notamment aux personnes, aux groupements, aux organisations et aux phénomènes. La loi impose que ces données soient adéquates, pertinentes et non excessives au regard des missions et des finalités citées ci-dessus.

Préalablement à sa création, les ministres de l'Intérieur et de la Justice doivent faire une déclaration de la banque de données commune au COC et au Comité permanent R, qui doivent émettre conjointement un avis dans les 30 jours à compter de la réception de la déclaration. Il s'agit là d'une forme de contrôle *a priori,* complété par le contrôle (permanent), comme prévu à l'article 44/6 LFP (*supra*).

Pour chaque banque de données commune, un Arrêté royal délibéré en Conseil des ministres détermine, après avis de la Commission de la protection de la vie privée, les types de données à caractère personnel traitées, les règles de responsabilité en matière de protection des données, les règles en matière de sécurité de traitements ainsi que les règles d'utilisation, de conservation et d'effacement des données.

VI.1.2. LA CONSULTATION ET LA TRANSMISSION D'INFORMATIONS

Six catégories différentes de services peuvent avoir connaissance (d'une partie) des informations d'une banque de données commune, par la consultation ou la transmission de celles-ci.

La loi dispose que la banque de données est, sur la base du besoin d'en connaître (‘*need to know*’), directement accessible à l'OCAM, à la police intégrée et aux services de renseignement et de sécurité (art. 44/11/3*ter* § 1er LFP). Ces services sont dénommés ‘services de base’ dans l'AR FTF (voir VI.2.2).

À côté de ceux-ci, l'on retrouve les services suivants (dits 'services partenaires' dans l'AR FTF) : la Commission Permanente de la Police Locale, la Direction générale Centre de crise, la Direction générale Sécurité et Prévention du SPF Intérieur, la Direction générale des Établissements pénitentiaires et les établissements pénitentiaires, le SPF Affaires étrangères – Direction générale Affaires consulaires, le Ministère public, la Cellule de traitement des informations financières, l'Office des étrangers et les services d'enquête et de recherche de l'Administration générale des douanes et accises. Pour ces services, les données peuvent être directement accessibles ou faire l'objet d'une interrogation directe (voir également VI.2.2).

En outre, le Roi peut accorder l'accès à d'autres « *autorités publiques belges chargées par la loi de l'application de la loi pénale* » aux données et informations dont elles ont besoin pour l'exercice de leurs compétences de prévention et de suivi du terrorisme ou de l'extrémisme lorsqu'il peut mener au terrorisme (art. 44/11/3*ter* § 3 LFP).

La loi impose que les données et les informations introduites dans la banque de données commune soient immédiatement communiquées au chef de corps de chaque zone de police concerné qui, à son tour, informe[207] les autorités de police administrative compétentes (art. 44/11/3 *ter* § 4 LFP).

Le législateur autorise également à communiquer les données et informations « *à une autorité ou une entité tierce* », selon les modalités déterminées par le Roi et après une évaluation spécifique (art. 44/11/3*quater* LFP).

Enfin, dans le respect des règles nationales et internationales liant la Belgique, ces données peuvent être communiquées, sur la base de modalités à fixer par le Roi, aux services de police étrangers, aux organisations internationales de coopération judiciaire et policière, aux services de répression internationaux, ainsi qu'aux services de renseignement étrangers et à des organes étrangers équivalents à l'OCAM.

VI.1.3. L'OBLIGATION D'ALIMENTER LA BANQUE DE DONNÉES COMMUNE

L'idée sous-jacente étant la nécessité de la mise en commun des informations (le principe de '*need to share*'), la loi prévoit une obligation d'alimentation de la banque de données commune. Ainsi, les services qui accèdent directement à celle-ci – les services de base et les services qui sont indiqués par le Roi sur base de la Loi (voir VI.2.2.) – transmettent d'office leurs informations pertinentes. L'enregistrement se fait sous la responsabilité du service concerné et selon sa procédure de validation interne.

---

207 Dans le respect des conditions prévues à l'article 44/1 § 4 LFP et en application de cet article.

La loi n'exclut pas la possibilité de traiter des informations classifiées dans des banques de données communes.[208]

Il existe deux dérogations à l'obligation d'introduire des informations dans la banque de données commune. L'alimentation peut être différée aussi longtemps que le magistrat compétent, avec l'accord du Procureur fédéral, estime que cette alimentation peut compromettre l'exercice de l'action publique ou la sécurité d'une personne. La même possibilité s'applique à l'information provenant d'un service de renseignements : lorsque (et aussi longtemps que) le dirigeant du service juge que l'alimentation peut compromettre la sécurité d'une personne ou la règle du tiers service, il peut différer la transmission (art. 44/11/3*ter* § 5 LFP).

VI.1.4. ACTEURS SPÉCIFIQUES

Indépendamment des services qui ont accès aux données et de l'obligation d'alimentation, la loi a prévu un nombre d'acteurs auxquels elle a assigné des rôles importants dans le cadre du fonctionnement d'une banque de données commune.

Tout d'abord, un 'conseiller en sécurité et en protection de la vie privée' doit être désigné conjointement par les ministres de l'Intérieur et de la Justice. Il est particulièrement chargé de veiller au respect des conditions générales de licéité du traitement telles que prévues aux articles 4 à 8 de la Loi du 8 décembre 1992 relative à la protection de vie privée. Il est en outre la personne de contact du COC et du Comité permanent R (art. 44/3 § 2 LFP).

D'autre part, un 'gestionnaire' est chargé de la gestion technique et fonctionnelle de la banque de données comprenant *au moins* les missions de création et de mise à disposition de la banque de données commune, la gestion et la maintenance de celle-ci, la traduction en règles fonctionnelles des modalités relatives au traitement de l'information, la détermination des normes techniques nécessaire au fonctionnement de la banque de données, l'organisation des droits et des accès nécessaires, la gestion et le traitement des incidents de sécurité ainsi que la fourniture d'avis, de documentation et d'assistance technique (art. 44/11/3*bis* § 9 LFP).

---

208 L'Exposé des Motifs précise à cet égard : *« Ces données et informations relatives à différentes catégories de données ne sont en principe pas des données à caractère personnel ou des informations classifiées. Il convient en effet de permettre le partage assez large de données et d'informations sans mettre de barrière à leur traitement. Toutefois, s'il est absolument nécessaire que de telles données soient traitées dans ces banques de données afin de rencontrer les finalités pour lesquelles elles ont été créées, alors la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité est d'application. Dès lors, toute personne qui souhaite par exemple accéder à ces données et informations classifiées doit disposer de l'habilitation de sécurité appropriée. » Doc. parl.,* Chambre, 2016-2017, n° 54-1727/1, 21-22.

Enfin, un 'responsable opérationnel' est désigné. Il assure *au moins* les missions suivantes : le contrôle de la qualité des données et de leur pertinence au regard des finalités de la banque de données, la coordination de l'alimentation de la banque de données par les différents services, l'organisation de la collaboration adéquate entre services en vue de réaliser les finalités prévues et le contrôle que l'exploitation des données et des informations réponde à ces finalités (art. 44/11/3*bis* § 10 LFP).

VI.2. LA BANQUE DE DONNÉES COMMUNE '*FOREIGN TERRORIST FIGHTERS*'

L'Arrêté royal du 21 juillet 2016 (AR FTF) crée la banque de données commune '*foreign terrorist fighters*' ('la banque de données FTF') et lui assigne la finalité de contribuer à l'analyse, à l'évaluation et au suivi de personnes en lien avec la problématique du djihadisme.

VI.2.1. DES FICHES DE RENSEIGNEMENTS

La 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. Il s'agit de fiches personnelles, appelées à être actualisées, contenant toutes les données à caractère personnel et les informations[209] non classifiées[210] concernant les intéressés et provenant de l'ensemble des services compétents (cf. art. 1, 11° AR FTF). Aux termes du rapport au Roi, cette fiche doit permettre « *non seulement de pouvoir évaluer la menace potentielle que représentent ces personnes, mais surtout d'en assurer le suivi afin d'anticiper et d'empêcher de possibles actes terroristes de leur part* ».[211]

Les fiches de renseignements 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 :

– elles se sont rendues dans une zone de conflit djihadiste ;
– elles ont quitté la Belgique pour se rendre dans une zone de conflit djihadiste ;

---

209 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).

210 À la différence de ce qui était prévu par le législateur (voir l'exposé des motifs, *supra*), l'AR FTF n'autorise pas le traitement d'informations classifiées. L'AR FTF impose toutefois la détention d'une habilitation de sécurité du degré 'secret' à toute personne accédant à la banque de données FTF (art. 7 § 2 AR FTF).

211 *M.B.* 22 septembre 2016, 63970.

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

VI.2.2. UNE GRADATION DES ACCÈS

L'article 7 AR FTF met en œuvre la gradation des accès prévue par la loi :

- les services dits 'de base' (l'OCAM, les services de renseignement et de sécurité et la police intégrée) ainsi que certains '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) ont directement accès à la banque de données FTF et, corollairement, l'obligation de l'alimenter (VI.1.3) ;
- d'autres 'services partenaires' (la DGCC, la DGSP, la DG Affaires consulaires du SPF Affaires étrangères et les services d'enquête et de recherche des douanes et accises), se voient attribuer un accès par une interrogation directe, qui porte sur l'existence ou non de données FTF concernant une personne (principe du *'hit/no hit'*). En cas de *'hit'*, il appartient au service concerné de prendre contact avec un des services de base ;
- enfin, un accès direct et une obligation d'alimentation sont également prévus pour l'Administration générale des Maisons de Justice de la Communauté française, le Département Maison de Justice du Ministère de la Communauté Germanophone, la Division des Maisons de Justice du Ministère des services compétents de l'Autorité flamande et la *Vlaams Agentschap Jongerenwelzijn*. Cet accès est limité aux données des FTF pour lesquels ces services assurent leurs missions.

VI.2.3. DES CARTES D'INFORMATIONS

A côté des fiches de renseignements, des 'cartes d'informations' (cf. les articles 44/11/3*quater* LFP et 11 AR FTF) sont élaborées à destination des instances qui n'ont pas d'accès aux fiches. La carte est un extrait de la fiche de

renseignements et contient les données et des informations strictement limitées aux informations dont le destinataire a besoin.

Seuls les services de base sont autorisés à transmettre la carte d'informations. L'AR FTF prévoit, dans ce cadre, 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 (art. 12 AR FTF).

VI.2.4. L'ATTRIBUTION DES DIFFÉRENTS RÔLES

La Police fédérale est désignée en qualité de gestionnaire de la banque de données FTF. Outre les missions prévues par la LFP, l'AR FTF lui impose de tenir une liste des personnes accédant à la banque de données, de veiller à une journalisation des traitements ainsi que d'informer l'OCAM, le conseiller en sécurité, le COC et le Comité permanent R de tout incident de sécurité constaté ou rapporté (art. 3 AR FTF).

L'OCAM se voit quant à lui désigné comme responsable opérationnel. Il répond de l'évaluation de la fiche de renseignements, de la validation comme FTF, il assure les contacts avec les responsables de traitement et il informe le service concerné dans le cas où une donnée émanant de celui-ci n'est pas ou plus évaluée comme adéquate, pertinente ou non excessive (art. 4 AR FTF).

L'AR FTF précise davantage les missions du conseiller en sécurité et en protection de la vie privée : sensibilisation à la protection des données, coopération avec la Police fédérale pour l'élaboration des procédures ainsi qu'avec les autres conseillers en sécurité. Son statut est également précisé. Il agit donc en toute indépendance, mais dans le respect des compétences des différents services (art. 5 AR FTF).

VI.2.5. UN SYSTÈME DE VALIDATION DES DONNÉES

Les services qui ont directement accès à la banque de données FTF doivent mettre en place un système de validation afin de garantir que les données transmises soient adéquates, pertinentes et non excessives au regard de la finalité de la banque de données de contribuer à l'analyse, à l'évaluation et au suivi de personnes en lien avec la problématique du djihadisme.

Ce système de validation doit être communiqué à l'OCAM (responsable opérationnel) qui, à son tour, doit le communiquer à la Police fédérale (gestionnaire), au conseiller en sécurité ainsi qu'au COC et au Comité permanent R.

VI.2.6. LA GESTION DES DONNÉES

VI.2.6.1. L'ajout, la modification et la suppression de données

Les données concernant un FTF sont évidemment appelées à être actualisées en permanence. C'est dans cette perspective que la banque de données est qualifiée de 'dynamique'. Selon le Rapport au Roi, étant donné le nombre important de services ayant accès directement à la banque de données, il fallait faire une distinction entre les services plus au courant de la problématique des combattants étrangers terroristes et ceux qui se limitent à enrichir les données et les informations. Les règles peuvent être résumées comme suit :

- seuls les services de base peuvent créer une fiche de renseignements (c'est-à-dire enregistrer une personne dans la banque de données). Si une personne est déjà enregistrée, les services disposant de l'accès direct ajoutent après validation leurs propres informations sans modifier ou supprimer celles déjà existantes ;
- le service qui a enregistré une information est le seul à pouvoir modifier, rectifier ou supprimer celle-ci. Lorsqu'un service estime qu'une information introduite par un autre service doit être modifiée ou supprimée, il s'adresse au service ayant procédé à l'enregistrement de celle-ci ;
- en cas de position divergente quant à la modification ou à la suppression d'une donnée, il revient à l'OCAM, en sa qualité de responsable opérationnel, de prendre la décision finale (art. 9 AR FTF) ;
- l'AR FTF règle également la situation où un service supprimerait l'enregistrement du FTF dans sa propre base de données. Dans cette hypothèse, il doit en informer l'OCAM qui peut, s'il estime que l'information reste adéquate, pertinente et non excessive, décider de la maintenir dans la banque de données FTF (art. 8 § 2 AR FTF).

VI.2.6.2. La conservation et l'archivage des données[212]

Les informations doivent être supprimées si la finalité de la banque de données FTF disparaît, et au maximum trente ans après leur dernier traitement.[213]

Après le dernier traitement, il est examiné au minimum tous les trois ans si les données présentent toujours un lien direct avec la finalité. Dans l'affirmative, elles sont conservées.

Cette règle comporte une exception pour les personnes pour lesquelles il existe des indices sérieux qu'elles appartiennent à une des catégories de FTF

212 Art. 13 et 14 AR FTF lus en combinaison avec l'article 44/11/3*bis* § 5 et § 7 LFP.

213 Sans préjudice de la Loi du 24 juin 1995 relative aux archives.

visées à l'article 6 § 1er, 1° AR FTF. Pour celles-ci, le délai maximum de conservation est ramené à six mois après leur enregistrement. A l'échéance de ce délai, si leur appartenance à une catégorie de FTF est avérée, leurs données sont conservées selon les règles susmentionnées. Si leur appartenance n'est pas avérée, leurs données sont effacées.

Les données et les informations qui doivent être supprimées peuvent être archivées pour une durée maximum de trente ans. Les données archivées ne peuvent être exploitées que pour des finalités définies (en matière de politique policière[214], pour le traitement des antécédents dans le cadre d'une enquête relative à un fait criminel de terrorisme ou pour assurer la défense des autorités administratives, de police judiciaire ou de police administrative). À l'issue de ce délai de trente ans, elles sont effacées.[215]

En sa qualité de gestionnaire de la banque de données, la Police fédérale est chargée de traduire en règles fonctionnelles les modalités relatives au traitement de l'information (voir *supra*). Il lui revient donc de prendre les mesures nécessaires pour une gestion correcte des données.

VI.2.7. LA COLLABORATION INTERNATIONALE

Seuls les services de base sont autorisés à communiquer des informations issues de la banque de données FTF à des services étrangers (art.15 AR FTF).

Pour les services de police, la communication doit être conforme aux dispositions de l'AR du 30 octobre 2015 relatif aux conditions afférentes à la communication des données à caractère personnel et des informations des services de police belges aux membres d'Interpol et à Interpol ainsi qu'aux dispositions du chapitre Ier/1 de la Loi du 9 décembre 2004 sur la transmission policière internationale de données à caractère personnel et d'informations à finalité judiciaire, l'entraide judiciaire internationale en matière pénale et modifiant l'article 90*ter* CIC.

En ce qui concerne les services de renseignements, l'AR FTF impose que la communication à des services de renseignement étrangers s'effectue conformément à l'article 20 § 3 L.R&S, c'est-à-dire sur base de conditions définies par le Conseil national de sécurité.

Enfin, s'agissant de l'OCAM, l'AR renvoie à l'article 8, 3° L.OCAM l'autorisant à assurer des relations internationales spécifiques avec des services étrangers ou internationaux homologues, conformément aux directives du Conseil national de sécurité et lui imposant de communiquer les informations obtenues aux services belges compétents.

214 Dans ce cas, les données doivent être anonymisées.
215 Sans préjudice de la Loi du 24 juin 1995 relative aux archives.

VI.2.8. RESPONSABILITÉS FINALES ET OBLIGATIONS GÉNÉRALES

Après avoir rendu obligatoire un contrôle de la qualité des données en imposant un système de validation interne à tous les services disposant de l'accès direct (voir *supra*), l'AR FTF détermine les responsabilités si cette qualité fait défaut (art. 16 AR FTF). La responsabilité de la qualité des données incombe :

- au responsable du traitement propre à chaque service qui alimente la banque de données FTF en ce qui concerne les informations que ce service a transmises ;
- aux ministres de l'Intérieur et de la Justice en ce qui concerne les informations validées sur les fiches de renseignements.

En outre, chaque responsable de traitement d'un service disposant de l'accès direct doit veiller à la légalité de la transmission des données par ce service à la banque de données FTF.

Les ministres de l'Intérieur et de la Justice doivent, quant à eux, veiller à la légalité de la transmission des informations contenues dans la banque de données FTF, au bon fonctionnement technique et opérationnel de celle-ci, à la sécurité des systèmes d'accès ainsi qu'à l'intégrité, la disponibilité et la confidentialité des informations. L'AR FTF prévoit qu'il leur appartient de déterminer, par directive, les mesures nécessaires en vue respecter ces obligations.

VI.3. LES CONTRÔLES DU COC ET DU COMITÉ PERMANENT R

L'AR FTF créant la banque de données FTF n'est entré en vigueur que le 22 septembre 2016, et la déclaration préalable obligatoire de la banque de données date du 3 novembre 2016. Le contrôle du COC et du Comité permanent R s'est donc limité en 2016 à l'avis sur cette déclaration (VI.3.2). Cependant, un premier avis avait été formulé sur base d'une déclaration préalable provisoire (VI.3.1) (art. 44/11/3*bis* § 3 LFP).

VI.3.1. UN PREMIER AVIS

En mai et juin 2016, les ministres de l'Intérieur et de la Justice ont demandé un avis sur le projet d'Arrêté royal relatif à la banque de données communes FTF et sur la déclaration préalable requise.

L'avis (intégralement repris en annexe F), a été rendu le 20 juin 2016. En résumé, le COC et le Comité permanent R :

- soulignaient que cet avis était provisoire dans la mesure où l'Arrêté royal n'était pas encore publié. Le COC et le Comité permanent R insistaient sur la nécessité que les déclarations futures de banques de données communes interviennent après la publication des Arrêtés royaux qui s'y rapportent ;
- observaient que les personnes qui soutiennent les FTF ou les recrutent n'allaient pas être reprises dans la base de données, alors que leur prise en considération aurait accru l'utilité opérationnelle de celle-ci, ceci d'autant plus que cette catégorie est reprise dans la circulaire COL 10/2015 du Collège des Procureurs généraux concernant l'approche judiciaire relative aux FTF ;
- relevaient l'importance de la désignation d'un conseiller en sécurité et en protection de la vie privée pour la banque de données, mais aussi au sein de chacun des services y accédant, et insistaient sur la désignation de points de contact auprès de l'OCAM et de la Police fédérale ;
- pointaient les difficultés qui pourraient survenir dans la mesure où le projet d'AR et la déclaration spécifient que la banque de données ne contiendrait que des informations non classifiées, alors que les services de renseignement et de sécurité disposent essentiellement d'informations classifiées et qu'ils sont obligés, par la loi, d'alimenter cette banque de données avec toutes les données dont ils disposent ;
- suggéraient de modifier le projet d'Arrêté royal pour prévoir la transmission au COC et au Comité permanent R de la liste des personnes disposant d'un accès à la banque de données ;
- s'interrogeaient sur le fondement de l'accès prévu pour la Commission Permanente de la Police Locale, qui est un organe exclusivement stratégique.
- demandaient à ce que les règles de validation des différents services soient insérées dans la déclaration ;
- préconisaient, pour permettre un suivi effectif dans le cadre de leur mission de contrôle, de prévoir la possibilité de pouvoir obtenir un historique des fiches de renseignements et des cartes d'informations ;
- relevaient que les conditions de collaboration avec les services de renseignements étrangers devaient encore être déterminées par le Conseil national de sécurité. Le même constat était posé pour l'OCAM concernant sa collaboration avec des organes homologues étrangers.

VI.3.2. UN DEUXIÈME AVIS

Après la publication de l'AR FTF, les ministres ont adressé une déclaration adaptée le 3 novembre 2016, accompagnée d'un manuel d'utilisation (*user guide*).

Le second avis du COC et du Comité permanent R a été émis le 1er décembre 2016 (voir annexe F). Ce second avis était favorable, sous certaines réserves. En résumé, le COC et le Comité permanent R :

- pointaient l'absence (persistante) de désignation du conseiller en sécurité et en protection de la vie privée. Ils soulignaient l'importance de ce rôle et insistaient sur une désignation rapide. En revanche, les Comités relevaient avec satisfaction la désignation de tels conseillers au niveau des services accédant à la banque de données FTF ;
- insistaient sur le nécessaire principe du '*need to know* ' devant régir les accès des différents services ;
- recommandaient que les services soient en mesure de leur communiquer, via leur conseiller en sécurité respectif, les objectifs concrets pour lesquels l'accès est légitime (en particulier au regard des fonctions des personnes disposant d'un accès) ;
- notaient que les modalités de l'accès direct des Maisons de Justice et de la *Vlaams Agentschap Jongerenwelzijn* feraient l'objet d'une déclaration complémentaire ;
- relevaient que la déclaration préalable n'abordait pas la nécessité, pour les instances de contrôle, de pouvoir disposer d'un historique des données traitées. Ils notaient que la traçabilité relève des missions du gestionnaire de la banque de données FTF, c'est-à-dire la Police fédérale ;
- constataient que les systèmes de validation décrits dans la déclaration étaient souvent trop sommaires, voire complètement inexistants. Ils exhortaient dès lors les services à veiller à ce que les données à caractère personnel qu'ils introduisent soient adéquates, pertinentes et non excessives.

CHAPITRE VII
AVIS, ÉTUDES ET AUTRES ACTIVITÉS

Les missions légales du Comité permanent R sont très variées : réalisation d'enquêtes de contrôle ; compétence juridictionnelle en matière de méthodes particulières de données, missions dans le cadre de la compétence d'interception du SGRS, tâches judiciaires remplies par son service d'Enquêtes, contrôle de la banque de données dynamique FTF, avis communs avec l'Organe de contrôle de l'information policière, rôle dans l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité… Le Comité mène aussi des études, et il est consulté en raison de son expertise. En 2016, le Comité a fait l'objet de quatre demandes d'avis officiels sur diverses questions.

VII.1. AVIS SUR L'AVANT-PROJET DE LOI MODIFIANT LA LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

Dans son courrier daté du 22 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 sur les services de renseignement du 30 novembre 1998.[216] Le projet de loi « *vise à améliorer et à clarifier la loi organique en répondant aux problèmes opérationnels rencontrés, sans toucher ni aux méthodes existantes, ni aux garanties prévues pour protéger les droits fondamentaux des citoyens, ni aux différents contrôles* ».[217]

Dans son avis, le Comité soulignait le fait qu'il était en faveur de tout projet visant à accroître l'efficacité des services de renseignement belges, pour autant que des garanties suffisantes soient prévues pour sauvegarder les libertés et les droits fondamentaux. Ceci est particulièrement vrai dans le contexte sociétal

---

216 Vu les délais de réponse extrêmement courts, d'une part, et vu l'étendue et la complexité des modifications proposées, d'autre part, le Comité n'a pas été en mesure d'examiner chaque aspect du projet en détail, et encore moins d'effectuer un contrôle légistique ou d'élaborer des propositions de modification alternatives. L'avis du Comité permanent R, qui date du 4 mars 2016, est repris en intégralité à l'annexe E du présent rapport.

217 *Doc. parl.*, Chambre, 2015-16, 54-2043/1.

actuel, où la lutte contre le terrorisme et le radicalisme doit pouvoir être menée de manière optimale.

Le Comité a pu constater que le projet tenait compte, en grande partie, des recommandations qu'il avait formulées au fil des ans. Cependant, des modifications importantes à la Loi sur les services de renseignement étaient envisagées dans certains domaines. Ces modifications allaient plus loin que les dispositions insérées par la Loi MRD du 4 février 2010 (comme par exemple les possibilités de collecte du SGRS à l'étranger). D'autres dispositions légales – également perfectibles[218] – n'ont pas été abordées.

Le Comité considérait que l'évaluation de la réglementation en vigueur à ce moment-là portait essentiellement sur l'efficacité des services de renseignement, ce qui s'est traduit par un projet axé sur l'octroi, aux deux services de renseignement, de compétences supplémentaires (parfois utiles et nécessaires) et de moyens légaux. Mais ce projet n'accordait pas toujours suffisamment d'attention au contrôle externe ni aux '*checks and balances*' pourtant indispensables. Plus encore, il apparaît que ce contrôle externe était parfois ramené à un niveau antérieur.[219]

VII.2. AVIS SUR LE PROJET DE LOI RÉGLEMENTANT LA SÉCURITÉ PRIVÉE

Fin septembre 2016[220], le ministre de la Sécurité et de l'Intérieur a demandé au président du Comité permanent R, qui préside également l'Organe de recours en matière d'habilitation, d'attestations et d'avis de sécurité, de formuler un avis sur les dispositions du projet de loi réglementant la sécurité privée qui concernent l'Organe de recours.[221] Le gouvernement envisageait, en effet, de transférer à l'Organe de recours le contentieux relatif à l'enquête sur les conditions de sécurité pour l'octroi d'une licence dans le secteur de la sécurité privée. Les lignes directrices de l'avis ont été examinées avec les membres du Comité permanent P et avec la Commission Vie privée qui siègent dans l'Organe de recours.[222]

---

218 Comme, par exemple, la recommandation selon laquelle les pouvoirs exécutif et législatif devraient préciser les articles 19 et 20 L.R&S. Ces dispositions essentielles régissent notamment la transmission d'informations (y compris les données à caractère personnel) à d'autres services (étrangers) et la collaboration/concours technique que les deux services belges peuvent prêter aux autorités judiciaires ou à des homologues étrangers.

219 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 a été publié au *Moniteur belge* le 28 avril 2017.

220 Courrier du 28 septembre 2016 du ministre de la Sécurité et de l'Intérieur au président de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité.

221 *Doc. parl.*, Chambre 2016-17, n°54-2388/7 (Projet de loi réglementant la sécurité privée).

222 L'avis est repris intégralement à l'annexe D de présent rapport. L'option retenue a été de rendre cet avis dans un délai particulièrement court, ce qui n'a pas permis un examen détaillé

Dans son avis, l'Organe de recours a insisté sur le fait qu'il n'éprouvait en soi aucune réticence quant à la proposition de transférer à l'Organe de recours une partie du contentieux administratif en matière de sécurité privée. Étant donné que ce tranfert est synonyme d'un surcroît de travail considérable, cet avis reprend des propositions visant à gagner en efficacité (l'introduction d'un acte d'appel simple, des délais de réponse obligatoires, une obligation pour l'autorité concernée de procéder à des auditions…). Par ailleurs, des propositions ont été ajoutées sur la modification de la Loi Classification du 11 décembre 1998 ainsi que sur la modification de la Loi du 11 décembre 1998 portant création de l'Organe de recours. Enfin, plusieurs considérations ont été émises à propos de l''enquête sur les conditions de sécurité'. La nouvelle Loi réglementant la sécurité privée et particulière a été adoptée le 8 juin 2017 en séance plénière. Le contentieux n'a finalement pas été transféré à l'Organe de contrôle ; il est resté au Conseil d'État.

VII.3. DOSSIERS D'INFORMATION

Outre les enquêtes de contrôle (Chapitre II), le Comité permanent R ouvre également des 'dossiers d'information', qui doivent permettre d'apporter une réponse à des questions relatives au fonctionnement des services de renseignement et de l'OCAM.[223] 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, par la suite, à l'ouverture d'une enquête de contrôle formelle. Si toutefois il est clair qu'une telle enquête ne constituerait aucune plus-value au regard des finalités du Comité permanent R, aucune suite n'est donnée au dossier d'information.

Des dossiers d'information ont par exemple été ouverts en 2016 sur la problématique des intérêts scientifiques et économiques du pays, sur le rapport établi par la VSSE concernant la participation éventuelle dans EANDIS d'une entreprise chinoise active dans le secteur de l'énergie, sur des informations recueillies concernant la problématique du travail avec les informateurs et du recrutement de ceux-ci, ainsi que sur les contacts avec des ambassades. Ces dossiers n'ont donné lieu à aucun suivi.

---

de chaque aspect. Voir également à cet égard 'Chapitre VIII. Le greffe de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité'.

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

VII.4. EXPERT DANS DIVERS FORUMS

En 2016, 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. En mai 2016, le BISC a organisé une journée d'étude intitulée *'Big data and intelligence services : perspectives and future challenges'* ;
- il a également été fait appel à l'expertise du Comité lors d'un séminaire pratique destiné à la police, à la magistrature et au barreau en matière de 'screening de personnes', et ce dans le contexte de la Loi relative à la classification et aux habilitations, attestions et avis de sécurité ;
- fin janvier 2016, le greffier a participé à un panel de discussion sur l'*'Intelligence services' surveillance in the EU : fundamental rights, safeguards and remedies'* dans le cadre de la conférence internationale *'Computers, Privacy & Data Protection. [In]visibilities & Infrastructures'*, organisée à Bruxelles ;
- en mars 2016, le président du Comité a participé, avec entre autres l'*EU Counter-Terrorism Coordinator* et le directeur d'Europol, à un panel d'experts sur *'The EU response to counter terrorism and the parliament's right to scrutiny'* dans le cadre de la conférence *'Counter terrorism, security and human rights'* ;
- une délégation du Comité permanent R a participé à des réunions d'experts *'National intelligence authorities and surveillance in the EU : Fundamental rights safeguards and remedies'*, organisée sur initiative du directeur du *Sector of Information Society, Privacy and Data Protection Freedoms and Justice Department* de l'Agence des droits fondamentaux de l'Union européenne (FRA). Celle-ci est chargée de réaliser une étude comparative sur le contrôle démocratique des services de renseignement dans les États membres de l'Union européenne pour le compte du Parlement européen, dans la foulée de la résolution du 12 mars 2014[224] ;
- le greffier du Comité permanent R a une nouvelle fois 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) ;

[224] 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).

- le président du Comité a été impliqué par l'Organisation internationale de la francophonie (OIF) dans l'organisation de la Conférence sur la lutte contre le terrorisme et la prévention de la radicalisation violente, qui s'est tenue à Paris ;
- le Comité continue à participer aux réunions du Groupe européen de recherche sur l'éthique du renseignement (GERER). Ce groupe de travail, notamment composé de représentants des services de renseignement (militaires) français, belges et luxembourgeois, et du Comité permanent R), mène une réflexion sur la relation 'éthique – services de renseignement' ;
- en février 2016, le directeur adjoint du service d'Enquêtes est intervenu comme expert pour le *Geneva Centre for the Democratic Control of Armed Forces* (DCAF) et pour la République tunisienne, dans le cadre de la table ronde 'Quelle gouvernance des services de renseignement dans une société démocratique ?'. Il était notamment question de la réforme des services de renseignement dans un nouveau contexte démocratique, de la manière dont sont échangés les renseignements dans un contexte international et de la définition des priorités des services de renseignement ;
- invité comme orateur par la présidente du Sénat, le président du Comité a pris part, en octobre 2016, au colloque intitulé 'La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux', lors duquel 'La protection des données à caractère personnel dans le domaine de la sécurité et de la vie publique' a été développée ;
- en 2016, le Président a fait deux exposés sur 'Le renseignement, ses défis et son contrôle' et 'Le contrôle parlementaire', à la demande du Département de Sciences Politiques de la Faculté de Droit de l'Université de Liège ;
- en novembre 2016, à l'invitation du *Geneva Centre for the Democratic Control of Armed Forces* (DCAF), le président et le greffier du Comité ont participé, en Tunisie, à une table ronde sur l' 'Accès à l'information : défis et opportunités pour la communauté du renseignement'. Les thèmes suivants ont été abordés : 'Concilier transparence et sécurité de l'État et des citoyens', 'Établir un système de classification de l'information', 'Concilier transparence et efficacité de la communauté du renseignement' et 'Garantir l'accès à l'information pour les acteurs de supervision et de contrôle de la communauté de renseignement' ;
- le Président a pris la parole, en novembre 2016 à Paris, dans le cadre du *'Fourth Seminar of the Queen Mary Reflection Group on Terrorism and Human Rights',* et ce dans le cadre d'un panel intitulé *'Inscribing in law oversight powers in respect of intelligence services'.*

VII.5. PROTOCOLE DE COOPÉRATION 'DROITS DE L'HOMME'

Contrairement à 22 autres pays européens, la Belgique ne s'est toujours pas dotée formellement d'un institut des droits de l'homme officiel fédéral.[225] Des réunions organisées avec d'autres institutions disposant d'un mandat en matière de droits de l'homme[226] ont abouti, à la mi-janvier 2015, à un protocole de coopération[227], dans lequel toutes les instances participantes se sont mises d'accord pour échanger leurs pratiques et leurs méthodes, pour examiner des questions communes et pour promouvoir la coopération mutuelle. En attendant la création d'un institut fédéral des droits de l'homme, elles doivent servir de plateforme de concertation entre des instituts exerçant partiellement ou entièrement un mandat d'institution chargée du respect des libertés et droits fondamentaux.

En 2016, les activités de cette plateforme ont consisté à organiser des réunions de concertation mensuelles, au cours desquelles ont été discutés tant des problématiques générales (p. ex. les mesures prises par les autorités fédérales et régionales suite aux attentats de Paris et la lutte contre la radicalisation, le nouveau règlement européen en matière de protection des données à caractère personnel, le traitement des plaintes et dénonciations…), que des cas très concrets. Par ailleurs, le site internet HRights, qui est une plateforme d'échanges pour les institutions participantes, a été lancé.[228]

VII.6. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

En octobre 2015, plusieurs organes de contrôle se sont réunis à Berne. La Suisse, les Pays-Bas, la Belgique ainsi que les pays scandinaves (Suède, Norvège et Danemark) étaient représentés. Cinq thèmes étaient à l'ordre du jour de cette réunion : (la mesure de) l'efficacité, l'accès pour les organes de contrôle à des informations des services de renseignement concernés, une vision sur les opérations en cours et l'échange d'informations au niveau international entre les services de renseignement et entre les organes de contrôle, ainsi que le contrôle

225 Le Conseil des droits de l'homme des Nations Unies l'a constaté en 2011 lors de son 'Examen périodique universel (EPU)'. Il a dû réitérer ce constat en 2016.

226 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.

227 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.

228 Le secrétariat de cette plateforme est assuré par les services administratifs des plus grandes organisations participantes.

de l'utilisation des données à caractère personnel par les services de renseignement. Lors de la réunion, il a été décidé d'initier une enquête de contrôle dans tous les pays participants sur la coopération internationale entre les différents services de renseignement en matière de lutte contre les *foreign terrorist fighters*. 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.[229] À la suite de cette réunion, les questions posées dans le cadre de l'enquête, ainsi que les définitions à retenir et le cadre légal en matière de diverses formes de coopération en Europe, ont été discutées en avril 2016 à La Haye.[230] Des réunions de suivi étaient prévues en septembre 2016 à Bruxelles et fin novembre 2016 à La Haye. La structure du rapport public commun et les progrès enregistrés dans les différentes enquêtes (meilleures pratiques, risques, définitions…) étaient notamment à l'ordre du jour de ces réunions.

Le 7 avril 2016, a eu lieu une visite de la commission d'enquête 'relative aux moyens mis en œuvre par l'État pour lutter contre le terrorime depuis le 7 janvier 2015' de l'Assemblée nationale française, sous la direction de son président. La délégation a rencontré le président du Comité permanent R, le vice-président du Comité permanent P ainsi que le président et les vice-présidents de la Commission Terrorisme.[231]

Toujours en avril 2016, le Comité permanent R a participé à la conférence scientifique *'Intelligence and democratic oversight from the end of the Cold War until today – key trends and developments'*, et ce à l'occasion des vingt ans d'existence de l'organe de contrôle parlementaire norvégien *(EOS-Committee)*. Dans la foulée de cette conférence, des contacts ont été établis avec l'*Interception of Communications Commissioner's Office* (IOCCO) du Royaume-Uni.

Par ailleurs, en 2016, le Comité permanent R a maintenu des contacts étroits avec la Commission nationale de contrôle des interceptions de sécurité (CNCIS) française et avec la nouvelle Commission nationale de contrôle des techniques de renseignement (CNCTR). Une visite de travail a eu lieu le 23 juin 2016 à Bruxelles.

En marge de l'*International Intelligence Oversight Forum*, organisé conjointement à Bucarest à la mi-octobre 2016 par le *Special Rapporteur for Privacy* (SRP) des Nations Unies et les quatre commissions du parlement roumain qui sont chacune compétentes pour un aspect du fonctionnement des

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

230 La réunion était précédée d'un exposé du directeur général de l'*Algemene Inlichtingen- en Veiligheidsdienst* (AIVD), et par ailleurs président du *Counter Terrorism Group* (CTG), sur l'échange de données à caractère personnel relatives aux *foreign terrorist fighters* au sein du CTG.

231 Leurs conclusions ont donné lieu à un rapport final (www.assemblée-nationale.fr/14/rap-enq/r3922-t1.asp).

services de renseignement[232], une délégation du Comité permanent R a eu des contacts informels avec des organes de contrôle des Pays-Bas, du Royaume-Uni, du Canada, du Danemark, d'Allemagne… L'objectif de ce forum était de mieux appréhender, dans un cadre confidentiel, les défis auxquels sont confrontés les organes de contrôle démocratiques dans un monde digitalisé.

Enfin, à la mi-décembre 2016, une délégation suisse a été reçue au Comité permanent R. Lors de cette rencontre, l'accent a été mis sur l'organisation du contrôle de l'application des méthodes particulières de renseignement.

VII.7. CONTRÔLE DES FONDS SPÉCIAUX[233]

Au nom de la Chambre des Représentants, la Cour des comptes contrôle l'utilisation des moyens financiers par les services publics. La Cour des comptes est amenée à contrôler la légalité, la légitimité et l'efficacité de toutes les dépenses, y compris, en principe, de toutes les dépenses des services de renseignement. Cependant, en raison du caractère sensible de la matière, une partie du budget de la VSSE et du SGRS (à savoir les 'fonds spéciaux' avec des dépenses destinées, par exemple, aux opérations et aux informateurs) n'est pas examinée par la Cour des comptes. Pour la VSSE, le contrôle de ces dépenses est effectué par le directeur de la Cellule politique générale du ministre la Justice. Depuis 2006, c'est le chef des Forces armées qui exerce seul le contrôle des fonds spéciaux du SGRS, et ce à raison de quatre fois par an. À la suggestion de la Cour des comptes, ce contrôle se déroule, depuis 2010, en présence du président du Comité permanent R. En 2016 également, ce contrôle a été effectué en sa présence.

VII.8. 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.

---

232 *The Joint Permanent Commission of the Chamber of Deputies and the Senate to exercise parliamentary control over the activity of the SRI, the Special Commission of the Chamber of Deputies and the Senate to exercise parliamentary control over the activity of the Foreign Intelligence Service, the Committee for Defense, Public Order, and National Security in the Chamber* en *the Committee for Defense, Public Order, and National Security in the Senate*. Cette initiative était également soutenue par le *Department of Information Policy and Governance* de l'Université de Malte et par le *Security, Technology & e-Privacy Research Group* de l'Université de Groningen.

233 Voir aussi à ce propos : COMITÉ PERMANENT R, dans son *Rapport d'activités 2015*, 11-16 ('II.2. La gestion, l'utilisation et le contrôle des « fonds spéciaux »'). Le Comité a formulé diverses recommandations à cet égard, dans le même rapport d'activités, 102-103 ('IX.2.2. Recommandations relatives à la gestion et au contrôle des « fonds spéciaux »').

Date	Sujet/titre	Organe de presse
6 janvier 2016	'Les services secrets belges pourront espionner les espions étrangers'	Le Soir
7 janvier 2016	'Spionnen mogen collega's controleren'	Het Laatste Nieuws
12 février 2016	'Dertigtal salafistische moskeeën in België'	Het Laatste Nieuws
26 février 2016	'Staasveiligheid onterecht kop van Jut'	De Tijd
22 mars 2016	'Aanslagen in Brussel : kroniek van een aangekondigde dood'	Knack
24 mars 2016	'Les services de renseignements belges ont-ils failli durant leur enquête?'	Le Soir
25 mars 2016	'Police, renseignement : imbroglio à la belge'	Libération
29 mars 2016	'Politie krijgt terreurinformatie niet verwerkt'	De Morgen
2 avril 2016	'La radicalisation en prison négligée depuis des années'	L'Écho
2 avril 2016	'Radicalisering in gevangenis laat aangepakt'	De Tijd
17 avril 2016	'Sécurité Brussels Airport : « On en va pas transformer Zaventem en Bunker mais il y a des problèmes a résoudre »'	RTBF
27 avril 2016	'Terrorisme : le Comité R sévère avec les renseignements belges'	RTBF
28 avril 2016	'Les services de renseignement belges sont-ils à la hauteur ?'	RTBF
28 avril 2016	'La Défense gratte les fonds de tiroir, mais ne peut se passer de nouveaux avions'	RTBF
12 mai 2016	'Te weinig informanten in strijd tegen terroristen'	De Tijd
12 mai 2016	'Trop peu d'indicateurs pour nos services secrets'	L'Écho
12 mai 2016	'22 nieuwe spionnen voor Staatsveiligheid, maar er is meer nodig'	De Standaard
12 mai 2016	'La Sûreté de l'État n'avait aucun informateur pour les frères Abdeslam'	Le Soir
18 mai 2016	'Kritieke infrastructuur onvoldoende beschermd'	De Tijd
19 mai 2016	'La Sûreté et le SGRS ne se parlent pas assez'	La Libre Belgique
11 août 2016	'De bewaking van de bewakers'	Trends
6 septembre 2016	'La commission « attentats » s'attaque à l'enquête'	Le Soir

14 septembre 2016	'Mag de Staatsveiligheid samenwerken met folterende inlichtingendiensten?'	Knack
17 septembre 2016	'Als Michael Freilich spreekt, moet iedereen zwijgen'	De Morgen
27 septembre 2016	'Waarom de Staatsveiligheid het moeilijk heeft met Eandis'	De Tijd
5 octobre 2016	'Renseignements : recrutement à la traîne'	L'Avenir
12 octobre 2016	'Staatsveiligheid krijgt eigen politie'	De Standaard
12 octobre 2016	'Leger mag voluit spioneren'	De Standaard
21 octobre 2016	'Staatsveiligheid : Eens geheim, altijd geheim ? Onzin ?'	Knack
2 novembre 2016	'Parijs-Brussel aller-retour – Caroline Van den Berghe & Dirk Leestmans'	De Redactie
18 novembre 2016	'Nog te weinig terreurinfo uitgewisseld'	VTM nieuws
16 décembre 2016	'Mogelijk 450 gevangenen geradicaliseerd'	De Tijd
22 décembre 2016	'Al vijfde valse start voor proces tegen Syriëstrijders'	Het Laatste Nieuws
22 décembre 2016	'Comité P, Comité I en Privacycommissie zijn « virtueel failliet » '	De Redactie
23 décembre 2016	'Tiental salafisten in Belgische leger'	Het Laatste Nieuws
23 décembre 2016	'Une dizaine de salafistes dans l'armée belge'	La Libre Belgique

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.[234] Il s'agit de missions confiées au service d'Enquêtes R par les autorités judiciaires. Cette compétence est décrite à l'article 40, alinéa 3 de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace. La Loi du 10 juillet 2006 relative à l'analyse de la menace a élargi cette compétence aux crimes et délits commis par des membres de l'Organe de coordination pour l'analyse de la menace (OCAM). En ce qui concerne les membres des autres 'services d'appui', cette disposition s'applique uniquement à l'obligation de communiquer à l'OCAM tout renseignement pertinent (art. 6 et 14 L.OCAM).

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le directeur du service d'Enquêtes R sont soumis à l'autorité du Procureur général près la cour d'appel ou du Procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a aucune autorité sur eux. Le président du Comité doit cependant veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle, et ce pour une raison évidente : l'organe de contrôle est avant tout à la disposition du Parlement. Cette mission pourrait être mise en péril si les dossiers judiciaires requéraient trop de temps. Le président peut, le cas échéant, se concerter avec les autorités judiciaires quant à la participation des membres du service d'Enquêtes R à des enquêtes pénales (art. 61*bis* L.Contrôle).

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

---

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

En 2016, le service d'Enquêtes R a réalisé quelques devoirs d'enquête dans le cadre d'une enquête judiciaire classée sans suite en février 2015, mais rouverte suite à la constitution de partie civile d'un membre de la famille de la victime.

CHAPITRE IX

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.[235]

Ces activités de l'Organe de recours ont un impact direct à la fois sur le budget et sur le personnel du Comité permanent R. En effet, tous les frais de fonctionnement sont supportés par le Comité permanent R, qui met à disposition non seulement son président et son greffier, mais aussi le personnel administratif requis.

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

En 2016, le nombre de recours et de décisions a connu une augmentation significative par rapport à l'année précédente, passant respectivement de 130 à 169 et de 137 à 173. À noter que le nombre de recours et de décisions est revenu globalement au niveau de 2014. L'augmentation constatée en 2016 est particulièrement marquée en ce qui concerne le nombre de recours introduits contre des avis de sécurité négatifs (de 63 à 101). Cette tendance à la hausse est également visible dans le nombre de recours introduits contre des refus d'octroi

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

d'attestations de sécurité concernant le secteur nucléaire[236], tandis que les refus d'octroi d'attestations de sécurité donnant accès à des zones classifiées a suivi le mouvement inverse. Les demandes d'informations complémentaires (passant de 7 à 23) et les auditions du requérant et de son avocat (de 107 à 127) se sont elles aussi inscrites dans une courbe ascendante.

Il convient de souligner que, derrière ces chiffres, se cache une charge de travail élevée en termes de préparation, de traitement et de suivi, et ce tant pour le greffe que pour l'Organe de recours lui-même. En effet, les dossiers ne cessent de se complexifier du point de vue de la gestion administrative, des audiences et des décisions.

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.[237] 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 la même veine, l'application de l'article 5 § 3 L. Org.recours se révèle problématique : la demande de soustraire certaines pièces du dossier à la consultation par le requérant 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.[238]

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

---

236 Cette catégorie d'attestations de sécurité a été insérée par la Loi du 30 mars 2011 modifiant la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire et modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *M.B.* 18 avril 2011 (article 8*bis* L.C.&HS). Précédemment, ces recours étaient intégrés dans les recours concernant les autres attestations de sécurité (article 22 L.C.&HS). Pour plus de clarté, et afin de prendre en compte les évolutions futures des recours concernant les attestations de sécurité délivrées dans le secteur nucléaire, celles-ci sont présentées séparément à compter du présent rapport.

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

238 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 du dossier à la consultation par le requérant (ou par 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 sur 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.

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 requiert 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 croissant de questions de procédure (p. ex. le débat sur la recevabilité, la question linguistique, les droits de la défense, l'obligation de motivation…). D'autre part, l'Organe de recours est plus souvent confronté à des dossiers hautement sensibles, qui sont liés à la problématique de la radicalisation et à la menace terroriste actuelle. De tels dossiers nécessitent évidemment un traitement extrêmement minutieux et une motivation adaptée. De plus, des mesures de sécurité spécifiques doivent parfois être prises.

Divers éléments conduisent à penser que la charge de travail de l'Organe de recours va encore (sensiblement) s'accroître dans le futur. Le gouvernement a annoncé son intention d'augmenter les contrôles de moralité (screenings), notamment dans l'optique de renforcer la sécurité des infrastructures critiques. Différents textes en projet circulent déjà en ce sens. Cette augmentation ne sera pas sans incidence sur les moyens du Comité permanent R. Il convient aussi de souligner que le gouvernement avait songé, dans un premier temps, à lui confier le contentieux administratif des recours en matière de sécurité privée (accès à la profession d'agent de gardiennage).[239] Il a ultérieurement abandonné cette piste.

Enfin, il convient de mentionner que l'Organe de recours a fait part aux instances compétentes – en particulier l'Autorité nationale de sécurité (ANS) – de sa profonde inquiétude face à l'extrême complexité de la législation et aux droits parfois limités du citoyen (p. ex. les délais de recours trop courts).

Tableau 1. Autorités de sécurité concernées

	2012	2013	2014	2015	2016
Autorité nationale de sécurité	40	98	99	68	92
Sûreté de l'État	0	1	0	1	0
Service Général du Renseignement et de la Sécurité	27	78	60	47	68
Agence fédérale de Contrôle nucléaire	11	9	8	10	8
Police fédérale	1	1	3	3	1

239 Voir 'VII.2. Avis sur le projet de loi réglementant la sécurité privée'. L'avis est repris à l'annexe D de ce rapport d'activités.

	2012	2013	2014	2015	2016
Police locale	2	2	1	1	0
Commission aéroportuaire locale	10	–	–	–	–
TOTAL	**91**	**189**	**171**	**130**	**169**

Tableau 2. Nature des décisions contestées

	2012	2013	2014	2015	2016
Habilitations de sécurité (art. 12 et s. L.C&HS)					
Confidentiel	7	5	5	9	5
Secret	29	56	43	35	38
Très secret	9	5	4	4	7
Refus	33	41	25	36	28
Retrait	12	5	9	7	9
Refus et retrait	0	4	0	0	0
Habilitation pour une durée limitée	0	1	2	3	4
Habilitation pour un niveau inférieur	1	0	1	0	1
Pas de décision dans les délais	1	15	15	2	7
Pas de décision dans les nouveaux délais	0	0	0	0	1
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	**45**	**66**	**52**	**48**	**50**
Attestations de sécurité zone classifiée (art. 22*bis*, al.1er L.C&HS)					
Refus	23	0	4	6	1
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	0	15	16	12	9
Retrait	0	0	0	1	0
Pas de décision dans le délai	0	0	0	0	0
Attestations de sécurité lieu secteur nucléaire (art. 8*bis* L.C&HS)					
Refus	–	–	–	–	7
Retrait	–	–	–	–	1

	2012	2013	2014	2015	2016
Pas de décision dans le délai	–	–	–	–	0
Avis de sécurité (art. 22*quinquies* L.C&HS)					
Avis négatif	23	106	99	63	101
Pas d'avis	0	2	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	**46**	**123**	**119**	**82**	**119**
TOTAL DÉCISIONS CONTESTÉES	**91**	**189**	**171**	**130**	**169**

Tableau 3. Nature du requérant

	2012	2013	2014	2015	2016
Fonctionnaire	5	4	0	4	2
Militaire	26	26	17	29	23
Particulier	54	159	145	93	139
Personne morale	6	0	6	4	5

Tableau 4. Langue du requérant

	2012	2013	2014	2015	2016
Français	51	92	92	75	99
Néerlandais	40	97	76	54	70
Allemand	0	0	0	0	0
Autre langue	0	0	0	1	0

Tableau 5. Nature des décisions interlocutoires prises par l'Organe de recours[240]

	2012	2013	2014	2015	2016
Demande du dossier complet (1)	90	187	168	130	167
Demande d'informations complémentaires (2)	5	12	16	7	23
Audition d'un membre d'une autorité (3)	10	3	11	7	10
Décision du président (4)	0	0	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (5)	44	68	78	50	54
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 d'enquête aux autorités de sécurité. Comme ce dossier contient davantage de données que le rapport d'enquête seul, cette requête est systématique.
(2) L'Organe de recours peut également demander tout complément d'informations qu'il juge nécessaire pendant la procédure.
(3) L'Organe de recours peut décider d'entendre les membres des services de renseignement et de police ou des autorités de sécurité qui ont participé à l'enquête ou à la vérification de sécurité.
(4) Le président de l'Organe de recours peut décider de permettre au membre du service de renseignement de garder secrètes certaines données pendant son audition.
(5) Si le service de renseignement ou de police concerné le demande, le président de l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant (voir *supra*).
(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'.

240 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 2016, alors que la décision n'a été rendue qu'en 2017.

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

	2012	2013	2014	2015	2016
Consultation du dossier par le requérant et/ou l'avocat	54	103	84	84	87
Audition du requérant (assisté ou non d'un avocat)[239]	65	138	115	107	127

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

	2012	2013	2014	2015	2016
Habilitations de sécurité (art. 12 et s. L.C&HS)					
Recours irrecevable	0	2	0	4	0
Recours sans objet	1	3	3	3	7
Recours non fondé	19	20	12	19	18
Recours fondé (avec octroi partiel ou complet)	23	35	14	24	24
Devoir d'enquête complémentaire par l'autorité	1	0	0	0	2
Délai supplémentaire pour l'autorité	0	14	12	1	2
Sans suite	0	0	0	1	0
Attestations de sécurité zone classifiée (art. 22*bis*, al.1er L.C&HS)					
Recours irrecevable	0	0	0	0	0
Recours sans objet	0	0	0	0	0
Recours non fondé	0	0	2	4	1
Recours fondé (avec octroi)	0	0	0	2	1
Attestations de sécurité pour lieux ou événements (art. 22*bis*, al.2 L.C&HS)					
Recours irrecevable	3	1	0	0	0
Recours sans objet	1	0	0	0	0
Recours non fondé	8	6	6	8	2
Recours fondé (avec octroi)	6	11	8	10	4
Donne acte de retrait de recours	0	0	0	2	0

241 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.

	2012	2013	2014	2015	2016
Attestations de sécurité pour le secteur nucléaire (art. 8*bis* § 2 L.C&HS)					
Recours irrecevable	–	–	–	–	1
Recours sans objet	–	–	–	–	1
Recours non fondé	–	–	–	–	0
Recours fondé (avec octroi)	–	–	–	–	7
Avis de sécurité (art. 22*quinquies* L.C&HS)					
Organe de recours non compétent	5	0	4	0	0
Recours irrecevable	1	4	4	6	15
Recours sans objet	0	1	4	0	0
Confirmation de l'avis négatif	9	25	53	28	42
Transformation en avis positif	4	65	41	23	46
Recours contre des actes normatifs d'une autorité administrative (art. 12 L. Org.recours)	0	0	0	0	0
TOTAL	**81**	**187**	**163**	**135**[240]	**173**

242 Il y avait encore deux autres décisions spécifiques donnant acte de retrait de recours, ce qui portait le total à 137 en 2015.

CHAPITRE X
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

X.1. COMPOSITION DU COMITÉ PERMANENT R

La composition du Comité permanent R n'a subi aucune modification en 2016 : la présidence a été assurée par Guy Rapaille (F), avocat général près la cour d'appel de Liège, tandis que les fonctions de conseiller ont été remplies par Gérald Vande Walle (F) et Pieter-Alexander De Brock (N).

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

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

X.2. RÉUNIONS AVEC LA COMMISSION DE SUIVI

Dans le courant de l'année 2016, six réunions ont eu lieu avec la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent des services de police et du Comité permanent des services de renseignement et de sécurité. Si cette commission comptait toujours treize membres avec voix délibérative[243], des changements sont néanmoins intervenus à plusieurs reprises en 2016. La commission était composée comme suit : Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Peter De Roover (N-VA), Laurette Onkelinx (PS), André Frédéric (PS), Denis Ducarme (MR), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld),

[243] 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* »).

Hans Bonte (sp.a), Gilles Vanden Burre (Ecolo-Groen) et George 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 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'. Il ne faut donc pas s'étonner que toutes les réunions de la Commission de suivi se soient tenues au premier semestre de 2016, et que l'accent ait été mis, à partir de ce moment-là, sur les activités de la commission d'enquête.

Lors des six réunions de la Commission, diverses 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 été discutées. Le *Rapport d'activités 2015* du Comité permanent R a également fait l'objet d'une discussion. La Commission a pris « *acte du rapport d'activités 2015 du Comité R et souscrit à ses recommandation* ».[244] Enfin, du temps a été consacré à un échange sur le rapport annuel concernant 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).

X.3. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

Les articles 52 à 55 L.Contrôle déterminent les cas où le Comité permanent R et le Comité permanent P doivent organiser des réunions communes et la manière dont ils doivent les organiser. La présidence de ces réunions communes est exercée en alternance par les présidents des deux Comités permanents (art. 54 L.Contrôle). Ces réunions poursuivent un double objectif: d'une part, échanger des informations, et d'autre part, initier des enquêtes de contrôle communes et discuter des enquêtes en cours. Début juillet 2016, une réunion spéciale a été entièrement consacrée à l'Organe de coordination de l'analyse de la menace. Le nouveau directeur de l'OCAM et son adjoint ont été invités à donner leur vision de l'OCAM. Une concertation a également été menée sur les problèmes budgétaires structurels auxquels sont confrontées toutes les instances à dotation. Les deux comités étaient d'accord sur le fait qu'il convenait de développer une

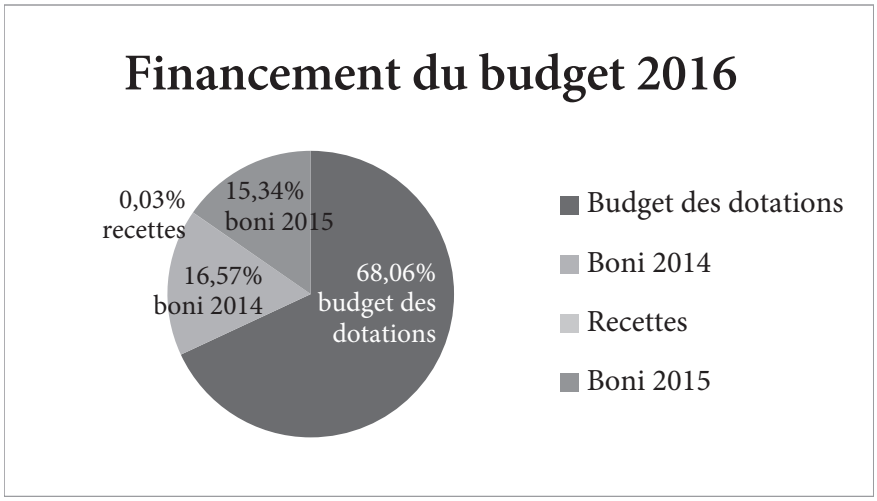
244 *Doc. parl.*, Chambre 2016-17, n° 54-2185/1 (Rapport d'activités 2015 du Comité permanent de contrôle des services de renseignement et de sécurité, Rapport fait au nom de la commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de contrôle des services de police et du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

méthodologie commune, en premier lieu pour les enquêtes de contrôle communes.

Sept réunions communes se sont tenues en 2016, en plus des contacts informels fréquents sur le terrain.

X.4. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Le budget 2016 du Comité permanent R a été fixé à 3,768 millions d'euros[245], soit une diminution de 2,48 % par rapport à 2015. Les sources de financement de ce budget ont été attribuées par la Chambre des Représentants[246] comme suit :



Tout en maintenant une réserve budgétaire nécessaire pour financer ses missions légales qui ont augmenté, en nombre et en volume, le Comité permanent R s'est inscrit dans une volonté de réduire ses budgets de fonctionnement, malgré un contexte très changeant.

L'exécution du budget 2016 a produit un boni comptable de 0,880 million d'euros, ce qui représente la différence entre les éléments constitutifs du budget et les dépenses constatées.

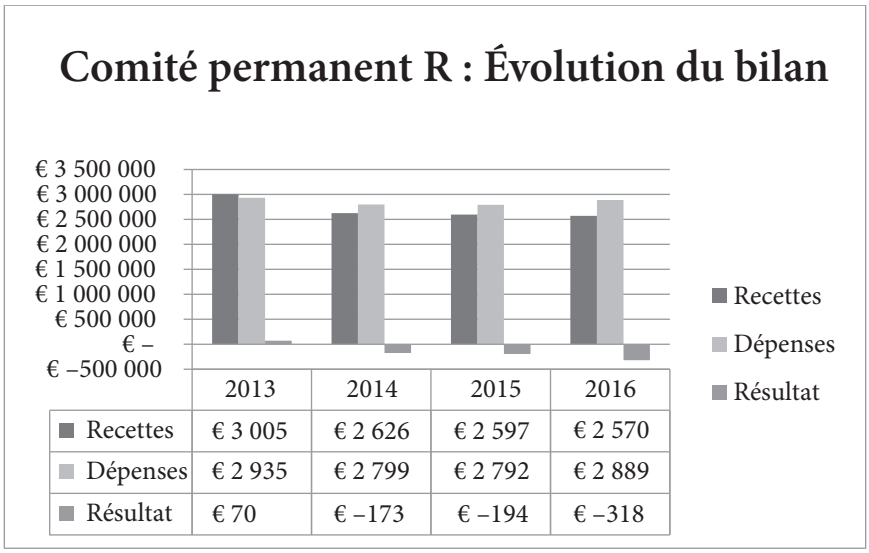
Cependant, la réalité financière donne lieu à un constat nettement moins favorable. L'article 57, alinéa 1er, L.Contrôle stipule que les crédits de fonctionnement doivent être inscrits au budget des dotations. Or, comme le

245 Loi du 18 décembre 2015 contenant le budget général des dépenses pour l'année budgétaire 2016, *M.B.* 30 décembre 2015.

246 *Doc. parl.*, Chambre 2015-2016, 54-1497/1, 20-22.

montre le tableau ci-dessus, le budget 2016 a été établi sur base de différentes sources de financement.

Le seul apport nouveau en termes de trésorerie nette est la dotation inscrite au budget général de l'État, ce qui se traduit au niveau du résultat d'exploitation par une perte de 0,319 million d'euros (en augmentation de 63,53 % par rapport à l'exercice budgétaire 2015 (- 0,195 million d'euros)). Il s'agit d'une tendance observée depuis quelques années et dont on peut affirmer qu'elle aura de graves conséquences à politique inchangée.



	2013	2014	2015	2016
Recettes	€ 3 005	€ 2 626	€ 2 597	€ 2 570
Dépenses	€ 2 935	€ 2 799	€ 2 792	€ 2 889
Résultat	€ 70	€ –173	€ –194	€ –318

La décision du Conseil des ministres du 15 octobre 2014 de diminuer chaque année de 2 %, de façon linéaire, le budget des dotations, associée à l'augmentation des dépenses réelles du Comité, va certainement accentuer cette tendance dans les années suivantes. En outre, le Comité se voit sans cesse confier de nouvelles missions (contrôle de la banque de données FTF, contrôle de nouvelles méthodes particulières de renseignement…), sans que le budget suive la même courbe.[247]

Lorsque les réserves constituées par les bonis des exercices antérieurs seront épuisées, le Comité permanent R risque bien d'être confronté à des problèmes de trésorerie, ce qui se traduira inévitablement par des problèmes de fonctionnement.

[247] La Commission de la Justice de la Chambre en a été informée explicitement à l'occasion de la discussion de la modification de la Loi organique des services de renseignement et de sécurité (L.R&S).

X.5. 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 des formations et conférences propres au secteur.[248] Concernant cette dernière catégorie, un ou plusieurs membre du Comité permanent R ou membre de son personnel ont assisté aux journées d'étude mentionnées ci-dessous.

DATE	TITRE	ORGANISATION	LIEU
2015-2016	Hautes études de sécurité et de défense, une opportunité multisectorielle	Institut royal supérieur de défense (IRSD)	Bruxelles
27-29 janvier 2016	(In)visibilities & Infrastructures	Computers, Privacy & Data Protection (CPDP)	Bruxelles
24 février 2016	Table ronde – Quelle gouvernance des services de renseignement dans une société démocratique ?	République tunisienne et Centre pour le contrôle démocratique des forces armées (DCAF)	Gammarth (Tunisie)
2 mars 2016	Counter-Terrorism, Security and Human Rights	Group of the Progressive Alliance of Socialists and Democrats in the European Parliament	Bruxelles
12 avril 2016	Intelligence and democratic oversight from the end of the Cold War until today – key trends and developments	EOS-Committee	Oslo (Norvège)
18 avril 2016	Comment lutter contre le terrorisme et par quels moyens ?	Université de Namur	Namur
29 avril 2016	Protection des données à caractère personnel en 5 questions	Université de Namur	Namur
13 mai 2016	'Big data' and intelligence services : perspectives and future challenges	Belgian Intelligence Studies Centre (BISC)	Wavre

248 Des formations ont été dispensées en interne, notamment plusieurs briefings de sécurité (auxquels les collaborateurs étaient tenus d'assister), ainsi que des formations liées au renseignement (p. ex. la conférence des Prof. Damien Van Puyvelde et Stephen Coulthard portant sur les thèmes suivants : *'Diversifying the US intelligence community workforce'* et *'Implementing structured analytical techniques'*) et celle du Prof. Matthew Levitt. En outre, des déjeuners-conférences ont été régulièrement organisés sur différents sujets (p. ex. avec Alain Grignard sur l'islam, avec Frank Schueremans et Koen Strobbe sur les banques de données policières…).

DATE	TITRE	ORGANISATION	LIEU
31 mai 2016	Radicalisering aanpakken : Nu of nooit !	Centre for Policing and Security (CPS)	Vilvorde
11-15 septembre 2016	World Summit on Counter-Terrorism – Unpuzzling Terrorism	International Institute for Counter-Terrorism	Herzliya (Israël)
29 septembre 2016	Rapport de la commission d'enquête sur les attentats de janvier et novembre 2015	Haut Comité Français pour la Défense Civile (HCFDC)	Paris
6 octobre 2016	Coopération internationale contre le terrorisme et échange de renseignements	Institut royal supérieur de défense (IRSD)	Bruxelles
10 octobre 2016	Les obligations de sécurité informatique des entreprises	Université de Namur	Namur
11-12 octobre 2016	International Intelligence Oversight Forum 2016	Special rapporteur on the right to privacy (United Nations)	Bucarest (Roumanie)
17 octobre 2016	Les enjeux de la vie privée des citoyens et la protection des données face aux nouvelles technologies	Sénat	Bruxelles
25 octobre 2016	La lutte contre le crime financier organisé : l'urgence d'une synergie des forces	Organisation internationale européenne de la lutte contre le crime financier	Bruxelles
28-29 octobre 2016	Witness to change. Intelligence analysis in a changing environment	Netherlands Intelligence Studies Association (NISA)	La Haye
7-8 novembre 2016	Table ronde – L'accès à l'information : défis et opportunités pour la communauté du renseignement	Centre pour le contrôle démocratique des forces armées (DCAF)	Gammarth (Tunisie)
28-29 novembre 2016	Surveillance, Oversight, and Human Rights in Counter Terrorism	Criminal Justice Centre, The Queen Mary Reflection Group on Terrorism and Human Rights	Paris
9 décembre 2016	Innovation and Information Technologies for the European security and intelligence community	Eurosint Forum	Paris

CHAPITRE XI
RECOMMANDATIONS

À la lumière des enquêtes de contrôle clôturées en 2016, 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 (XI.1), sur la coordination et l'efficacité des services de renseignement, de l'OCAM et des services d'appui (XI.2) et, enfin, sur l'optimalisation des possibilités de contrôle du Comité permanent R (XI.3).

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

XI.1.1. COMBLER UNE LACUNE EN MATIÈRE DE RÉTENTION DE DONNÉES[249]

Lors de l'élaboration de la réglementation relative au recours à des opérateurs (voir III.1.3), 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.

XI.1.2. UTILISATION DE RENSEIGNEMENTS RECUEILLIS DE MANIÈRE ILLÉGALE[250]

La VSSE et le SGRS peuvent bien évidemment 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

249 Cette recommandation découle du rapport sur l'application des méthodes particulières de renseignement par les services de renseignement et de sécurité et le contrôle effectué sur celles-ci par le Comité permanent R (2016).

250 Voir 'Chapitre II.1. La problématique des *foreign terrorist fighters*'.

(p. ex. l'OCAM). Dans ce contexte, le Comité avait déjà souligné par le passé[251] 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, refuser des données provenant de pays tiers qui ont été collectées illégalement.[252]

XI.1.3. ÉCHANGE D'INFORMATIONS ET COLLABORATION AVEC DES SERVICES ÉTRANGERS[253]

En ce qui concerne la collaboration avec des services étrangers, le Comité avait déjà insisté à plusieurs reprises sur une directive qui devait être émise par le Conseil national de sécurité.[254] Le 26 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'*[255], classifiée 'Confidentiel Loi 11.12.1998'. La transmission d'informations/de données à caractère personnel à des services étrangers n'y est cependant traitée que de manière sommaire. Le Comité maintient dès lors ses recommandations antérieures et juge l'initiative prioritaire. Il convient, de toute façon, de prêter attention au principe de prudence, que les services de renseignement sont tenus de respecter dans le cadre des échanges d'informations.

XI.1.4. ASSISTANCE TECHNIQUE PRÊTÉE À LA JUSTICE[256]

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.[257] Les services de renseignement doivent y veiller en permanence.

---

251 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 8-35.

252 Cf. *'Richtlijn aangaande de relaties van Belgische inlichtingendiensten met buitenlandse inlichtingendiensten'* du 26 septembre 2016 (Directive concernant les relations des services de renseignement belges avec les services de renseignement étrangers (traduction libre)), mettant notamment l'accent sur l'aspect 'respect des droits de l'homme'.

253 Voir 'Chapitre II.1. La problématique des *foreign terrorist fighters*' et 'Chapitre II.5. La protection du potentiel économique et scientifique et les révélations d'Edward Snowden'.

254 COMITÉ PERMANENT R, *Rapport d'activités 2014*, 116-117.

255 Directive concernant les relations des services de renseignement belges avec les services de renseignement étrangers (traduction libre).

256 Voir 'Chapitre II.1. La problématique des *foreign terrorist fighters*'.

257 COMITÉ PERMANENT R, *Rapport d'activités 2004*, 133 et *Rapport d'activités 2006*, 54-55. Le législateur MRD partageait donc la vision du Comité en la matière : si la proposition initiale prévoyait que la VSSE et le SGRS puissent utiliser des méthodes ordinaires et spécifiques dans des enquêtes pénales, cette possibilité n'a pas été retenue dans la réglementation finale.

XI.1.5. RESPECT DE L'ARTICLE 36*BIS* DE LA LOI VIE PRIVÉE[258]

Le Comité recommande à la VSSE de prendre les initiatives nécessaires pour satisfaire à l'obligation visée 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 »*.

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

XI.2.1. RECOMMANDATIONS SPÉCIFIQUES À LA LUTTE CONTRE LE TERRORISME ET CONTRE LE RADICALISME

XI.2.1.1. La collaboration au sein des local task forces (LTF)[259]

Le Comité permanent R recommande que les différents participants aux LTF s'informent mutuellement de leurs besoins et leurs possibilités, mais aussi de leurs limitations. Cette approche permettra à tous les participants de comprendre ce qu'une LTF peut fournir ou non. Dans le cas spécifique de la VSSE, il apparaît que les participants ne savent pas toujours clairement ce qu'ils peuvent dire ou non lors des réunions (informations classifiées). Le Comité recommande d'éclaircir ce point au sein des services, et que les représentants des services provinciaux participant aux réunions soient activement soutenus et orientés par l'administration centrale.

Le Comité permanent R a également recommandé que pour chaque information ou renseignement arrivant sur la table de la LTF, les services de renseignement déterminent le niveau de classification correct/adéquat.[260]

---

258 Protocole d'accord réglant la coopération entre la Sûreté de l'État (VSSE) et la Direction générale de l'Exécution des Peines et Mesures (DGEPM).

259 Voir 'Chapitre II.1. La problématique des *foreign terrorist fighters*'.

260 Une solution (ou du moins un début de solution) a été trouvée à la faveur de la nouvelle circulaire FTF. Celle-ci prévoit que la fonction d''*information officer (InfOffr)*' soit introduite au niveau de la Police locale. En tant que remplaçant du chef de corps, l'*information officer* représente la zone de police dans la LTF. Au sein de son organisation, il guide de manière transversale les efforts de recherche et de suivi en matière de *foreign fighters* et veille à la qualité du flux d'informations dans la zone. Il est le point de contact pour les services de

XI.2.1.2. La collaboration et les synergies entre les deux services de renseignement[261]

Dans le cadre de la problématique syrienne, la collaboration entre les deux services de renseignement était limitée et ponctuelle. Le Comité permanent R recommande que les deux services examinent les synergies possibles et l'éventualité d'une collaboration 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.

XI.2.1.3. Le HUMINT dans les milieux radicalisés et terroristes[262]

Les informations fournies via le HUMINT sont souvent décisives en termes d'apport utile à une stratégie disruptive ou dans la prévention d'un attentat. Même s'il n'est pas simple de recruter des sources dans les milieux terroristes et radicalisés, cela doit constituer une priorité.

XI.2.1.4. Du personnel doté de connaissances linguistiques et d'une connaissance du terrain[263]

Tant pour la gestion des informateurs dans les milieux radicaux (HUMINT) que pour le suivi des sources ouvertes (OSINT et SOCMINT), il est indiqué que les services puissent 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).

XI.2.1.5. Des analyses stratégiques dans la lutte contre le terrorisme[264]

La lutte contre le terrorisme exige souvent une réaction rapide. Les analystes n'ont donc pas souvent la possibilité de réaliser des analyses stratégiques, et la collecte d'informations est axée sur les besoins immédiats, plutôt que sur une analyse à long terme. La VSSE doit mener une réflexion sur sa particularité en

---

renseignement, l'OCAM et la Police fédérale pour l'échange d'informations classifiées. Il ou elle est titulaire, à l'instar du chef de corps, d'une habilitation de sécurité.

261 'Chapitre II.1. La problématique des *foreign terrorist fighters*' et 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris'.

262 Voir 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris'.

263 Voir 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris'. Le Comité avait déjà formulé une recommandation en ce sens : COMITÉ PERMANENT R, *Rapport d'activités 2007*, 74 ('VIII.2.4. Le recrutement de personnel disposant d'une connaissance de langues spécifiques').

264 Voir 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris'.

tant que service de renseignement et sur son rôle dans la lutte contre le terrorisme.

XI.2.2. RECOMMANDATIONS AYANT UNE PORTÉE GÉNÉRALE

XI.2.2.1. Un meilleur échange d'informations via des banques de données interconnectées[265]

L'échange d'informations est très important. 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 convient donc de tendre vers 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 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.

XI.2.2.2. Renseignements prédictifs[266]

Le Comité permanent R estime 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 et ce qu'on peut en attendre, et enfin comment les services pourraient concrétiser leurs ambitions en la matière.

XI.2.2.3. Utilisation de techniques d'analyse standardisées[267]

L'analyse est une composante essentielle du travail de renseignement. Il existe toutes sortes de techniques standardisées en matière d'analyse. 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 pouvant survenir dans les processus de renseignement et d'avoir, au final, une influence sur la position d'information.

---

265 Voir 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris'.

266 Voir 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris'.

267 Voir 'Chapitre II.1. La problématique des *foreign terrorist fighters*' et 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris'.

Le Comité constate que les services ne recourent pas de façon cohérente à des méthodes d'analyse formelles.[268] Il recommande dès lors aux services 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).

Une méthode importante consiste à établir divers scénarios (comme 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. Par exemple, un scénario terroriste a des composantes civiles *et* militaires, ce qui requiert une collaboration entre la VSSE et le SGRS.

XI.2.2.4. Approche planifiée de phénomènes[269]

Les processus de renseignement requièrent une approche planifiée ou une 'conception', qui détermine les questions posées dans le cadre de l'enquête concernant 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 du 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 idéalement aussi tenir compte et utiliser des capacités de collecte et d'analyse à l'extérieur du service, donc les capacités d'autres services.

XI.2.2.5. Consultation des clients[270]

Le Comité permanent R réitère sa recommandation[271] selon laquelle les deux services devraient demander explicitement à leurs 'clients' quels renseignements ils veulent exactement et comment ils évaluent les renseignements (*feedback*). Il s'agit d'une responsabilité partagée. D'une part, les services doivent spécifier à

---

268 Consciente de l'importance de telles techniques d'analyse, la VSSE a l'intention de les intégrer de manière structurelle dans les activités d'analyse.

269 Voir 'Chapitre II.1. La problématique des *foreign terrorist fighters*' et 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris'.

270 Voir 'Chapitre II.1. La problématique des *foreign terrorist fighters*'.

271 Voir notamment: COMITÉ PERMANENT R, *Rapport d'activités 2011*, 104-105 ('IX.2.2.1. Recommandations relatives aux conditions organisationnelles requises pour une affectation adéquate des moyens').

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 termes de renseignements.

XI.2.2.6. Forme et contenu des produits d'analyse[272]

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.

Par ailleurs, 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. Les destinataires doivent par ailleurs être spécifiés.

XI.2.2.7. Gestion des données au SGRS[273]

Le Comité permanent R recommande, et ce n'est pas la première fois[274], d'œuvrer de toute urgence à l'élaboration des bases 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).

XI.2.2.8. Traducteurs qualifiés pour le SIGINT[275]

Le Comité constate une nouvelle fois la nécessité, pour la section SIGINT du SGRS, de disposer de traducteurs qualifiés.

XI.2.2.9. Standardisation des procédures[276]

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

---

272 Voir 'Chapitre II.3. La position d'information des deux services de renseignement avant les attentats de Paris'.

273 Voir 'Chapitre II.1. La problématique des *foreign terrorist fighters*'.

274 À ce propos: COMITÉ PERMANENT R, *Rapport d'activités 2015*, 6 ('I.2.3. Gestion des informations au sein du SGRS').

275 Voir 'Chapitre IV. Le contrôle de l'interception de communications émises à l'étranger'.

276 Voir 'Chapitre II.2. La position d'information de la VSSE et l'attentat manqué du Thalys'.

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. Le travail que la VSSE a initié avec ses partenaires dans ce cadre doit être poursuivi.

XI.2.2.10. Enquête sur des flux d'informations et les moyens ICT[277]

Le Comité permanent R recommande à la VSSE de procéder à une enquête sur ses processus de travail, sur les flux d'informations et sur les moyens ICT qui supportent l'ensemble.

XI.2.3. RECOMMANDATIONS RELATIVES AUX MÉTHODES PARTICULIÈRES DE RENSEIGNEMENT

XI.2.3.1. Référence correcte dans les décisions MRD[278]

Le Comité recommande que, dans leurs décisions MRD, la VSSE et le SGRS se réfèrent explicitement, le cas échéant, à la nouvelle compétence pour suivre les activités de services de renseignement étrangers sur le territoire belge (voir III.1.1).

XI.2.3.2. Mise en œuvre de MRD à l'étranger[279]

Le SGRS dispose d'un mandat légal spécifique (art. 259*bis* § 5 CP *juncto* art. 11 § 2, 3° L.R&S) pour l'interception de communications émises à l'étranger, par exemple pour des motifs de sécurité et de protection des troupes belges et alliées lors de missions à l'étranger. Contrairement aux SIGINT qui peuvent être mis en œuvre à l'étranger, les MRD sont limitées au territoire national. Le Comité a rappelé[280] sa recommandation selon laquelle le législateur devrait mener un débat sur la nécessité de permettre l'utilisation de certaines MRD à l'étranger. La question a été résolue par la modification de loi du 30 mars 2017.

---

277 Voir 'Chapitre II.2. La position d'information de la VSSE et l'attentat manqué du Thalys'.

278 Cette recommandation découle du rapport sur l'application des méthodes particulières de renseignement par les services de renseignement et de sécurité et le contrôle effectué sur celles-ci par le Comité permanent R (2016).

279 Voir 'Chapitre II.1. La problématique des *foreign terrorist fighters*'.

280 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 114 et *Rapport d'activités 2014*, 122.

XI.2.3.3. Limitations dans la mise en œuvre des méthodes de renseignement[281]

Le Comité recommande que les autorités examinent l'efficacité des moyens d'action dont les services de renseignement et de sécurité disposent sur le terrain et les limitations actuelles (par exemple les cartes GSM prépayées anonymes).[282]

XI.2.4. RECOMMANDATIONS DANS LE CADRE DE LA PROTECTION DU POTENTIEL ÉCONOMIQUE ET SCIENTIFIQUE (PES)[283]

XI.2.4.1. 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.

XI.2.4.2. Une plateforme d'informations en matière de protection stratégique du PES

Le Comité permanent R recommande qu'une plateforme d'informations, par exemple dirigée par le Conseil national de sécurité, soit créée 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. À cet égard, 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 peut 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 cyber sécurité. Le Centre pour la cybersécurité peut jouer ici un rôle capital (et

281 Voir 'Chapitre II.2. La position d'information de la VSSE et l'attentat manqué du Thalys'.

282 Ce problème a été résolu en ce qui concerne la carte prépayée (voir III.1.4. 'L'identification d'un détenteur d'une carte prépayée).

283 Cette recommandation découle du 'Chapitre II.5. La protection du potentiel économique et scientifique et les révélations d'Edward Snowden'.

il le fera, à en croire sa présentation). 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.

XI.2.4.3. Homologation de systèmes ICT et cryptage

La mission d'homologation de systèmes ICT produits en Belgique, y compris leur cryptage, doit être confiée sans délai à un service public comme l'Autorité nationale de sécurité (ANS) ou au Centre pour la cybersécurité Belgique.

XI.2.4.4. Approbation de la liste PES du SGRS

L'approbation par le Conseil national de sécurité d'une liste d'acteurs (personnes physiques *et* morales) s'impose, et ce conformément aux dispositions de l'article 11 de la Loi de 1998 organique des services de renseignement et de sécurité. Il s'agit ici d'acteurs qui sont actifs dans les secteurs économiques et industriels liés à la défense.

XI.2.5. RECOMMANDATIONS EN MATIÈRE DE COLLABORATION AVEC LES ÉTABLISSEMENTS PÉNITENTIAIRES[284]

XI.2.5.1. Cap sur un nouveau protocole

Le Comité permanent R estime que le protocole de coopération entre la VSSE et DG EPI est dépassé dans sa forme actuelle. Il doit être adapté ou réécrit pour pouvoir anticiper des défis futurs, tels que de nouveaux phénomènes et de nouvelles évolutions en termes d'usages et de méthodes. En outre, des pratiques qui ont vu le jour au fil des ans, en marge du protocole actuel, doivent être intégrées à ce dernier ou être régularisées. Toutes les initiatives prises par la VSSE en dehors du protocole devraient être reprises dans celui-ci.

XI.2.5.2. Recommandations pour un meilleur échange d'informations et un meilleur traitement des informations

Dans le cadre des échanges d'informations, le Comité permanent R estime que, puisque les informations doivent être concentrées au siège de Bruxelles, il convient de privilégier un point de contact fixe (POC) par rapport à l'échange d'informations via des postes provinciaux de la VSSE.

284 Recommandations du 'Chapitre II. 6. La VSSE et le Protocole de coopération avec les Établissements pénitentiaires'.

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 le compartimentage inutile des différentes modalités d'échange d'informations).

XI.2.6. RECOMMANDATIONS DANS LE CADRE DE L'OCAM[285]

Les Comités permanents R et P recommandent à l'OCAM de :
- refuser toute demande d'évaluation d'une menace qui ne relève pas de sa compétence légale ;
- ne plus procéder à des détachements d'agents non statutaires des services d'appui sans une éventuelle modification de la loi ;
- régulariser la situation administrative de ces personnes détachées ;
- constituer un dossier personnel pour chaque membre du personnel, qu'il ou elle soit statutaire, ou détaché(e), et même de la direction ;
- soumettre aux ministres compétents des propositions de modifications de l'Arrêté royal réglant le statut du personnel statutaire et détaché ;
- 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 gestion, en vertu duquel la personne concernée par la mesure doit être entendue.

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

XI.3.1. LE PLAN D'ÉCOUTES[286]

La liste d'interceptions est trop souvent transmise avec retard.[287] Le Comité n'est donc pas en mesure d'assurer pleinement sa mission de contrôle. Il recommande dès lors que cette liste lui soit envoyée à temps. En outre, le Comité a une nouvelle fois insisté sur l'importance d'une description plus précise des personnes et des organisations visées.

---

285 Recommandation du 'Chapitre II.13. Dysfonctionnements spécifiques au sein de l'OCAM'.

286 Voir 'Chapitre IV. Le contrôle de l'interception de communications émises à l'étranger'.

287 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 103 ('IX.3.2. L'envoi à temps des interceptions de sécurité visées') et *Rapport d'activités 2015*, 71. Le Comité n'a reçu le Plan d'écoutes 2017 qu'en juillet 2017.

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 2016 AU 31 DÉCEMBRE 2016)

Loi 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

Loi 29 janvier 2016 modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique, *M.B.* 24 février 2016

Loi 21 avril 2016 portant des dispositions diverses Intérieur – police intégrée, *M.B.* 29 avril 2016

Loi 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme, *M.B.* 9 mai 2016

Loi 29 mai 2016 relatif à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.* 18 juillet 2016

Loi 12 juillet 2016 contenant le premier ajustement du budget général des dépenses pour l'année budgétaire 2016, *M.B.* 14 septembre 2016

Loi 1er septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, *M.B.* 7 décembre 2016

Loi du 7 décembre 2016 insérant un article 106/1 dans la loi du 13 juin 2005 relative aux communications électroniques, *M.B.* 19 décembre 2016

Loi du 21 novembre 2016 modifiant diverses dispositions relatives au statut des militaires, *M.B.* 23 décembre 2016

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

Extrait de l'arrêt n° 108/2016 du 14 juillet 2016, numéro du rôle: 6045, En cause: le recours en annulation de la loi du 18 mars 2014 relative à la gestion de l'information policière et modifiant la loi du 5 août 1992 sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction criminelle, introduit par l'ASBL « Liga voor Mensenrechten » et l'ASBL « Ligue des Droits de l'Homme », *M.B.* 13 octobre 2016

A.R. 7 mars 2016 modifiant l'arrêté royal du 26 janvier 2006 relatif à la création d'un Comité fédéral pour la Sûreté du Transport ferroviaire et portant diverses mesures pour la sûreté du transport intermodal, *M.B.* 1er avril 2016

A.R. 19 février 2016 portant exécution des articles 13, 24 et 25 de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour le secteur du Transport, sous–secteur du transport ferroviaire, *M.B.* 7 avril 2016

A.R. 1er mai 2016 portant fixation du plan d'urgence national relatif à l'approche d'une prise d'otage terroriste ou d'un attentat terroriste, *M.B.* 18 mai 2016

A.R. 23 mai 2016 accordant une indemnité de transfert aux assistants de protection de la Sûreté de l'État transférés à la police fédérale, *M.B.* 27 mai 2016

A.R. 23 mai 2016 organisant le transfert des assistants de protection de la Sûreté de l'État vers la police fédérale, *M.B.* 30 mai 2016

A.R. 4 mai 2016 portant répartition partielle, pour ce qui concerne des dédommagements et des frais de justice, du crédit provisionnel inscrit au programme 03-41-1 du budget général des dépenses pour l'année budgétaire 2016 et destiné à couvrir des dépenses non structurelles concernant la sécurité, *M.B.* 13 juin 2016

A.R. 6 juin 2016 modifiant l'arrêté royal du 4 juillet 2014 fixant le statut de certains agents civils du département d'état-major renseignement et sécurité des forces armées, *M.B.* 5 juillet 2016

A.R. 27 juin 2016 modifiant l'arrêté royal du 23 janvier 2007 relatif au personnel de l'Organe de coordination pour l'analyse de la menace, *M.B.* 25 juillet 2016

A.R. 21 juillet 2016 complétant la liste des personnes et entités visée aux articles 3 et 5 de l'arrêté royal du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme, *M.B.* 28 juillet 2016

A.R. 3 juillet 2016 portant exécution de I'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, *M.B.* 3 août 2016

A.R. 10 juillet 2016 modifiant l'arrêté royal du 5 décembre 2006 relatif à l'administration générale et à la cellule d'appui de la Sûreté de l'État, *M.B.* 12 août 2016

A.R. 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters et portant exécution de certaines dispositions de la section Ibis « de la gestion des informations » du chapitre IV de la loi sur la fonction de police, *M.B.* 22 septembre 2016

A.R. 28 septembre 2016 relatif à l'armement des agents de police, *M.B.* 4 octobre 2016

A.R. 26 septembre 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.* 13 octobre 2016

A.R. 3 novembre 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.* 25 novembre 2016

A.R. 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée, *M.B.* 7 décembre 2016

A.M. 28 septembre 2016 relatif à la formation en armement des agents de police, *M.B.* 4 octobre 2016

A.M. 14 novembre 2016 portant désignation d'un comité de sélection chargé de l'évaluation des candidatures pour la fonction de directeur de l'analyse de la Sûreté de l'État, *M.B.* 21 novembre 2016

Appel aux candidats pour la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité, *M.B.* 19 janvier 2016

Comité permanent de contrôle des services de renseignement et de sécurité, recrutement pour l'entrée en service immédiate et constitution d'une réserve de recrutement d'une secrétaire francophone statutaire (m/f) (niv. B), *M.B.* 17 février 2016

Sélection comparative d'inspecteurs pour les Services extérieurs (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État (SPF Justice) (ANG16050), *M.B.* 1er mars 2016

Sélection comparative d'inspecteurs pour les Services extérieurs (m/f/x) (niveau B), francophones, pour la Sûreté de l'État (SPF Justice) (AFG16050), *M.B.* 1er mars 2016

Sélection comparative de traducteurs (m/f/x) (niveau A), néerlandophones pour la Sûreté de l'État (ANG16056), *M.B.* 18 mars 2016

Sélection comparative d'un analyste en matière d'intelligence économique (m/f/x) (niveau A1), francophone, pour le Ministère de la Défense (AFG16021), *M.B.* 1er avril 2016

Sélection comparative d'un analyste en matière d'intelligence économique (m/f/x) (niveau A1), néerlandophone, pour le Ministère de la Défense (ANG16046), *M.B.* 1er avril 2016

Recrutement pour l'entrée en service immédiate et constitution d'une réserve de recrutement d'un(e) juriste statutaire (m/f) (niv. A) pour le Comité permanent de contrôle des services de renseignement et de sécurité, *M.B.* 13 avril 2016

Sélection comparative d'administrateurs réseau (m/f/x) (niveau B), néerlandophones, pour le Sûreté de l'État (ANG16022), *M.B.* 4 mai 2016

Sélection comparative d'experts de Cyber Security, néerlandophones – clôture, *M.B.* 17 mai 2016

Sélection comparative de gestionnaires de bases de données (m/f/x), francophones, pour la Sûreté de l'État (AFG15193), *M.B.* 23 mai 2016

Sélection comparative d'analystes, néerlandophones (m/f/x) pour l'Organe de Coordination pour l'Analyse de la Menace (OCAM) (niveau A3) pour le SPF Intérieur (ANG16124), *M.B.* 27 mai 2016

Sélection comparative d'analystes, francophones (m/f/x) pour l'Organe de Coordination pour l'Analyse de la Menace (OCAM) (niveau A3) pour le SPF Intérieur (AFG16096), *M.B.* 27 mai 2016

Sélection comparative de traducteurs (m/f/x) (niveau A), francophones, pour l'Organe de Coordination pour l'Analyse de la Menace – SPF Intérieur (AFG16131), *M.B.* 15 juillet 2016

Sélection comparative de collaborateurs Helpdesk IT (m/f/x) (niveau C), francophones, pour la Sûreté de l'État SPF Justice (AFG16138), *M.B.* 16 août 2016

Sélection comparative de collaborateurs Helpdesk IT (m/f/x) (niveau C), néerlandophones, pour la Sûreté de l'État SPF Justice (ANG16169), *M.B.* 16 août 2016

Sélection comparative de conseiller général Relations internationales pour la Sûreté de l'État (m/f/x) (niveau A4), francophones, pour la Sûreté de l'État SPF Justice (AFG16156), *M.B.* 23 septembre 2016

Sélection comparative de conseiller général Relations internationales pour la Sûreté de l'État (m/f/x) (niveau A4), néerlandophones, pour la Sûreté de l'État SPF Justice (ANG16187), *M.B.* 23 septembre 2016

Règlement d'ordre intérieur de la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité (Commission BIM), *M.B.* 27 septembre 2016

Circulaire modifiant la circulaire GPI 62 du 14 février 2008 relative à l'armement de la police intégrée, structurée à deux niveaux, *M.B.* 4 octobre 2016

La sélection comparative d'analystes (m/f/x) (niveau A), néerlandophones, pour l'Organe de Coordination pour l'Analyse de la Menace (ANG16124), a été clôturée le 28 septembre 2016, *M.B.* 10 octobre 2016

Sélection comparative des porte-paroles (m/f/x) (niveau A), néerlandophones, pour la Sûreté de l'État, *M.B.* 4 novembre 2016

Emploi vacant de directeur de l'analyse de la Sûreté de l'État – appel aux candidats, *M.B.* 10 novembre 2016

Résultat de la sélection comparative de conseiller généraux Relations internationales (m/f/x) (niveau A4), néerlandophones pour la Sûreté de l'État, *M.B.* 7 décembre 2016

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 2016 AU 31 DÉCEMBRE 2016)

Sénat

Rapport sur la radicalisation en Belgique, *Doc. parl.*, Sénat, 2015-2016, nº 6-205/1

Par lettre du 22 novembre 2016, le président du Comité permanent de Contrôle des services de renseignement et de sécurité a transmis au Sénat, le rapport d'activités pour 2015, *Ann. Parl.*, Sénat, 2016-2017, 16 décembre 2016, nº 6-24, p. 40

Chambre des Représentants

Note d'orientation politique du secrétaire d'État à la Lutte contre la fraude sociale, à la Protection de la vie privée et à la Mer du Nord, *Doc. parl.*, Chambre, 2015-2016, nº 54-20/63

Proposition de loi modifiant la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de

renseignement étrangers en Belgique, *Doc. parl.*, Chambre, 2015-2016, nos 54-0553/4, 54-0553/5, 54-0553/6 et 54-0553/7

Projet de loi modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice, *Doc. parl.*, Chambre, 2015-2016, no 54-1418/9

Projets et propositions de loi déposés, *C.R.I.*, Chambre, 2015-2016, 14 janvier 2016, PLEN 094, p. 34

Renvoi d'une proposition en commission pour avis, *C.R.I.*, Chambre, 2015-2016, 14 janvier 2016, PLEN 094, p. 41.

Prise en considération de propositions, *C.R.I.*, Chambre, 2015-2016, 14 janvier 2016, PLEN 094, p. 41.

Projet de loi modifiant le droit pénal et la procédure pénale et portant des dispositions diverses en matière de justice (1418/1-13) – Proposition de loi modifiant le Code d'instruction criminelle en ce qui concerne l'extension de la mini instruction à la perquisition (108/1-4) – Proposition de loi modifiant la loi du 17 avril 1878 contenant le titre préliminaire du Code de procédure pénale en vue d'établir de meilleurs délais de prescription pour les abus sexuels commis sur des personnes mineures en cas d'unité d'intention (758/1-2) – Proposition de loi modifiant les articles 399, 400 et 405*bis* du Code pénal en ce qui concerne les coups et blessures volontaires (969/1-2) – Proposition de loi modifiant l'article 35, § 2, de la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme (1139/1-2) – Proposition de loi modifiant, en ce qui concerne l'absence de condamnations antérieures, la loi du 29 juin 1964 concernant la suspension, le sursis et la probation (1368/1-2) – Proposition de loi modifiant le Code pénal en ce qui concerne l'incapacité temporaire et permanente (1369/1-2) – Proposition de loi modifiant le Code judiciaire en vue d'assurer le bon fonctionnement et la continuité du parquet fédéral (1385/1-2), *C.R.I.*, Chambre, 2015-2016, 28 janvier 2016, PLEN 096, p. 51.

Proposition de loi visant à améliorer la coopération entre la CTIF et les organismes chargés de la lutte contre le terrorismes, *Doc. parl.*, Chambre, 2015-2016, no 54-1544/3

Projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques, *Doc. parl.*, Chambre, 2015-2016, nos 54-1567/12, 54-1567/13 et 54-1567/14

Renvoi de la proposition de loi élargissant l'utilisation des données obtenues dans le cadre de l'échange automatique de renseignements (n° 1589/1) à la commission temporaire « lutte contre le terrorisme », *C.R.I.*, Chambre, 2015-2016, 4 février 2016, PLEN 097, p. 53

Proposition de modification du Règlement de la Chambre des représentants en ce qui concerne la composition de la commission chargée du suivi du Comité permanent P et du Comité permanent R, *Doc. parl.*, Chambre, 2015-2016, no 54-1598/1

Proposition de loi complétant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, en ce qui concerne le financement d'associations incitant à la haine, à la discrimination, à la violence ou à la ségrégation, *Doc. parl.*, Chambre, 2015-2016, no 54-1620/1

Proposition modifiant le chapitre X et l'article 151 du Règlement de la Chambre des représentants en vue d'étendre la compétence de la Commission spéciale chargée des

achats militaires à la vente de matériel militaire par la Défense, *Doc. parl.*, Chambre, 2015-2016, nº 54-1621/1

Proposition de résolution pour une lutte efficace et démocratique contre le terrorisme, *Doc. parl.*, Chambre, 2015-2016, nº 54-1624/1

Proposition visant à instituer une commission d'enquête parlementaire chargée d'enquêter sur la cellule terroriste molenbeekoise qui a commis une série d'attentats à Paris, *Doc. parl.*, Chambre, 2015-2016, nº 54-1626/1 à 54-1626/3

Proposition de loi modifiant la loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace du 18 juillet 1991, *Doc. parl.*, Chambre, 2015-2016, nº 54-1629/1 et *C.R.I.*, Chambre, 2015-2016, 4 février 2016, PLEN 097, p. 54

Projet de loi portant des dispositions diverses – Intérieur – Police intégrée (1644/1-5) – discussion générale, *C.R.I.*, Chambre, 2015-2016, 3 mars 2016, PLEN 100, p. 40

Projet de loi portant des dispositions diverses – Intérieur – Police intégrée, *Doc. parl.*, Chambre, 2015-2016, nº 54-1644/1

Proposition de loi créant un Comité permanent de contrôle de la sécurité des infrastructures publiques fédérales, *Doc. parl.*, Chambre, 2015-2016, nº 54-1660/1

Proposition de loi modifiant la loi du 5 août 1992 sur la fonction de police en vue de permettre une transmission efficace des données relatives aux combattants terroristes étrangers, *Doc. parl.*, Chambre, 2015-2016, nº 54-1711/1

Projet de loi relatif à des mesures complémentaires en matière de lutte contre le terrorisme), *Doc. parl.*, Chambre, 2015-2016, nºs 54-1727/1 à 54-1727/8

Proposition visant à instituer une commission d'enquête parlementaire chargée d'enquêter sur les informations à disposition des enquêteurs avant les attentats de Paris et sur la manière dont elles ont été traitées, *Doc. parl.*, Chambre, 2015-2016, nº 54-1742/1

Échange de vues avec M. Miguel De Bruycker, directeur du Centre pour la Cybersécurité en Belgique, *Doc. parl.*, Chambre, 2015-2016, nº 54-1744/1

Prise en considération de propositions – conformément à l'avis de la Conférence des présidents du 7 avril 2016, je vous propose de prendre en considération la proposition (M. Patrick Dewael, Mmes Meryame Kitir et Catherine Fonck) visant à instituer 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, nº 1752/1, *C.R.I.*, Chambre, 2015-2016, 12 avril 2016, PLEN 104, p. 2

Proposition visant à instituer 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, *Doc. parl.*, Chambre, 2015-2016, nº 54-1752/5

Proposition de résolution demandant la désignation d'un commissaire du gouvernement chargé de coordonner le suivi des Foreign Terrorist Fighters et de remédier aux dysfonctionnements dans la politique de sécurité, *Doc. parl.*, Chambre, 2015-2016, nº 54-1785/1

Renvoi de propositions de loi à une autre commission de la proposition de loi (MM. Marco Van Hees et Raoul Hedebouw) modifiant la loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace du 18 juillet 1991, nº 1629/1, *C.R.I.*, Chambre, 2015-2016, 28 avril 2016, PLEN 108, p. 112

Projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques (1567/1-14), *C.R.I.*, Chambre, 2015-2016, 4 mai 2016, PLEN 109, p. 47

Projet de loi contenant l'ajustement du budget des Voies et Moyens de l'année budgétaire 2016, *Doc. parl.*, Chambre, 2015-2016, nº 54-1804/3

Projet de loi contenant le premier ajustement du Budget général des dépenses de l'année budgétaire 2016, *Doc. parl.*, Chambre, 2015-2016, nos 54-1805/3 et 54-1805/5

Projet 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, *Doc. parl.*, Chambre, 2015-2016, nº 54-1829/1

Proposition de résolution relative à la lutte contre les chaînes satellitaires, les stations de radio et les sites Internet islamiques qui diffusent une propagande anti-occidentale haineuse et violente sur le territoire belge et européen, *Doc. parl.*, Chambre, 2015-2016, nº 54-1874/1

Proposition de loi modifiant, en ce qui concerne le fonctionnement de l'Organe de contrôle de l'information policière, 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, 2015-2016, nº 54-1943/2

Projet de loi portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, *Doc. parl.*, Chambre, 2015-2016, nos 54-1964/1 à 54-1964/3 et *C.R.I.*, Chambre, 2015-2016, 20 juillet 2016, PLEN 123, p. 42

Échange de vues sur le Plan national de sécurité et la Note-cadre de sécurité intégrale 2016-2019, *Doc. parl.*, Chambre, 2015-2016, nº 54-2026/1

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 54-2043/1 et 54-2043/2

Projet de loi portant diverses dispositions en matière de fonction publique, *Doc. parl.*, Chambre, 2016-2017, nº 54-2064/3

Projet de loi relatif au traitement des données des passagers, *Doc. parl.*, Chambre, 2015-2016, nos 54-2069/1 à 54-2069/3 et54-2069/5

Proposition de résolution visant à la création d'une agence fédérale du renseignement, *Doc. parl.*, Chambre, 2016-2017, nº 54-2086/1

Demandes d'urgence émanant du gouvernement lors du dépôt du projet de loi relatif au traitement des données des passagers, n° 2069/1, *C.R.I.*, Chambre, 2016-2017,
13 octobre 2016, PLEN 130, p. 74

Discussion de la déclaration du gouvernement, *C.R.I.*, Chambre, 2016-2017, 17 octobre 2016, PLEN 132, p. 4 et *C.R.I.*, Chambre, 2016-2017, 17 octobre 2016, PLEN 134, p. 1

Projet de loi relatif au traitement des données des passagers (2069/1-8), *C.R.I.*, Chambre, 2016-2017, 23 novembre 2016, PLEN 140, p. 105

Proposition de loi modifiant le Code pénal en ce qui concerne la répression du terrorisme (1579/1-12), *C.R.I.*, Chambre, 2016-2017, 1er décembre 2016, PLEN 142, p. 44

Projet de loi contenant le budget des Voies et Moyens de l'année budgétaire 2017, *Doc. parl.*, Chambre, 2016-2017, nos 54-2108/1, 54-2108/3 et 54-2108/5

Projet du budget général des dépenses pour l'année budgétaire 2017, *Doc. parl.*, Chambre, 2016-2017, nos 54-2109/1 et 54-2109/3

Justification du budget général des dépenses pour l'année budgétaire 2017, *Doc. parl.*, Chambre, 2016-2017, no 54-2110/2

Note de politique générale – Justice, *Doc. parl.*, Chambre, 2016-2017, nos 54-2111/6, 54-2111/7, 54-2111/17, 54-2111/20 et 54-2111/21

Proposition de résolution visant le désengagement de la Défense de l'opération Vigilant Guardian au profit d'un corps policier spécifique, *Doc. parl.*, Chambre, 2016-2017, no 54-2156/1

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, 2016-2017, no 54-2179/6

Projet de loi visant à approuver le compte général de l'Administration générale pour l'année 2015 et des comptes d'exécution des budgets des Services de l'État à gestion séparée pour des années précédentes, *Doc. parl.*, Chambre, 2016-2017, nos 54-2192/1

Proposition de loi modifiant le Code pénal en ce qui concerne la répression du terrorisme (1579/1-12), *C.R.I.*, Chambre, 2016-2017, 1er décembre 2016, PLEN 142, p. 44

Projet de loi relatif au traitement des données des passagers (2069/1-9), *C.R.I.*, Chambre, 2016-2017, 21 décembre 2016, PLEN 148, p. 1

Projet de loi relatif à l'amélioration des méthodes particulières de recherche et de certaines mesures d'enquête concernant Internet, les communications électroniques et les télécommunications (1966/1-10), *C.R.I.*, Chambre, 2016-2017, 21 décembre 2016, PLEN 150, p. 5

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, Commission BIM, Organe de contrôle de l'information policière et Commission fédérale de déontologie – Comptes de l'année budgétaire 2015 – Ajustements budgétaires de l'année 2016 – Propositions budgétaires pour l'année 2017, *Doc. parl.*, Chambre, 2016-2017, nos 54-2225/1 à 54-2225/3 et *C.R.I.*, Chambre, 2016-2017, 22 décembre 2016, PLEN 151, p. 25 et 39

Comptes de l'année budgétaire 2015 du Comité permanent de contrôle des services de renseignements et de sécurité (2225/1), *C.R.I.*, Chambre, 2016-2017, 22 décembre 2016, PLEN 151, p. 58

Propositions budgétaires pour l'année budgétaire 2017 du Comité permanent de contrôle des services de renseignements et de sécurité (2225/1), *C.R.I.*, Chambre, 2016-2017, 22 décembre 2016, PLEN 151, p. 59

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 2016 AU 31 DÉCEMBRE 2016)

Sénat

Question écrite de J.-J. De Gucht au ministre de l'Intérieur sur la 'radicalisation – secret professionnel lié à la profession ou à la fonction – possibilité de signaler des faits de radicalisation – vie privée' (Sénat, 2015-2016, 13 janvier 2016, Q. nº 6-802)

Question écrite de J.-J. De Gucht au ministre de la Justice sur la 'radicalisation – secret professionnel lié à la profession ou à la fonction – possibilité de signaler des faits de radicalisation – vie privée' (Sénat, 2015-2016, 13 janvier 2016, Q. nº 6-803)

Question écrite de J.-J. De Gucht au secrétaire d'État à la Lutte contre la fraude sociale sur la 'radicalisation – secret professionnel lié à la profession ou à la fonction – possibilité de signaler des faits de radicalisation – vie privée' (Sénat, 2015-2016, 13 janvier 2016, Q. nº 6-804)

Question écrite de J.-J. De Gucht au ministre de la Justice sur la 'accueil des réfugiés – radicalisation – aide – pratiques de recrutement – exemple de la fondation Al-Ighaatha – détenus – coopération avec les autorités néerlandaises' (Sénat, 2015-2016, 4 février 2016, Q. nº 6-823)

Question écrite de J.-J. De Gucht au ministre de l'Intérieur sur le 'salafisme – dons à des terroristes condamnés – suivi et dépistage – gel des fonds' (Sénat, 2015-2016, 31 mars 2016, Q. nº 6-901)

Question écrite de P. Van Rompuy au ministre de l'Intérieur sur les 'combattants partis en Syrie – registre de la population – radiation – procédure – chiffres' (Sénat, 2015-2016, 25 avril 2016, Q. nº 6-934)

Question écrite de J.-J. De Gucht au ministre de l'Intérieur sur la 'radicalisation – phase de préparation des jihadistes – petite criminalité – signal d'alarme dans la détection et la prévention' (Sénat, 2015-2016, 7 juillet 2016, Q. nº 6-998)

Question écrite de J.-J. De Gucht au ministre de l'Intérieur sur les 'prédicateurs de haine – chiffres – lutte – condamnation – retrait de visa – liste européenne' (Sénat, 2015-2016, 7 juillet 2016, Q. nº 6-1000)

Question écrite de J.-J. De Gucht au ministre des Affaires étrangères sur les 'prédicateurs de haine – chiffres – lutte – condamnation – retrait de visa – liste européenne' (Sénat, 2015-2016, 7 juillet 2016, Q. nº 6-1001)

Question écrite de J.-J. De Gucht au ministre de la Justice sur les 'prédicateurs de haine – chiffres – lutte – condamnation – retrait de visa – liste européenne' (Sénat, 2015-2016, 7 juillet 2016, Q. nº 6-1002)

Question écrite de J.-J. De Gucht au ministre de l'Intérieur sur les 'réseaux jihadistes – premiers stades – détection accélérée études approfondies – accès des enquêteurs aux informations confidentielles' (Sénat, 2015-2016, 12 juillet 2016, Q. nº 6-1009)

Question écrite de J.-J. De Gucht au ministre de la Justice sur les 'réseaux jihadistes – premiers stades – détection accélérée études approfondies – accès des enquêteurs aux informations confidentielles' (Sénat, 2015-2016, 12 juillet 2016, Q. nº 6-1010)

Question écrite de B. Anciaux au ministre de la Mobilité sur la 'protection du Roi et d'autres personnalités de haut rang – sécurité routière – sécurité des usagers ordinaires de la route – danger – règlementation' (Sénat, 2015-2016, 21 octobre 2016, Q. nº 6-741)

Question écrite de J.-J. De Gucht au ministre de l'Intérieur sur le 'terrorisme – passé criminel – recrutement de criminels dans des réseaux jihadistes – nouvelle étude – politique carcérale surpopulation – détection de la radicalisation – formation des membres du personnel des prisons' (Sénat, 2016-2017, 26 octobre 2016, Q. nº 6-1072)

Question écrite de J.-P. Wahl au ministre de la Justice sur les 'prisons – radicalisation – lutte – Direction générale Établissements pénitentiaires (DG EPI) – agents coordinateurs – rôle – évolution – formation – nombre' (Sénat, 2015-2016, 7 juillet 2016, Q. nº 6-1140)

Chambre des Représentants

Question de S. Van Hecke au ministre de la Justice sur 'le protocole d'accord entre la Banque nationale et la Sûreté de l'État' (*C.R.I.*, Chambre, 2015-2016, 6 janvier 2016, COM 301, p. 3, Q. nº 8170)

Question de M. Van Hees au ministre de l'Intérieur sur les 'belges radicalisés – communes vigilantes' (*Q.R.*, Chambre, 2015-2016, 11 janvier 2016, nº 057, p. 188, Q. nº 732)

Question de R. Deseyn au ministre de la Coopération au développement sur le 'Service de Médiation pour les télécommunications – rétention des données' (*Q.R.*, Chambre 2015-2016, 11 janvier 2016, nº 057, p. 230, Q. nº 296)

Question d'A. Top au ministre de la Défense sur le 'fonctionnement du système BINII' (*Q.R.*, Chambre, 2015-2016, 11 janvier 2016, nº 057, p. 503, Q. nº. 505)

Échange de vues avec le ministre de la Défense et questions jointes de S. Pirlot, W. De Vriendt, P. Buysrogge, A. Top, V. Yüksel, R. Hedebouw et G. Dallemagne sur 'le plan stratégique de la Défense' (*C.R.I.*, Chambre, 2015-2016, 13 janvier 2016, COM 305, p. 1, Q. nºs 97, 8140, 8154, 99, 8417, 8425 et 8447)

Question de S. Van Hecke au ministre de la Justice sur 'le transfert de la mission de protection des personnes de la Sûreté de l'État vers la police' (*C.R.I.*, Chambre, 2015-2016, 13 janvier 2016, COM 306, p. 7, Q. nº 8253)

Questions jointes de P. Vanvelthoven, É. Thiébaut, J.-M. Nollet, M. Van Hees et K. Jadin au ministre de l'Intérieur sur 'les incidents techniques de certaines centrales nucléaires belges' (*C.R.I.,* Chambre, 2015-2016, 13 janvier 2016, COM309, 15, Q. nºs. 8113, 8131, 8141, 8142, 8143, 8158, 8220, 8221, 100 et 8151)

Question d'A. Top au ministre de la Justice sur 'la possibilité pour les agents de la Sûreté de l'État de surfer anonymement' (*C.R.I.*, Chambre, 2015-2016, 20 janvier 2016, COM 314, p. 8, Q. nº 8460)

Question de K. Metsu ministre de la Justice sur 'l'imam Tarik Ibn Ali' (*C.R.I.*, Chambre, 2015-2016, 20 janvier 2016, COM 314, p. 28, Q. nº 8602)

Question de Ph. Pivin au ministre de l'Intérieur sur 'le niveau d'alerte terroriste et les fédérations de commerçants' (*C.R.I.*, Chambre, 2015-2016, 20 janvier 2016, COM 316, p. 29, Q. nº 8397)

Questions jointes de G. Dallemagne, H. Bonté et N. Ben Hamou au ministre de l'Intérieur sur 'les initiatives en matière de lutte contre le terrorisme' (*C.R.I.,* Chambre, 2015-2016, 21 janvier 2016, PLEN095, 7, Q. n$^{OS.}$ 937 à 939)

Question de K. Jadin au ministre de l'Intérieur sur le 'niveau d'alerte augmenté dans les centres d'accueil' (*Q.R.*, Chambre, 2015-2016, 25 janvier 2016, n° 059, p. 147, Q. n° 910)

Question de V. Yüksel au ministre de la Justice sur le 'scandale chez VW – incidence sur le parc automobile du SPF Justice' (*Q.R.*, Chambre, 2015-2016, 25 janvier 2016, n° 059, p. 170, Q. n° 617)

Question d'A. Carcaci au premier ministre sur '12 mesures pour lutter plus efficacement contre le terrorisme' (*C.R.I.*, Chambre, 2015-2016, 26 janvier 2016, COM 317, p. 14, Q. n° 8720)

Question de R. Hedebouw au premier ministre sur 'la transparence et le contrôle parlementaire relatif au Conseil national de sécurité et la détermination du niveau de menace' (*C.R.I.*, Chambre, 2015-2016, 26 janvier 2016, COM 317, p. 37, Q. n° 8840)

Question de V. Van Peel au ministre des Classes moyennes sur 'le secret professionnel et l'obligation de signalement des CPAS' (*C.R.I.*, Chambre, 2015-2016, 27 janvier 2016, COM 323, p. 4, Q. n° 8014)

Question de B. Pas au premier ministre sur 'la connaissance de longue date par les services belges de sécurité de l'existence de la cellule terroriste de Paris et de ses projets' (*C.R.I.,* Chambre, 2015-2016, 28 janvier 2016, PLEN096, 23, Q. n° 970)

Question de F. Schepmans au ministre de l'Intérieur sur 'les résultats du projet BELFI' (*Q.R.*, Chambre, 2015-2016, 1er février 2016, n° 60, p. 110, Q. n° 856)

Question de Ph. Pivin au ministre de la Justice sur 'la Sûreté de l'État et la coopération avec l'Office des Étrangers' (*C.R.I.*, Chambre, 2015-2016, 3 février 2016, COM 334, p. 30, Q. n° 9089)

Question d'E. Kir au ministre de l'Intérieur sur 'les propos du ministre dans la presse et l'image de la communauté musulmane qui est y véhiculée' (*C.R.I.*, Chambre, 2015-2016, 3 février 2016, COM 335, p. 7, Q. n° 8624)

Question de G. Dallemagne au ministre de l'Intérieur sur 'l'effectivité de la surveillance FTF à travers les task forces mises en place dans les communes bruxelloises' (*C.R.I.*, Chambre, 2015-2016, 3 février 2016, COM 335, p. 30, Q. n° 8640)

Questions jointes de V. Yüksel au ministre de l'Intérieur sur 'la création d'un centre européen de lutte contre le terrorisme' (*C.R.I.*, Chambre, 2015-2016, 3 février 2016, COM 335, p. 43, Q. n^{os} 8912 et 8980)

Question d'O. Chastel au secrétaire d'État à l'Asile et la Migration sur le 'centre d'accueil dans la caserne d'Elsenborn' (*Q.R.*, Chambre, 2015-2016, 8 février 2016, n° 61, p. 478, Q. n° 413)

Questions jointes de W. De Vriendt et A. Top au ministre de la Défense sur 'les attachés de défense et le trafic d'armes' (*C.R.I.*, Chambre, 2015-2016, 17 février 2016, COM 337, p. 18, Q. n^{os} 8771 et 8790)

Questions jointes de K. Jadin, B. Hellings et Ph. Pivin au ministre des Affaires étrangères sur 'le screening des personnes travaillant dans les centrales nucléaires' (*C.R.I.*, Chambre, 2015-2016, 17 février 2016, COM 340, p. 36, Q. n^{os} 8994, 9000 et 9088)

Questions jointes de M. de Lamotte, J.-M. Nollet et Ph. Pivin au ministre de l'Intérieur sur 'la sécurité dans les installations nucléaires et autour de celles-ci' (*C.R.I.*, Chambre, 2015-2016, 18 février 2016, PLEN 098, p. 20, Q. n^{os} 1004, 1005 et 1006)

Question de K. Metsu au ministre de la Justice sur les 'poursuites pour la diffusion de films de propagande de l'État islamique (EI)' (*Q.R.*, Chambre, 2015-2016, 23 février 2016, nº 63, p. 236, Q. nº 687)

Question de D. Ducarme au ministre de la Défense sur 'la mission 'Resolute Support'' (*Q.R.*, Chambre, 2015-2016, 23 février 2016, nº 63, p. 430, Q. nº 548)

Question de N. Lanjri au secrétaire d'État à l'Asile et la Migration sur 'l'exécution du plan de répartition européen' (*Q.R.*, Chambre, 2015-2016, 23 février 2016, nº 63, p. 464, Q. nº 453)

Question d'A. Top au ministre de la Défense sur 'la présence de militaires dans les rues' (*Q.R.*, Chambre, 2015-2016, 29 février 2016, nº 64, p. 408, Q. nº 560)

Question de B. Pas au secrétaire d'État à l'Asile et la Migration sur 'des visites de sympathisants djihadistes aux centres d'asile' (*C.R.I.*, Chambre, 2015-2016, 2 mars 2016, COM 353, p. 15, Q. nº 8690)

Échange de vues et questions jointes d'A. Top, G. Vanden Burre, R. Hedebouw, N. Ben Hamou, E. Kir, O. Maingain, K. Degroote, F. Schepmans, G. Dallemagne, S. Lahaye-Battheu et W. Demeyer avec le ministre de l'Intérieur sur 'le plan Canal' (*C.R.I.*, Chambre, 2015-2016, 2 mars 2016, COM 358, p. 1, Q. nºs 9115, 9335, 9357, 9526, 9529, 9630, 9725, 9728, 9809, 9831, 9849, 9859 et 9861)

Questions jointes d'O. Maingain, A. Carcaci, S. Van Hecke, K. Degroote et S. Lahaye-Battheu au premier ministre sur 'l'enregistrement des empreintes digitales sur la carte d'identité' (*C.R.I.*, Chambre, 2015-2016, 3 mars 2016, PLEN 100, p. 7, Q. nºs 1036 à 1040)

Question de J.-M.Nollet au ministre de l'Intérieur sur 'les téléphones cryptés dans le cadre d'enquêtes judiciaires' (*Q.R.*, Chambre, 2015-2016, 7 mars 2016, nº 65, p. 214, Q. nº 904)

Question de F. Dewinter au ministre de l'Intérieur sur 'le retour en Belgique de combattants partis en Syrie et/ou de membres du groupe EI' (*Q.R.*, Chambre, 2015-2016, 7 mars 2016, nº 65, p. 226, Q. nº 952)

Question de Ph. Goffin au ministre de l'Intérieur sur 'l'accès des services de police aux renseignements de l'OCAM' (*Q.R.*, Chambre, 2015-2016, 7 mars 2016, nº 65, p. 230, Q. nº 966)

Question de S. Crusnière au ministre des Affaires étrangères sur 'la Tunisie' (*Q.R.*, Chambre, 2015-2016, 7 mars 2016, nº 65, p. 266, Q. nº 323)

Question de Ph. Goffin au ministre de l'Intérieur sur 'les mesures de sécurité à l'égard du palais de justice de Liège' (*Q.R.*, Chambre, 2015-2016, 14 mars 2016, nº 66, p. 132, Q. nº 967)

Question de D. Ducarme au ministre de la Coopération au développement sur 'l'état de la législation et de la réglementation belges encadrant l'usage de logiciels de cryptage de données' (*Q.R.*, Chambre, 2015-2016, 14 mars 2016, nº 66, p. 177, Q. nº 423)

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, 2015-2016, 14 mars 2016, nº 66, p. 199, Q. nº 609)

Question de D. Ducarme au secrétaire d'État à l'Asile et la Migration sur 'Fedasil – radicalisme' (*Q.R.*, Chambre, 2015-2016, 14 mars 2016, nº 66, p. 363, Q. nº 494)

Questions jointes d'É. Thiébaut, G. Dallemagne, B. Hellings, B. Pas, H. Bonte, K. Degroote, Ph. Pivin et V. Yüksel au ministre l'Intérieur sur 'les perquisitions

menées à Forest' (*C.R.I.*, Chambre, 2015-2016, 17 mars 2016, PLEN 102, p. 2, Q. nos 1078 à 1085)

Question de F. Dewinter au ministre de la Justice sur le 'flux financiers en provenance de pays arabes ou de régimes extrémistes musulmans et destinés à des mosquées ou à des associations musulmanes établies dans notre pays' (*Q.R.*, Chambre, 2015-2016, 21 mars 2016, no 67, p. 252, Q. no 667)

Échange de vues avec le ministre de l'Intérieur sur 'les attentats terroristes' (*C.R.I.*, Chambre, 2015-2016, 25 mars 2016, COM 373, p. 1)

Question de N. Lijnen au ministre de la Défense sur 'OTAN et UE – cyberdéfense' (*Q.R.*, Chambre, 2015-2016, 4 avril 2016, no 68, p. 387, Q. no 574)

Question de Ph. Pivin au ministre de la Défense sur la 'sécurité et protection au sein des administrations publiques fédérales' (*Q.R.*, Chambre, 2015-2016, 4 avril 2016, no 68, p. 409, Q. no 591)

Questions jointes de Ph. Blanchart et S. Crusnière au ministre de la Justice sur 'la rencontre avec M. Mehmet Görmez, le président de la Diyanet' (*C.R.I.*, Chambre, 2015-2016, 13 avril 2016, COM 379, p. 65, Q. nos 10206 et 10234)

Question d'I. De Coninck à la ministre de la Mobilité sur 'la présence de terroristes parmi les membres du personnel des chemins de fer' (*C.R.I.*, Chambre, 2015-2016, 13 avril 2016, COM 381, p. 30, Q. no 10486)

Questions jointes de B. Pas, V. Yüksel et K. Lalieux à la ministre de la Mobilité sur 'la lettre ouverte de la police aéronautique concernant le problème de la sécurité à Zaventem' (*C.R.I.*, Chambre, 2015-2016, 13 avril 2016, COM 381, p. 41, Q. nos 138, 10561 et 10651)

Questions jointes de V. Yüksel, A. Top et V. Matz au ministre de l'Intérieur sur 'la liste des combattants de l'EI' (*C.R.I.*, Chambre, 2015-2016, 13 avril 2016, COM 382, p. 28, Q. nos 10093, 10095 et 10116)

Question de J.-J. Flahaux au ministre de l'Intérieur sur 'les contrôles à la frontière franco-belge' (*Q.R.*, Chambre, 2015-2016, 14 avril 2016, no 69, p. 172, Q. no 1017)

Question de F. Schepmans au ministre de l'Intérieur sur 'l'application du retrait des cartes d'identités' (*Q.R.*, Chambre, 2015-2016, 14 avril 2016, no 69, p. 192, Q. no 1131)

Question de B. Pas au ministre des Affaires étrangères sur les 'ANS – attestations de sécurité – radicalisme' (*Q.R.*, Chambre, 2015-2016, 14 avril 2016, no 69, p. 251, Q. no 507)

Question de Ph. Goffin au ministre de la Justice sur 'les mesures de sécurité à l'égard du palais de justice de Liège' (*Q.R.*, Chambre, 2015-2016, 14 avril 2016, no 69, p. 278, Q. no 777)

Question de Ph. Pivin au secrétaire d'État à l'Asile et la Migration sur 'le demandeur d'asile arrêté' (*C.R.I.*, Chambre, 2015-2016, 20 avril 2016, COM 387, p. 1, Q. no 9091)

Question de Ph. Pivin au secrétaire d'État à l'Asile et la Migration sur 'la Sûreté de l'État et la coopération avec l'Office des Étrangers' (*C.R.I.*, Chambre, 2015-2016, 20 avril 2016, COM 387, p. 14, Q. no 9582)

Question de K. Jadin au secrétaire d'État à l'Asile et la Migration sur 'le rapatriement des illégaux marocains' (*C.R.I.*, Chambre, 2015-2016, 20 avril 2016, COM 387, p. 45, Q. no 9870)

Questions jointes d'A. Top, S. Pirlot, B. Hellings, D. Clarinval et V. Yüksel au ministre de la Défense sur 'la présence accrue de militaires dans les rues' (*C.R.I.*, Chambre, 2015-

2016, 20 avril 2016, COM 388, p. 23, Q. nos 10620, 10638, 10667, 10723, 10809 et 10819)

Question de G. Dallemagne au ministre de la Justice sur 'le contrôle de certains lieux de culte' (*C.R.I.*, Chambre, 2015-2016, 20 avril 2016, COM 391, p. 10, Q. no 10238)

Question de L. Onkelinx au Premier ministre sur 'la conférence de presse de l'OCAM' (*C.R.I.*, Chambre, 2015-2016, 21 avril 2016, PLEN 107, p. 8, Q. no 1115)

Question de K. Van Vaerenbergh au ministre de l'Intérieur sur les 'missions de protection – mesures de sécurité' (*Q.R.*, Chambre, 2015-2016, 25 avril 2016, no 70, p. 107, Q. no 823)

Question de F. Schepmans au ministre des Affaires étrangères sur 'l'EU INTCEN' (*Q.R.*, Chambre, 2015-2016, 25 avril 2016, no 70, p. 182, Q. no 517)

Question de G. Dallemagne au ministre des Affaires étrangères sur 'le harcèlement à l'encontre de l'opposition démocratique rwandaise en Belgique' (*Q.R.*, Chambre, 2015-2016, 25 avril 2016, no 70, p. 185, Q. no 522)

Question de Ph. Pivin au ministre des Affaires étrangères sur 'Actiris – lutte contre le radicalisme' (*Q.R.*, Chambre, 2015-2016, 25 avril 2016, no 70, p. 187, Q. no 529)

Question de Ph. Pivin au ministre des Affaires étrangères sur la 'STIB – lutte contre le radicalisme' (*Q.R.*, Chambre, 2015-2016, 25 avril 2016, no 70, p. 189, Q. no 530)

Question de V. Yüksel au ministre de la Défense sur 'l'utilisation de rayonnements électromagnétiques à des fins de brouillage' (*Q.R.*, Chambre, 2015-2016, 25 avril 2016, no n 70, p. 314, Q. no 631)

Question de R. Hedebouw au ministre de l'Intérieur sur 'l'approche de la lutte anti–terroriste par le gouvernement' (*C.R.I.*, Chambre, 2015-2016, 27 avril 2016, COM 399, p. 15, Q. no 10453)

Question de R. Hedebouw au ministre de l'Intérieur sur 'les Belges partis combattre en Syrie' (*C.R.I.*, Chambre, 2015-2016, 27 avril 2016, COM 399, p. 17, Q. nos10456 et 10457)

Question d'A. Carcaci au ministre de l'Intérieur sur 'l'ouverture d'une section secondaire à une école fondamentale islamique à Schaerbeek' (*C.R.I.*, Chambre, 2015-2016, 27 avril 2016, COM 400, p. 2, Q. no10963)

Questions jointes de G. Gilkinet au ministre de la Justice sur 'l'utilisation de la possibilité de gel des fonds et des ressources économiques dans le cadre de la lutte contre le terrorisme' (*C.R.I.*, Chambre, 2015-2016, 27 avril 2016, COM 400, p. 11, Q. nos 11070 et 11071)

Question de H. Bonte au premier ministre sur 'le suivi des djihadistes rentrés de Syrie' (*C.R.I.*, Chambre, 2015-2016, 28 avril 2016, PLEN 108, p. 12, Q. no 1135)

Question de F. Dewinter au ministre de l'Intérieur sur 'le screening des combattants de l'État islamique parmi les candidats à l'asile' (*Q.R.*, Chambre, 2015-2016, 29 avril 2016, no 71, p. 91, Q. no 1154)

Question de Ph. Pivin au ministre de l'Intérieur sur la 'procédure de recrutement des aspirants inspecteurs de la police – screening' (*Q.R.*, Chambre, 2015-2016, 29 avril 2016, no 71, p. 124, Q. no 1136)

Question de B. Pas au ministre de la Défense sur 'la présence d'extrémistes musulmans dans l'armée' (*Q.R.*, Chambre, 2015-2016, 29 avril 2016, no 71, p. 256, Q. no 636)

Question d'I. De Coninck au ministre de la Mobilité sur la 'radicalisation au sein du personnel aéroportuaire' (*Q.R.*, Chambre, 2015-2016, 29 avril 2016, no 71, p. 280, Q. no 1241)

Question de G. Dallemagne au ministre de l'Intérieur sur 'l'évolution du nombre de départs de combattants étrangers vers la Syrie' (*C.R.I.*, Chambre, 2015-2016, 4 mai 2016, PLEN 109, p. 17, Q. nº 1160)

Question de K. Gabriëls au premier ministre sur 'la coordination de la lutte contre le financement du terrorisme' (*Q.R.*, Chambre, 2015-2016, 9 mai 2016, nº 72, p. 54, Q. nº 131)

Questions jointes de P.-O. Delannois et Ph. Blanchart au ministre de l'Intérieur sur 'la sécurité des grands évènements dans les mois à venir' (*C.R.I.*, Chambre, 2015-2016, 11 mai 2016, COM 411, p. 28, Q. nºs 10705 et 10706)

Questions jointes de V. Matz et K. Gabriëls au ministre de l'Intérieur sur 'la sûreté des aéroports' (*C.R.I.*, Chambre, 2015-2016, 11 mai 2016, COM 411, p. 39, Q. nºs 10823 et 10824)

Questions jointes de M. De Lamotte et Ph. Blanchart au ministre de l'Intérieur sur 'le risque de cyberattaques contre des centrales nucléaires' (*C.R.I.*, Chambre, 2015-2016, 11 mai 2016, COM 411, p. 47, Q. nºs 10905 et 11450)

Question de J.-M. Nollet au ministre de l'Intérieur sur 'le niveau de la menace pour le secteur nucléaire' (*C.R.I.*, Chambre, 2015-2016, 11 mai 2016, COM 411, p. 59, Q. nº 10988)

Question de B. Hellings au ministre de la Justice sur 'le fichage potentiel de 1200 ressortissants belgo-turcs par la Turquie et la mise en œuvre de la loi modifiant la loi du 30 novembre 1998 des services de renseignement et de sécurité, concernant le contrôle des activités des services de renseignement étrangers en Belgique' (*C.R.I.*, Chambre, 2015-2016, 11 mai 2016, COM 413, p. 21, Q. nº 11150)

Questions jointes de K. Metsu et C. Cassart-Mailleux au ministre de la Défense sur 'le Selor' (*C.R.I.*, Chambre, 2015-2016, 11 mai 2016, COM 414, p. 13, Q. nºs 10671, et 10883)

Débat d'actualité et questions jointes de G. Grovonius, D. Van der Maelen, W. De Vriendt, J.-J. Flahaux, S. Claerhout et N. Lijnen au ministre des Affaires étrangères sur 'la mission du ministre en Israël et en Palestine' (*C.R.I.*, Chambre, 2015-2016, 11 mai 2016, COM 418, p. 1, Q. nºs 10327, 10791, 10928, 11294, 11423, 11455 et 11469)

Question de G. Vanden Burre au de la Justice sur 'l'inauguration de la première aile pour détenus 'radicalisés' de la prison d'Ittre' (*C.R.I.*, Chambre, 2015-2016, 18 mai 2016, COM 423, p. 9, Q. nº 11282)

Question de J.-J. Flahaux au ministre de l'Intérieur sur 'le sommet de Washington pour la sécurité nucléaire' (*C.R.I.*, Chambre, 2015-2016, 18 mai 2016, COM 424, p. 16, Q. nº 11087)

Question de V. Yüksel au ministre de l'Intérieur sur 'l'application de la loi du 10 août 2015 concernant le retrait des cartes d'identité des djihadistes partis en Syrie (*C.R.I.*, Chambre, 2015-2016, 18 mai 2016, COM 424, p. 61, Q. nº 11595)

Questions jointes de K. Calvo, O. Maingain, M. Kitir, D. Ducarme, C. Fonck, P. Dedecker et J.-M. Nollet au premier ministre sur 'l'appel de dirigeants d'entreprise' (*C.R.I.*, Chambre, 2015-2016, 19 mai 2016, PLEN 111, p. 20, Q. nº 1210 à 1214, 1216 et 1217)

Question de V. Matz au ministre de l'Intérieur sur 'le transfert des assistants de protection de la Sûreté de l'État vers la police fédérale' (*C.R.I.*, Chambre, 2015-2016, 25 mai 2016, COM 428, p. 14, Q. nº 11567)

Question de N. Ben Hamou au ministre de l'Intérieur sur 'un protocole d'alerte dans les lieux à risque' (*C.R.I.*, Chambre, 2015-2016, 25 mai 2016, COM 428, p. 22, Q. nº 11613)

Question de N. Ben Hamou au ministre de l'Intérieur sur 'les retraits de cartes d'identité aux personnes radicalisées' (*C.R.I.*, Chambre, 2015-2016, 25 mai 2016, COM 428, p. 46, Q. nº 11690)

Questions jointes de V. Matz et G Vanden Burre au ministre de l'Intérieur sur 'le plan d'urgence national relatif à l'approche d'une prise d'otage terroriste ou d'un attentat terroriste' (*C.R.I.*, Chambre, 2015-2016, 25 mai 2016, COM 428, p. 54, Q. nºs 11752 et 11775)

Question de Ph. Pivin au ministre de l'Intérieur sur 'les vols de cartes d'identité dans les administrations' (*C.R.I.*, Chambre, 2015-2016, 25 mai 2016, COM 428, p. 64, Q. nº 11780)

Question de G. Gilkinet au ministre de la coopération au développement sur 'la sécurité des agents des SPF' (*Q.R.*, Chambre, 2015-2016, 30 mai 2016, nº 75, p. 120, Q. nº 505)

Question de R. Deseyn au ministre de l'Énergie sur 'le service d'inspection de l'infrastructure critique' (*Q.R.*, Chambre, 2015-2016, 30 mai 2016, nº 75, p. 217, Q. nº 267)

Question de D. Ducarme au ministre de la Défense sur 'le recrutement du personnel à la Défense nationale' (*Q.R.*, Chambre, 2015-2016, 30 mai 2016, nº 75, p. 245, Q. nº 685)

Questions jointes de K. Jadin, V. Yüksel, S. Pirlot et T. Vandenput au ministre de la Défense sur 'l'utilisation de drones pour certaines missions de surveillance' (*C.R.I.*, Chambre, 2015-2016, 31 mai 2016, COM 430, p. 22, Q. nºs 11092, 11183, 11313 et 11948)

Question de S. Pirlot au ministre de la Défense sur 'le budget exceptionnel promis pour la sécurité par le gouvernement' (*C.R.I.*, Chambre, 2015-2016, 31 mai 2016, COM 430, p. 32, Q. nº 11484)

Questions jointes de K. Gabriëls et M. De Coninck au secrétaire d'État à l'Asile et la Migration sur 'la transposition de la directive relative au permis de séjour et de travail unique pour les travailleurs non ressortissants de pays de l'Union européenne' (*C.R.I.*, Chambre, 2015-2016, 1er juin 2016, COM 435, p. 5, Q. nºs 11145 et 11328)

Question de F. Dewinter au ministre de l'Intérieur sur 'les événements organisés par Halal Events en Ardenne' (*C.R.I.*, Chambre, 2015-2016, 2 juin 2016, PLEN 113, p. 37, Q. nº 1265)

Question de Ph. Blanchart au ministre de la Coopération au développement sur 'la visite effectuée au Maroc concernant la lutte contre le terrorisme' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 168, Q. nº 141)

Question de D. Ducarme au ministre de l'Intérieur sur 'le nombre de jihadistes en Libye' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 291, Q. nº 1247)

Question de D. Ducarme au ministre de l'Intérieur sur le 'risque de départs de « foreign fighters » belges vers la Libye' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 294, Q. nº 1265)

Question de V. Yüksel au ministre de la Coopération au développement sur les 'brouilleurs' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 329, Q. nº 528)

Question de G. Gilkinet au ministre des Affaires étrangères sur 'la sécurité des agents des SPF' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 341, Q. nº 548)

Question de G. Dallemagne au ministre des Affaires étrangères sur les 'mise sur écoute par la NSA' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 352, Q. nº 574)

Question de J.-M. Nollet au ministre des Affaires étrangères sur les 'retraits d'accréditation dans le secteur du nucléaire' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 354, Q. nº 576)

Question de G. Dallemagne au ministre des Affaires étrangères sur le 'fichier de recrues de l'État Islamique' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 362, Q. nº 587)

Question de G. Dallemagne au ministre des Affaires étrangères sur les 'enjeux du prochain sommet de l'OTAN à Varsovie' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 366, Q. nº 602)

Question de V. Yüksel au ministre de la Défense sur les 'brouilleurs' (*Q.R.*, Chambre, 2015-2016, 6 juin 2016, nº 76, p. 499, Q. nº 688)

Question d'A. Top au ministre de l'Intérieur sur 'le désengagement des drones au port d'Anvers' (*C.R.I.*, Chambre, 2015-2016, 8 juin 2016, COM 441, p. 48, Q. nº 11877)

Question de Ph. Pivin au ministre de l'Intérieur sur 'la sécurisation des retransmissions publiques pendant l'Euro de football' (*C.R.I.*, Chambre, 2015-2016, 8 juin 2016, COM 441, p. 31, Q. nº 11984)

Question de J. Penris au ministre de l'Intérieur sur 'la communication aux banques de noms des djihadistes' (*C.R.I.*, Chambre, 2015-2016, 9 juin 2016, PLEN 114, p. 19, Q. nº 1280)

Question de D. Ducarme au ministre de l'Intérieur sur la 'liste de 22.000 djihadistes' (*Q.R.*, Chambre, 2015-2016, 13 juin 2016, nº 77, p. 289, Q. nº 1261)

Question de V. Yüksel au ministre de la Justice sur 'le nombre de combattants rentrés de Syrie dans notre pays' (*C.R.I.*, Chambre, 2015-2016, 15 juin 2016, COM 444, p. 22, Q. nº 12399)

Question de J. Klaps au ministre de l'Emploi sur 'la réparation des dégâts causés par les attentats' (*C.R.I.*, Chambre, 2015-2016, 15 juin 2016, COM 446, p. 28, Q. nº 12040)

Questions jointes de V. Matz, M. Kitir, K. Degroote et Ph. Pivin au ministre de l'Intérieur sur 'la menace terroriste' (*C.R.I.*, Chambre, 2015-2016, 16 juin 2016, PLEN 115, p. 23, Q. nºs 1301 à 1304)

Question de V. Matz au ministre de l'Intérieur sur 'l'entraînement de groupes radicaux sur notre territoire et les moyens d'action pour s'y opposer' (*C.R.I.*, Chambre, 2015-2016, 22 juin 2016, COM 453, p. 9, Q. nº 12038)

Question de G. Dallemagne au ministre de l'Intérieur sur 'les désertions multiples au sein du groupe État islamique' (*C.R.I.*, Chambre, 2015-2016, 22 juin 2016, COM 453, p. 50, Q. nº 12338)

Question de K. Gabriëls au ministre de l'Intérieur sur 'le contrôle du domicile des djihadistes revenus de Syrie' (*C.R.I.*, Chambre, 2015-2016, 23 juin 2016, PLEN 116, p. 34, Q. nº 1327)

Question jointes d'E. Massin et Ph. Goffin au ministre de la Justice sur 'le secret des sources journalistiques' (*C.R.I.*, Chambre, 2015-2016, 23 juin 2016, PLEN 116, p. 38, Q. nºs 1329 et1330)

Question de V. Scourneau au ministre de l'Intérieur sur 'les menaces de contamination des châteaux et réservoirs d'eau' (*Q.R.*, Chambre, 2015-2016, 24 juin 2016, nº 79, p. 97, Q. nº 1243)

Question de D. Ducarme au ministre de l'Intérieur sur 'Daech – les femmes combattantes belges' (*Q.R.*, Chambre, 2015-2016, 24 juin 2016, nº 79, p. 105, Q. nº 1259)

Question de K. Metsu au ministre de l'Intérieur sur 'les enfants recrutés par Daech' (*Q.R.*, Chambre, 2015-2016, 24 juin 2016, nº 79, p. 111, Q. nº 1279)

Question d'O. Chastel au ministre de l'Intérieur sur 'l'accord sur la sécurité et l'échange de données entre la Belgique et le Maroc' (*Q.R.*, Chambre, 2015-2016, 24 juin 2016, nº 79, p. 121, Q. nº 1301)

Question d'A. Top au ministre de la Défense sur 'les centres de Systema en Belgique' (*C.R.I.*, Chambre, 2015-2016, 29 juin 2016, COM 457, p. 1, Q. nº 11182)

Question d'A. Top au ministre de la Défense sur 'l'interception par la Belgique d'avions russes' (*C.R.I.*, Chambre, 2015-2016, 29 juin 2016, COM 457, p. 16, Q. nº 12160)

Question de S. Van Hecke au ministre de la Justice sur 'le retour des magistrats après un détachement' (*C.R.I.*, Chambre, 2015-2016, 29 juin 2016, COM 459, p. 31, Q. nº 12762)

Question de B. Hellings au ministre de l'Intérieur sur 'le 'soutien aérien' de la police fédérale par des drones dans le contrôle des migrants en province de Flandre occidentale' (*C.R.I.*, Chambre, 2015-2016, 29 juin 2016, COM 461, p. 4, Q. nº 12313)

Question de Ph. Pivin au ministre de l'Intérieur sur 'les analyses par l'OCAM du niveau d'alerte pour les commissariats de police' (*C.R.I.*, Chambre, 2015-2016, 29 juin 2016, COM 461, p. 25, Q. nº 12626)

Question de V. Yüksel au ministre de l'Intérieur sur 'le retrait des cartes d'identité des djihadistes partis en Syrie (bis)' (*C.R.I.*, Chambre, 2015-2016, 29 juin 2016, COM 461, p. 47, Q. nº 12810)

Question de D. Ducarme au ministre de la Justice sur 'l'action contre les données cryptées sur les ordinateurs de suspects dans le cadre de la lutte contre le terrorisme' (*Q.R.*, Chambre, 2015-2016, 1er juillet 2016, nº 80, p. 231, Q. nº 867)

Question de P. Buysrogge au Premier ministre sur 'le rapport du Comité R sur l'attention (ou le manque d'attention) que les services de renseignement belges portent aux menaces que peuvent représenter pour le potentiel scientifique et économique de la Belgique, des programmes de surveillance électronique de systèmes de communication et d'information mis en œuvre à grande échelle par des puissances et/ou services de renseignement étrangers' (*C.R.I.*, Chambre, 2015-2016, 5 juillet 2016, COM 463, p. 16, Q. nº 12275)

Question de D. Ducarme au ministre de l'Intérieur sur la 'Fédéral Computer Crime Unit' (*Q.R.*, Chambre, 2015-2016, 8 juillet 2016, nº 81, p. 126, Q. nº 1332)

Question de F. Dewinter au ministre de l'Intérieur sur 'les combattants syriens' (*Q.R.*, Chambre, 2015-2016, 8 juillet 2016, nº 81, p. 132, Q. nº 1381)

Question de G. Calomne au ministre de de la Défense sur 'la sécurisation des transmissions entre les attachés militaires et les services de la Défense' (*Q.R.*, Chambre, 2015-2016, 8 juillet 2016, nº 81, p. 283, Q. nº 729)

Question de G. Dallemagne au ministre des Classes moyennes sur 'le secret professionnel et le transfert d'informations par les travailleurs sociaux de CPAS' (*C.R.I.*, Chambre, 2015-2016, 13 juillet 2016, COM 477, p. 5, Q. nº 11216)

Question de B. Pas au ministre de l'Intérieur sur 'la communication des noms des extrémistes musulmans aux banques dans le cadre du financement du terrorisme' (*C.R.I.*, Chambre, 2015-2016, 13 juillet 2016, COM 478, p. 4, Q. nº 12690)

Question de P.-O. Delannois au ministre de l'Intérieur sur 'l'habilitation de sécurité pour les bourgmestres lors des grands événements' (*C.R.I.*, Chambre, 2015-2016, 13 juillet 2016, COM 478, p. 23, Q. nº 13075)

Question de D. Ducarme au ministre de l'Emploi sur le 'retrait d'habilitations au SPF Économie' (*Q.R.*, Chambre, 2015-2016, 15 juillet 2016, nº 82, p. 244, Q. nº 919)

Question de Ch. D'Haese au ministre de la Justice sur les 'Services publics fédéraux et institutions publiques – politique du personnel' (*Q.R.*, Chambre, 2015-2016, 15 juillet 2016, nº 82, p. 281, Q. nº 865)

Question de F. Dewinter au ministre de la Défense sur 'les moyens de fonctionnement des services de sécurité' (*Q.R.*, Chambre, 2015-2016, 15 juillet 2016, nº 82, p. 451, Q. nº 737)

Question de F. Dewinter au ministre de la Défense sur le 'personnel des services de sécurité. – Arabe' (*Q.R.*, Chambre, 2015-2016, 15 juillet 2016, nº 82, p. 453, Q. nº 738)

Question de P. Buysrogge au ministre de la Défense sur le 'VSSE et SGRS – fonds pour la rémunération des informateurs – rapport d'enquête de contrôle' (*Q.R.*, Chambre, 2015-2016, 15 juillet 2016, nº 82, p. 455, Q. nº 742)

Question de V. Scourneau au ministre de la Justice sur 'le cryptage des smartphones' (*Q.R.*, Chambre, 2015-2016, 25 juillet 2016, nº 83, p. 165, Q. nº 888)

Question de V. Yüksel au ministre de la Défense sur 'les nominettes apposées sur les uniformes – l'utilisation des médias sociaux par les militaires' (*Q.R.*, Chambre, 2015-2016, 25 juillet 2016, nº 83, p. 301, Q. nº 761)

Question d'O. Chastel au ministre de la Défense sur 'la cellule radicalisation' (*Q.R.*, Chambre, 2015-2016, 25 juillet 2016, nº 83, p. 372, Q. nº 671)

Question de F. Dewinter au ministre de la Justice sur 'Sharia4Belgium' (*Q.R.*, Chambre, 2015-2016, 1er août 2016, nº 84, p. 141, Q. nº 1199)

Question de F. Dewinter au ministre de la Justice sur 'la présence de combattants djihadistes belges à l'étranger' (*Q.R.*, Chambre, 2015-2016, 1er août 2016, n° 84, p. 142, Q. nº 1201)

Question de F. Dewinter au ministre de la Justice sur le 'screening des mosquées, des associations de mosquées et des organisations islamistes' (*Q.R.*, Chambre, 2015-2016, 1er août 2016, nº 84, p. 143, Q. nº 1203)

Question de D. Ducarme au ministre de la Justice sur le 'retrait d'habilitations à la Sûreté de l'État' (*Q.R.*, Chambre, 2015-2016, 1er août 2016, nº 84, p. 153, Q. nº 1275)

Question de V. Scourneau au ministre des Finances sur les 'coûts de sécurité – niveau 4 de la menace' (*Q.R.*, Chambre, 2015-2016, 1er août 2016, nº 84, p. 191, Q. nº 703)

Question de D. Ducarme au ministre de la Défense sur le 'retrait des habilitations ANS – Service Général du Renseignement et de la Sécurité' (*Q.R.*, Chambre, 2015-2016, 1er août 2016, nº 84, p. 266, Q. nº 768)

Question de F. Schepmans au ministre de l'Intérieur sur 'le cryptage des messages de l'application « WhatsApp »' (*Q.R.*, Chambre, 2015-2016, 16 août 2016, nº 85, p. 245, Q. nº 1330)

Question de D. Van der Maelen au ministre de l'Intérieur sur 'la compétence des services de renseignement britanniques sur le territoire belge' (*Q.R.*, Chambre, 2015-2016, 16 août 2016, nº 85, p. 250, Q. nº 1386)

Question de B. Pas au ministre des Affaires étrangères sur 'les mesures prises pour lutter contre le terrorisme – les procédures d'obtention des certificats de sécurité' (*Q.R.*, Chambre, 2015-2016, 16 août 2016, nº 85, p. 326, Q. nº 678)

Question de P. Pivin au ministre des Affaires étrangères sur le 'screening dans les entreprises publiques – ANS' (*Q.R.*, Chambre, 2015-2016, 16 août 2016, nº 85, p. 327, Q. nº 633)

Question de D. Ducarme au ministre des Affaires étrangères sur le 'retrait de passeports' (*Q.R.*, Chambre, 2015-2016, 16 août 2016, nº 85, p. 351, Q. nº 663)

Question de D. Ducarme au ministre des Affaires étrangères sur le 'retrait d'habilitations au SPF Affaires étrangères' (*Q.R.*, Chambre, 2015-2016, 16 août 2016, nº 85, p. 352, Q. nº 670)

Question de D. Ducarme au ministre de l'Intérieur sur le 'discours contre l'extrême droite' (*Q.R.*, Chambre, 2015-2016, 26 août 2016, nº 86, p. 153, Q. nº 1331)

Question de J.-M. Nollet au ministre de l'Intérieur sur les 'centrales nucléaires – sous-traitance dans le secteur IT' (*Q.R.*, Chambre, 2015-2016, 26 août 2016, nº 86, p. 162, Q. nº 1377)

Question de F. Dewinter au ministre de l'Intérieur sur 'les services de renseignement – traitement des données' (*Q.R.*, Chambre, 2015-2016, 26 août 2016, nº 86, p. 165, Q. nº 1382)

Question de F. Dewinter au ministre de l'Intérieur sur 'le screening des mosquées, des associations de mosquées et des organisations islamistes' (*Q.R.*, Chambre, 2015-2016, 26 août 2016, nº 86, p. 167, Q. nº 1391)

Question de F. Dewinter au ministre de l'Intérieur sur 'les moyens de fonctionnement des services de sécurité' (*Q.R.*, Chambre, 2015-2016, 26 août 2016, nº 86, p. 180, Q. nº 1413)

Question d'O. Chastel au ministre de l'Intérieur sur le 'Benelux – collaboration contre le terrorisme' (*Q.R.*, Chambre, 2015-2016, 26 août 2016, nº 86, p. 206, Q. nº 1460)

Question de D. Ducarme au ministre de l'Intérieur sur le 'retrait des cartes d'identité' (*Q.R.*, Chambre, 2015-2016, 26 août 2016, nº 86, p. 208, Q. nº 1473)

Question de K. Jadin au ministre de l'Intérieur sur 'l'accès aux données des messageries cryptées' (*Q.R.*, Chambre, 2015-2016, 26 août 2016, nº 86, p. 218, Q. nº 1493)

Question de D. Ducarme au ministre de l'Intérieur sur la 'radicalisation à la Grande Mosquée du Cinquantenaires' (*Q.R.*, Chambre, 2015-2016, 26 août 2016, nº 86, p. 225, Q. nº 1507)

Question de K. Gabriëls au ministre de l'Intérieur sur 'la cybersécurité de nos centrales nucléaires' (*Q.R.*, Chambre, 2015-2016, 5 septembre 2016, nº 87, p. 56, Q. nº 1287)

Question de Ph. Pivin au ministre de l'Intérieur sur les 'enquêtes policières – protocoles de collaboration en matière de techniques et de technologies' (*Q.R.*, Chambre, 2015-2016, 5 septembre 2016, nº 87, p. 60, Q. nº 1310)

Question de F. Dewinter au ministre de l'Intérieur sur 'Internet – islam radical' (*Q.R.*, Chambre, 2015-2016, 5 septembre 2016, nº 87, p. 78, Q. nº 1396)

Question de P. Buysrogge au ministre de l'Intérieur sur la 'VSSE – investissements dans l'infrastructure' (*Q.R.*, Chambre, 2015-2016, 5 septembre 2016, nº 87, p. 97, Q. nº 1438)

Question de N. Ben Hamou au ministre de l'Intérieur sur la 'lutte contre le terrorisme – collecte des données des passagers' (*Q.R.*, Chambre, 2015-2016, 5 septembre 2016, nº 87, p. 118, Q. nº 1520)

Question de V. Scourneau au ministre des Affaires étrangères sur les 'coûts de sécurité – niveau 4 de la menace' (*Q.R.*, Chambre, 2015-2016, 12 septembre 2016, nº 88, p. 172, Q. nº 428)

Question de R. Deseyn au ministre des Affaires étrangères sur 'le recrutement d'espions russes' (*Q.R.*, Chambre, 2015-2016, 12 septembre 2016, nº 88, p. 198, Q. nº 647)

Question de J.-M. Nollet au ministre des Affaires étrangères sur les 'retraits d'accréditation dans les centrales nucléaires belges' (*Q.R.*, Chambre, 2015-2016, 12 septembre 2016, nº 88, p. 202, Q. nº 652)

Question de S. Lahaye-Battheu au ministre des Affaires étrangères sur 'le rôle joué par les ambassades dans la promotion de la Belgique à l'étranger' (*Q.R.*, Chambre, 2015-2016, 12 septembre 2016, nº 88, p. 204, Q. nº 655)

Question de C. Fonck au ministre des Affaires étrangères sur les 'voyages dans les pays touchés par le zika' (*Q.R.*, Chambre, 2015-2016, 12 septembre 2016, nº 88, p. 244, Q. nº 748)

Question de K. Metsu au ministre de la Justice sur les 'services de renseignement – surveillance' (*Q.R.*, Chambre, 2015-2016, 12 septembre 2016, nº 88, p. 251, Q. nº 554)

Question de B. Pas au ministre de la Justice sur 'les mesures prises pour lutter contre le terrorisme – le soutien apporté aux enquêteurs' (*Q.R.*, Chambre, 2015-2016, 12 septembre 2016, nº 88, p. 284, Q. nº 1180)

Question de Ph. Pivin au ministre de la Justice sur la 'collaboration entre les services belges de renseignement et Europol' (*Q.R.*, Chambre, 2015-2016, 12 septembre 2016, nº 88, p. 313, Q. nº 1301)

Question de B. Hellings au ministre de la Justice sur 'la mise en œuvre de la loi du 29 janvier 2016 concernant le contrôle des activités des services de renseignement étrangers en Belgique au regard des événements récents politiques en Turquie (*C.R.I.*, Chambre, 2015-2016, 21 septembre 2016, COM 492, p. 25, Q. nº 13599)

Question de F. Dewinter au ministre de l'Intérieur sur 'l'infiltration de terroristes mêlés au flux des demandeurs d'asile' (*Q.R.*, Chambre, 2015-2016, 23 septembre 2016, nº 89, p. 73, Q. nº 1392)

Question de F. Dewinter au ministre de l'Intérieur sur 'Ibrahim El Bakraoui' (*Q.R.*, Chambre, 2015-2016, 23 septembre 2016, nº 89, p. 77, Q. nº 1385)

Question de F. Dewinter au ministre de l'Intérieur sur 'la présence de combattants djihadistes belges à l'étranger' (*Q.R.*, Chambre, 2015-2016, 23 septembre 2016, nº 89, p. 80, Q. nº 1388)

Question de F. Dewinter au ministre de l'Intérieur sur le 'personnel des services de sécurité – Arabe' (*Q.R.*, Chambre, 2015-2016, 23 septembre 2016, nº 89, p. 84, Q. nº 1414)

Question d'E. Lachaert au ministre des Affaires étrangères sur 'l'octroi d'attestations de sécurité pour des membres du personnel par l'Autorité Nationale de Sécurité' (*Q.R.*, Chambre, 2015-2016, 23 septembre 2016, nº 89, p. 174, Q. nº 741)

Question de J.-M. Nollet au ministre de la Justice sur la 'collaboration avec des sociétés privées dans le cadre d'enquêtes' (*Q.R.*, Chambre, 2015-2016, 23 septembre 2016, nº 89, p. 199, Q. nº 1278)

Question de F. Dewinter au ministre de la Justice sur 'l'enregistrement des jeunes partis combattre en Syrie' (*Q.R.*, Chambre, 2015-2016, 23 septembre 2016, nº 89, p. 200, Q. nº 1202)

Question de D. Geerts au ministre de la Mobilité sur 'les aéroports belges – délivrance et retrait des badges de sécurité' (*Q.R.*, Chambre, 2015-2016, 23 septembre 2016, nº 89, p. 363, Q. nº 1517)

Question de F. Dewinter au secrétaire d'État à l'Asile et la Migration sur 'les migrants originaires des pays membres de l'OCI – screening' (*Q.R.*, Chambre, 2015-2016, 23 septembre 2016, nº 89, p. 457, Q. nº 702)

Question de B. Vermeulen au ministre de l'Intérieur sur 'l'utilisation d'internet par les groupuscules et activistes d'extrême gauche' (*C.R.I.*, Chambre, 2015-2016, 21 septembre 2016, COM 493, p. 9, Q. nº 13200)

Questions jointes de K. Calvo et S. Lahaye-Battheu au ministre de la Justice sur 'les informations concernant State Grid' (*C.R.I.*, Chambre, 2015-2016, 28 septembre 2016, COM 497, p. 40, Q. nos 13912 à 13927)

Questions jointes de L. Onkelinx, F. Dewinter, H. Bonte, G. Vanden Burre et K. Degroote au ministre de l'Intérieur sur 'l'agression de policiers à Schaerbeek' (*C.R.I.*, Chambre, 2015-2016, 6 octobre 2016, PLEN 128, p. 19, Q. nos 1484 à 1489)

Question d'O. Chastel au ministre de l'Intérieur sur la 'mission en Turquie' (*Q.R.*, Chambre, 2016-2017, 7 octobre 2016, no 90, p. 60, Q. no 1149)

Question de B. Pas au ministre de l'Intérieur sur les 'mesures prises à la suite des attentats terroristes – engagements supplémentaires au sein des services de sécurité' (*Q.R.*, Chambre, 2016-2017, 7 octobre 2016, no 90, p. 73, Q. no 1364)

Question de B. Pas au ministre de l'Intérieur sur 'les mesures prises pour lutter contre le terrorisme – la prévention du départ de jeunes combattants' (*Q.R.*, Chambre, 2016-2017, 7 octobre 2016, no 90, p. 76, Q. no 1366)

Question de F. Dewinter au ministre de l'Intérieur sur 'le suivi des combattants de retour de Syrie' (*Q.R.*, Chambre, 2016-2017, 7 octobre 2016, no 90, p. 78, Q. no 1383)

Question de F. Dewinter au ministre de l'Intérieur sur 'l'enregistrement des jeunes partis combattre en Syrie' (*Q.R.*, Chambre, 2016-2017, 7 octobre 2016, no 90, p. 82, Q. no 1390)

Question de K. Jadin au ministre de de la Coopération au développement sur 'l'utilisation illégale des brouilleurs de GSM par le SEDEES' (*Q.R.*, Chambre, 2016-2017, 7 octobre 2016, no 90, p. 127, Q. no 637)

Question de W. De Vriendt au ministre de la Défense sur 'l'opération EUTM–RCA en République centrafricaine' (*Q.R.*, Chambre, 2016-2017, 7 octobre 2016, no 90, p. 480, Q. no 799)

Question de D. Ducarme au ministre de la Défense sur la 'concrétisation du protocole créant la Belgian Intelligence Academy' (*Q.R.*, Chambre, 2016-2017, 7 octobre 2016, no 90, p. 518, Q. no 833)

Question de S. Schepmans au ministre de la Défense sur 'l'Open Source and Social Media Collect and Analyse Tool' (*Q.R.*, Chambre, 2016-2017, 7 octobre 2016, no 90, p. 525, Q. no 847)

Question de Ph. Pivin au ministre de la Justice sur 'le recrutement de mineurs par Daech' (*C.R.I.*, Chambre, 2016-2017, 13 octobre 2016, PLEN 130, p. 57, Q. no 1515)

Question de L. Van Biesen au ministre de la Justice sur les 'administrations – entreprises publiques – engagement de personnes atteintes d'un handicap professionnel.' (*Q.R.*, Chambre, 2016-2017, 14 octobre 2016, no 91, p. 292, Q. no 48)

Question de K. Jadin au ministre des Affaires étrangères sur 'les attentats du 1er juillet 2016 à Dacca, Bangladesh' (*C.R.I.*, Chambre, 2016-2017, 19 octobre 2016, COM 513, p. 8, Q. no 12971)

Question d'O. Maingain au ministre de l'Intérieur sur 'les menaces à l'encontre d'écoles considérées comme liées à la mouvance güleniste' (*C.R.I.*, Chambre, 2016-2017, 19 octobre 2016, COM 514, p. 1, Q. no 13574)

Questions jointes de F. Dewinter et A. Carcaci au ministre de l'Intérieur sur 'le retour de djihadistes' (*C.R.I.*, Chambre, 2016-2017, 20 octobre 2016, PLEN 136, p. 16, Q. nos 1531 et 1532)

Question de B. Pas au ministre de l'Intérieur sur 'la menace que représentent les armes chimiques et biologiques' (*Q.R.*, Chambre, 2016-2017, 21 octobre 2016, no 92, p. 72, Q. no 1181)

Question de J.-M. Nollet au ministre de l'Intérieur sur 'la consultation du registre national' (*Q.R.*, Chambre, 2016-2017, 21 octobre 2016, nº 92, p. 91, Q. nº 1579)

Question de B. Pas au ministre de l'Intérieur sur 'la création d'une banque de données dans le cadre de la lutte contre la radicalisation' (*Q.R.*, Chambre, 2016-2017, 21 octobre 2016, nº 92, p. 101, Q. nº 1598)

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, 21 octobre 2016, nº 92, p. 129, Q. nº 1629)

Question de K. Jadin au ministre de la Défense sur 'le logiciel « Open Source and Social Media Collect and Analyse Tool »' (*Q.R.*, Chambre, 2016-2017, 21 octobre 2016, nº 92, p. 317, Q. nº 872)

Question de D. Ducarme au secrétaire d'État à l'Asile et la Migration sur 'les passeports syriens' (*Q.R.*, Chambre, 2016-2017, 21 octobre 2016, nº 92, p. 344, Q. nº 636)

Question de S. Smeyers au secrétaire d'État à l'Asile et la Migration sur 'le screening sur le radicalisme des demandeurs d'asile' (*C.R.I.*, Chambre, 2016-2017, 26 octobre 2016, COM 518, p. 16, Q. nº 14630)

Questions jointes de B. Pas et A. Frédéric au secrétaire d'État à l'Asile et la Migration sur 'l'expulsion des prédicateurs radicaux' (*C.R.I.*, Chambre, 2016-2017, 26 octobre 2016, COM 518, p. 13, Q. nºs 14150 et 14554)

Question de S. Van Hecke au secrétaire d'État à la Lutte contre la fraude sociale sur 'l'avis rendu par la Commission de la protection de la vie privée à propos de la possibilité de surveillance des câbles en fibre optique' (*C.R.I.*, Chambre, 2016-2017, 26 octobre 2016, COM 519, p. 1, Q. nº 11741)

Question de Z. Demir au ministre de l'Emploi sur les 'combattants partis en Syrie – allocations de chômage' (*Q.R.*, Chambre, 2016-2017, 28 octobre 2016, nº 93, p. 144, Q. nº 995)

Question de Ph. Pivin au ministre des Finances sur la 'collaboration entre le SPF Finances Douane et Europol' (*Q.R.*, Chambre, 2016-2017, 28 octobre 2016, nº 93, p. 278, Q. nº 1252)

Question de G. Dallemagne au ministre de la Défense sur 'l'impact de l'opération Vigilant Guardian sur la Défense et la possible création d'un corps de sécurité pour les bâtiments' (*Q.R.*, Chambre, 2016-2017, 28 octobre 2016, nº 93, p. 330, Q. nº 864)

Question de N. Lijnen au ministre de la Défense sur le 'travail à domicile' (*Q.R.*, Chambre, 2016-2017, 28 octobre 2016, nº 93, p. 335, Q. nº 867)

Question de B. Hellings au ministre des Affaires étrangères sur 'les actions et les positions de la Belgique à l'égard de l'enquête en cours au sujet de la mort suspecte en 1961 du secrétaire général de l'ONU Dag Hammarskjöld' (*C.R.I.*, Chambre, 2016-2017, 8 novembre 2016, COM 523, p. 50, Q. nº 14329)

Question de B. Hellings au ministre des Affaires étrangères sur 'le sort des archives dites 'africaines'' (*C.R.I.*, Chambre, 2016-2017, 8 novembre 2016, COM 523, p. 52, Q. nº 14555)

Question de K. Jadin au ministre des Affaires étrangères sur 'la surveillance des sectes' (*C.R.I.*, Chambre, 2016-2017, 9 novembre 2016, COM 529, p. 14, Q. nº 14723)

Question de V. Yüksel au ministre de l'Intérieur sur 'le suivi des combattants partis en Syrie' (*C.R.I.*, Chambre, 2016-2017, 9 novembre 2016, COM 533, p. 15, Q. nº 14371)

Questions jointes de G. Dallemagne et H. Bonte au ministre de l'Intérieur sur 'les moyens dévolus à la sécurité et à la lutte contre le terrorisme' (*C.R.I.*, Chambre, 2016-2017, 10 novembre 2016, PLEN 138, p. 17, Q. nºs 1574 et 1597)

Question de V. Yüksel au ministre de la Justice sur 'le gel des avoirs du terroriste Oussama Atar' (*C.R.I.*, Chambre, 2016-2017, 10 novembre 2016, PLEN 138, p. 20, Q. nº 1575)

Question de D. Ducarme au ministre de l'Intérieur sur la 'protection des lieux de culte' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 94, p. 100, Q. nº 1640)

Question de K. Jadin au ministre de l'Intérieur sur les 'Foreign terrorist fighters' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 94, p. 108, Q. nº 1690)

Question de D. Ducarme au ministre de l'Intérieur sur le '« Screening » de personnes travaillant dans le secteur nucléaire' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 94, p. 110, Q. nº 1693)

Question de D. Ducarme au ministre de la Justice sur 'l'action contre les données cryptées des smartphones dans le cadre de la lutte contre le terrorisme' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 94, p. 121, Q. nº 868)

Question de F. Dewinter au ministre de la Justice sur 'l'islam radical' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 94, p. 124, Q. nº 1195)

Question de D. Ducarme au ministre de la Défense sur l'utilisation des UAV en Mer du Nord' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 94, p. 241, Q. nº 876)

Question de R. Deseyn au vice-Premier ministre de la Coopération au développement sur 'le service d'inspection de l'infrastructure critique' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 95, p. 94, Q. nº 698)

Question de S. Crusnière au ministre des Affaires étrangères sur 'le retrait des passeports et titres de séjours' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 95, p. 101, Q. nº 624)

Question de F. Dewinter au ministre de la Justice sur 'les attentats terroristes de Daech en Europe' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 95, p. 120, Q. nº 1197)

Question de J.-J. Flahaux au ministre de la Justice sur 'les attaques par rançongiciels' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 95, p. 149, Q. nº 1467)

Question de B. Pas au ministre de la Justice sur 'l'utilisation de nouvelles technologies dans la lutte contre le terrorisme' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 95, p. 157, Q. nº 1482)

Question de B. Pas au ministre de la Justice sur 'les recrutements supplémentaires pour les services de sécurité' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 95, p. 158, Q. nº 1483)

Question de B. Pas au ministre de la Justice sur 'le screening des prédicateurs de haine' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 95, p. 160, Q. nº 1485)

Question de R. Deseyn au ministre des Finances sur 'le service d'inspection de l'infrastructure critique' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 95, p. 278, Q. nº 1226)

Question de R. Deseyn à la ministre de l'Énergie sur 'le service d'inspection de l'infrastructure critique' (*Q.R.*, Chambre, 2016-2017, 16 novembre 2016, nº 95, p. 290, Q. nº 356)

Question de F. Dewinter au ministre de la Justice sur 'les moyens de fonctionnement des services de sécurité' (*Q.R.*, Chambre, 2016-2017, 23 novembre 2016, nº 96, p. 146, Q. nº 1210)

Question de G. Dallemagne au ministre de la Défense sur 'l'agression de trois policiers à Schaerbeek par un ancien militaire' (*Q.R.*, Chambre, 2016-2017, 23 novembre 2016, nº 96, p. 278, Q. nº 925)

Question de B. Pas au ministre de la Justice sur 'le protocole entre l'administration flamande de l'enseignement et la Sûreté de l'État' (*Q.R.*, Chambre, 2016-2017, 23 novembre 2016, nº 97, p. 289, Q. nº 998)

Question de B. Pas au ministre de la Justice sur les 'mesures prises à la suite des attentats terroristes et les nouvelles technologies' (*Q.R.*, Chambre, 2016-2017, 23 novembre 2016, nº 97, p. 300, Q. nº 1184)

Questions jointes de G. Gilkinet au ministre de la Justice sur 'la date de prescription potentielle dans le dossier Chodiev' (*C.R.I.*, Chambre, 2016-2017, 30 novembre 2016, COM 545, p. 7, Q. nº 15247 à 1552)

Question de B. Pas au ministre de l'Intérieur sur 'les avantages sociaux des combattants partis en Syrie' (*Q.R.*, Chambre, 2016-2017, 7 décembre 2016, nº 98, p. 205, Q. nº 1738)

Question de J.-M. Nollet au ministre de l'Intérieur sur 'l'intervention de la Sûreté de l'État dans les entreprises' (*Q.R.*, Chambre, 2016-2017, 7 décembre 2016, nº 98, p. 211, Q. nº 1798)

Question de R. Deseyn au ministre de la Coopération au développement sur 'les cartes SIM anonymes' (*Q.R.*, Chambre, 2016-2017, 7 décembre 2016, nº 98, p. 212, Q. nº 697)

Question de D. Ducarme au ministre de la Justice sur le 'suivi de l'incendie volontaire contre l'INCC' (*Q.R.*, Chambre, 2016-2017, 7 décembre 2016, nº 98, p. 251, Q. nº 1383)

Question de S. Pirlot au ministre de la Défense sur 'le projet de loi modifiant la loi organique des services de renseignement et de sécurité du 30 novembre 1998 et particulièrement son article 21/1' (*C.R.I.*, Chambre, 2016-2017, 14 décembre 2016, COM 550, p. 25, Q. nº 15451)

Question de B. Hellings au ministre de la Défense sur 'la participation de la Défense à la probable future enquête de la Cour pénale internationale sur les crimes commis en Afghanistan depuis 2003' (*C.R.I.*, Chambre, 2016-2017, 14 décembre 2016, COM 550, p. 31, Q. nº 14988)

Question de K. Van Vaerenbergh au ministre de la Justice sur 'la radicalisation dans les prisons' (*C.R.I.*, Chambre, 2016-2017, 14 décembre 2016, COM 552, p. 21, Q. nº 15460)

Question de L. Onkelinx au Premier ministre sur 'l'alerte de voyage du département d'État américain concernant l'Europe' (*C.R.I.*, Chambre, 2016-2017, 14 décembre 2016, COM 555, p. 12, Q. nº 15160)

Question de F. Dewinter au ministre de l'Intérieur sur 'la fermeture éventuelle de la Grande Mosquée au parc du Cinquantenaire' (*Q.R.*, Chambre, 2016-2017, 14 décembre 2016, nº 099, p. 81, Q. nº 1470)

Question de G. Calomne au ministre de l'Intérieur sur 'la sécurisation des sites d'approvisionnement en eau potable' (*Q.R.*, Chambre, 2016-2017, 14 décembre 2016, nº 099, p. 82, Q. nº 1498)

Question de S. de Coster-Bauchau au ministre de la Justice sur 'le manque d'aumôniers musulmans au sein des prisons d'Ittre, Forest et Nivelles' (*Q.R.*, Chambre, 2016-2017, 14 décembre 2016, nº 099, p. 134, Q. nº 1509)

Questions jointes de F. Dewinter et P. De Roover au ministre de la Justice sur 'l'espionnage par les mosquées liées à la Diyanet' (*C.R.I.*, Chambre, 2016-2017, 15 décembre 2016, PLEN 144, p. 24, Q. nºs 1704 et 1705)

Question de K. Metsu au ministre de la Justice sur le 'radicalisme dans les prisons' (*Q.R.*, Chambre, 2016-2017, 23 décembre 2016, nº 100, p. 279, Q. nº 1535)

ANNEXE D.
AVIS SUR LE PROJET DE LOI RÉGLEMENTANT LA SÉCURITÉ PRIVÉE

Dans un courrier daté du 28 septembre 2016, le ministre de la Sécurité et de l'Intérieur a demandé au président du Comité permanent R, qui préside également l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité, de formuler un avis sur les dispositions du Projet de loi réglementant la sécurité privée qui concernent l'Organe de recours.

Étant donné que le projet de loi sera discuté dans quelques semaines en première lecture au Conseil des ministres, le Comité a rendu cet avis des délais particulièrement courts. De ce fait, il n'a pas été en mesure d'examiner chaque aspect en détail.[288]

Les lignes directrices de l'avis et de la proposition de modifications de la Loi du 11 décembre 1998 ci-annexée ont été examinées avec les membres (suppléants) du Comité permanent P et la Commission Vie privée qui siègent dans l'Organe de recours. Ceux-ci ont marqué leur accord.

Un surcroît de travail compensé par un gain d'efficacité

L'Organe de recours tient en premier lieu à souligner qu'il n'a pas de réticence à l'égard du projet visant à transférer une partie du contentieux administratif en matière de sécurité privée à l'Organe de recours.

Ce transfert est, il est vrai, synonyme de surcroît de travail considérable pour l'Organe de recours, qui ne dispose pas d'un budget ni des effectifs spécifiques. Les frais liés au fonctionnement de l'Organe de recours sont, en effet, à charge du budget du Comité permanent R, qui assure la fonction de greffe de l'Organe de recours. Un surcroît de travail signifie bien entendu aussi du travail supplémentaire pour les trois membres de l'Organe de recours ou leurs suppléants respectifs.

La charge de travail de l'Organe de recours s'est accrue de manière systématique ces dernières années, surtout en raison de la complexité toujours plus grande des dossiers à traiter au niveau de la gestion administrative, du traitement des auditions et de la rédaction des décisions. Ainsi, les dossiers administratifs qui sont transmis par les autorités de sécurité ne sont pas toujours complets, si bien que le greffe se voit contraint de poser de nouveaux actes pour les compléter. Il en va de même pour l'application de l'article 5 § 3 de la Loi relative à l'Organe de recours : la demande de ne pas donner accès à certaines pièces au requérant est rarement motivée ou n'émane pas de la bonne instance, si bien que le greffe doit recueillir des informations complémentaires. En outre, il convient de constater que les auditions prennent beaucoup plus de temps qu'il y a quelques années. Plusieurs raisons sont à l'origine de cette évolution. Les requérants sont toujours plus nombreux à se faire assister par un avocat qui, lors de l'audition, expose le point de vue de son client. De plus, les services de police et de renseignement concernés demandent de plus en plus souvent à être entendus.

288 Cet avis, établi en néerlandais, a été traduit en perspective du présent rapport d'activités.

Eu égard à la complexité de certaines affaires, davantage de temps y est consacré. Enfin, contrairement à ce qui se faisait dans le passé, nombre d'affaires sont reprises lors d'une seconde ou troisième audition, soit parce qu'un requérant demande un report, soit parce que des informations doivent encore venir compléter le dossier. Le processus de décision requiert lui aussi plus de temps qu'il y a quelques années. Deux raisons importantes l'expliquent : d'une part, davantage de questions de procédure sont soulevées (par exemple, le débat sur la recevabilité, la question linguistique, les droits de la défense, l'obligation de motivation…) et d'autre part, l'Organe de recours est plus souvent confronté à des dossiers extrêmement sensibles qui sont liés à la problématique du radicalisme et de la menace terroriste actuelle. De tels dossiers exigent bien entendu un traitement extrêmement consciencieux et une motivation adéquate. Par ailleurs, ces dossiers nécessitent des mesures de sécurité spécifiques.

Tant le Comité permanent R que l'Organe de recours veulent attirer l'attention sur la charge de travail qui augmentera encore dans un futur proche. D'une part, il faut s'attendre à ce que le contentieux de personnes actives dans la recherche privée soit transféré d'ici peu à l'Organe de recours. Sinon, une distinction difficilement justifiable semble être établie entre deux secteurs analogues qui sont toujours soumis à la même réglementation. D'autre part, le Gouvernement a déjà annoncé à plusieurs reprises que le nombre de screenings de sécurité augmentera (par exemple pour des personnes actives dans des infrastructures critiques). Étant donné qu'il est question ici de dix mille screenings supplémentaires, cela se traduira par un nombre croissant de recours.

L'Organe de recours estime qu'il est possible de remédier partiellement à la charge de travail supplémentaire en adaptant le dispositif existant, ce qui permettrait de réaliser un certain gain d'efficacité. L'Organe de recours pense surtout à l'introduction d'un acte d'appel simple et clair et à des délais de réponse obligatoires pour les parties. En effet, il se trouve que le greffe de l'Organe de recours doit actuellement investir beaucoup de temps et de moyens pour obtenir les pièces requises (rappels, courriels, entretiens téléphoniques…). L'introduction d'un droit de mise au rôle restreint – à l'instar par exemple du Conseil d'État – peut également éviter toute une série de recours inutiles. Par ailleurs, deux procédures strictement écrites sont envisagées : lorsque la requête est manifestement fondée ou lorsqu'elle est manifestement irrecevable, il est proposé de pouvoir se prononcer sur la base d'une procédure écrite, ce qui évite d'organiser des audiences inutiles.

Mais le plus grand gain d'efficacité consisterait indéniablement à introduire une obligation de procéder à une audition par l'autorité concernée lorsqu'elle souhaite formuler une évaluation de sécurité négative. L'Organe de recours est, en effet, trop souvent confronté à des dossiers qui auraient pu être clarifiés par l'administration concernée sur base d'un simple entretien, associé à un accès (limité) au dossier administratif. Dans la plupart des cas, l'intéressé n'a eu au préalable aucune possibilité de consulter le dossier : ce point est discutable sur le strict plan des principes, certainement lorsqu'il s'agit d'un retrait d'une autorisation accordée précédemment. Il convient de souligner à cet égard, que les décisions de la plupart des autorités de sécurité sont motivées de manière si sommaire que l'intéressé comprend à peine pourquoi il ou elle fait l'objet d'une décision négative. Cette pratique devrait changer.

Pour réaliser ce gain d'efficacité, il faut non seulement modifier le Projet de loi réglementant la sécurité privée, mais aussi la Loi Classification du 11 décembre 1998 et la Loi du 11 décembre 1998 portant création de l'Organe de recours et – par la suite – les arrêtés d'exécution. Une proposition de projet de modification de la Loi du 11 décembre 1998 portant création de l'Organe de recours figure en annexe de cet avis. Il existe d'ailleurs aussi une raison technico-juridique expliquant pourquoi cette loi doit être modifiée par le biais d'un projet distinct et non par le biais de plusieurs dispositions dans le Projet de loi réglementant la sécurité privée.

Modification nécessaire de la Loi du 11 décembre 1998 portant création de l'Organe de recours

Le Projet de loi réglementant la sécurité privée, qui selon l'article 1er règle une matière telle que prévue à l'article 74 de la Constitution, modifie *de facto*, dans ses articles 75 à 80, les règles qui portent sur l'Organe de recours, ne serait-ce qu'en accordant une nouvelle compétence à cette juridiction administrative. Cependant, « *les lois sur le Conseil d'État et sur les tribunaux administratifs fédéraux* » sont soumises à l'article 78 de la Constitution, en vertu duquel le projet de loi adopté par la Chambre doit être envoyé au Sénat. Le présent projet doit dès lors être scindé, et les dispositions portant sur le recours contre la décision du ministre doivent être insérées dans la Loi du 11 décembre 1998.

Les modifications proposées par l'Organe de recours à cette dernière loi n'apporteront pas seulement un gain d'efficacité, mais aussi davantage de clarté et d'uniformité. Ainsi, les délais seront harmonisés pour tous les recours. Quelques lacunes existantes disparaîtront également.

Par ailleurs, le droit de contradiction est renforcé, et ce notamment en modifiant les règles relatives à l'audition des membres des autorités concernées (sinon, les fonctionnaires du SPF Intérieur ne pourraient pas être auditionnés par l'Organe de recours), en s'appuyant sur les règles relatives à la transmission de pièces et en explicitant les exceptions au droit de consultation.

Cette dernière modification signifie aussi une amélioration sur le plan des droits de la défense. En effet, l'Organe de recours a constaté que les motifs d'exception prévus sont de plus en plus souvent invoqués, sans être véritablement motivés. Le projet y remédie. En outre, l'autorité concernée est obligée d'indiquer en termes généraux quelle est la nature des informations protégées. L'Organe de recours veillera naturellement à ce que l'autorité n'en arrive pas à utiliser des formules standard dénuées de sens. C'est l'Organe de recours qui décide *in fine* quelles données peuvent être consultées et quelles données ne le peuvent pas. En ce qui concerne le droit de la défense, il est parfois également possible pour le requérant de se faire représenter par un avocat. Actuellement, il ne peut que se faire assister par un avocat.

Plusieurs considérations concernant la proposition de disposition relative à l' « enquête sur les conditions de sécurité »

Les articles 66 et s. du Projet de loi réglementant la sécurité privée régissent la procédure pour ce que l'on appelle l'enquête sur les conditions de sécurité.

L'Organe de recours constate que dans des domaines (toujours plus) nombreux de la vie sociale, des screenings de sécurité sont requis. Leur finalité est en grande partie similaire, mais la procédure diffère énormément sur de nombreux plans: il y a des enquêtes de sécurité, des vérifications de sécurité, des screenings de candidats agents de police, une enquête sur des personnes souhaitant devenir belges, des screenings d'étrangers… Il est à noter que des règles différentes sont prévues quant au type d'informations qui peuvent être recueillies, par quelles autorités, via quelles méthodes, dans quels délais, après audition ou non…

L'enquête sur les conditions de sécurité a également toute sa place dans cette liste. Fort de son expérience dans de nombreux autres screenings de sécurité, l'Organe de recours formule les considérations suivantes concernant le dispositif proposé:

- L'article 67 du projet prévoit que sur base de données policières et judiciaires dures, la décision sera prise d'ouvrir ou non une enquête, en d'autres termes, de recueillir ou non des données auprès des services de renseignement. Ce qui signifie qu'il est possible qu'aucune enquête ne soit menée (et que l'intéressé reçoive donc son autorisation), alors que les services de renseignement disposent peut-être d'informations pertinentes (par exemple des contacts dans des milieux extrémistes qui ne figurent pas dans les banques de données policières). L'Organe de recours estime qu'il y a lieu – comme pour les vérifications de sécurité – d'interroger immédiatement tous les services pertinents afin que le fonctionnaire concerné puisse réaliser une évaluation sur base d'un dossier complet.
- En outre, l'Organe de recours considère qu'il faut vérifier dans quelle mesure il est possible d'harmoniser les screenings pour les candidats agents de police ou des vérifications de sécurité, certainement en ce qui concerne la nature des données qui peuvent être recueillies.
- L'Organe de recours estime indiqué que les articles 68 et 71 soient précisés, étant donné qu'il n'est pas clair qui doit ou peut faire quoi et qui effectue l'évaluation finale. Ainsi, dans l'article 68, la Sûreté de l'État est certes mentionnée, mais on ne retrouve pas les éléments dont ce service dispose dans l'énumération de l'article 71.
- L'Organe de recours fait remarquer que le délai dans lequel les différents services et le ministre compétent doivent prendre une décision n'est pas précisé. L'Organe de recours attire l'attention sur le fait que dans les procédures qu'il traite actuellement, le silence de l'autorité peut donner lieu à un recours.
- Le refus (ou le retrait) d'une autorisation pour des entreprises de gardiennage et les services internes de gardiennage peut aussi se fonder sur des informations émanant des services de renseignement, plus précisément de la Sûreté de l'État (article 18 du projet). Cet avis de la Sûreté de l'État peut lui aussi contenir des informations sensibles voire classifiées. Étant donné que le projet ne définit rien en la matière, un éventuel recours sera encore traité par le Conseil d'État. L'Organe de recours se demande si tel est le but recherché. De plus, on peut se demander pourquoi l'avis du Service général du renseignement et de la sécurité n'est pas recueilli à ce propos.
- La réglementation proposée ne permet que de demander des informations existantes aux différents services, comme cela se fait actuellement pour les vérifications de sécurité préalables à l'octroi d'une attestation ou d'un avis de sécurité; tout travail complémentaire de renseignement n'est pas autorisé. Ces informations peuvent toutefois être dépassées ou vagues. Certainement dans les dossiers les plus sensibles,

l'Organe de recours s'aperçoit régulièrement de la nécessité de disposer d'informations plus précises et actuelles, et ce dans l'intérêt de l'intéressé *et* de la sécurité. Cependant, la possibilité de laisser certains services recueillir des informations complémentaires doit faire l'objet d'une réglementation légale claire. Pour l'instant, cela ne peut se faire que dans le cadre d'une enquête de sécurité préalable à l'octroi d'une habilitation de sécurité.

- Lors de la communication de la décision (article 74 du projet), il faut tenir compte des éléments découlant d'une information ou d'un instruction judiciaire en cours. Ces motifs d'exception ont été insérés récemment, à juste titre, dans la Loi Classification et dans la Loi Organe de recours.
- Le projet requiert un nouvel examen périodique (tous les trois ans) et permet manifestement une évaluation intermédiaire permanente (articles 89 et 90). L'Organe de recours est d'avis que ce système doit pouvoir être étendu à toutes les vérifications de sécurité.

Exposé des Motifs

Enfin, l'Organe de recours souhaite encore formuler quelques considérations sur plusieurs passages de l'Exposé des Motifs relatifs à l'enquête sur les conditions de sécurité et la nouvelle compétence pour l'Organe de recours :

- Le passage suivant figure dans le commentaire des articles 66-69 : « *Pour ces raisons, il avait été décidé en 1998, lorsque la loi relative aux habilitations de sécurité a vu le jour, de confier les enquêtes de sécurité relatives aux acteurs du secteur de la sécurité privée au SPF Intérieur, dans le cadre de la loi relative à la sécurité privée* ». La portée de ce passage n'est pas claire pour l'Organe de recours.
- Dans le commentaire des articles 74-75, les modifications sont présentées comme nécessaires puisque l'intéressé doit, tant au niveau de l'administration que pour le Conseil d'État, avoir un accès illimité à toutes les informations (et donc aussi aux informations sensibles). L'Organe de recours veut cependant attirer l'attention sur les possibilités légales existantes permettant de protéger certaines informations (par exemple la Loi relative à la publicité de l'administration et la Loi relative à la motivation des actes administratifs) et sur la jurisprudence du Conseil d'État qui accepte parfois de ne pas soumettre certaines informations (secret d'affaires, informations classifiées). En revanche, l'Organe de recours dispose naturellement d'une base légale claire et complète en la matière. L'Organe de recours fait toutefois remarquer que la même problématique de motivation et de consultation se présente dans le cadre de l'évaluation des candidats agents.
- Dans le commentaire des articles 74-75, il est établi à tort que l'Organe de recours dispose déjà d'une certaine expertise en matière de sécurité privée. L'expertise porte plutôt sur la sécurité en général.
- Dans les mêmes articles, la nécessaire rapidité des décisions dans le cadre des évaluations de sécurité est mise en avant. L'Organe de recours signale que cet effet peut être perdu si un requérant doit non seulement s'adresser à l'Organe de recours pour l'enquête sur les conditions de sécurité, mais aussi au Conseil d'État pour l'évaluation des autres critères.

ANNEXE E.
AVIS DU COMITÉ PERMANENT R SUR L'AVANT-PROJET DE LOI MODIFIANT LA LOI DU 30 NOVEMBRE 1998 ORGANIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ (L.R&S)

Dans un courrier daté du 22 février 2016, le ministre de la Justice a demandé au Comité permanent R de rendre un avis sur l'avant-projet de loi modifiant la Loi organique des services de renseignement et de sécurité du 30 novembre 1998, et ce pour le 4 mars 2016 au plus tard. Vu les délais de réponse extrêmement courts, d'une part, et vu l'étendue et la complexité des modifications proposées, d'autre part, le Comité n'a pas été en mesure d'examiner chaque aspect du projet en détail et encore moins d'effectuer un contrôle légistique ou d'élaborer des propositions alternatives. Le Comité a dès lors choisi de formuler plusieurs lignes directrices et, si nécessaire, de les étoffer avec des exemples concrets. Le Comité reste évidemment à la disposition des autorités compétentes pour toute information ou commentaire complémentaire au présent avis.

Toujours en raison des délais impartis, le Comité n'a établi cet avis qu'en néerlandais.[289]

Le Comité tient à souligner au préalable qu'il est en faveur de toute proposition permettant d'accroître l'efficacité des services de renseignement belges, dans la mesure où des garanties suffisantes sont prévues pour sauvegarder les libertés et les droits fondamentaux. Ceci est particulièrement vrai dans le contexte sociétal actuel, dans lequel la lutte contre le terrorisme et le radicalisme doit être menée de manière optimale. En outre, le Comité attire l'attention sur le fait que la réglementation proposée – qui doit permettre une intervention plus performante – ne s'applique pas seulement à la lutte contre le terrorisme et le radicalisme, mais aussi à tous les domaines dans lesquels la Sûreté de l'État (VSSE) et le Service Général du Renseignement et de la Sécurité (SGRS) sont actifs.

Dans l'Accord de gouvernement du 10 octobre 2014, il était annoncé que *« la loi relative aux méthodes particulières […] sera évaluée et le cas échéant adaptée »*. Dans l'Exposé des Motifs du projet de loi, il est fait référence à une *« première évaluation »*. Le Comité était au courant de l'existence d'un groupe de travail qui était chargé d'une telle évaluation, mais il n'a jamais eu connaissance des résultats de cette évaluation. Dans cette optique, il était difficile pour le Comité d'évaluer à quel niveau les compétences des services de renseignement et les possibilités qui leur sont offertes actuellement seraient insuffisantes ou ne permettraient pas aux services de remplir leur mission comme il se doit, ce qui justifierait donc une modification de la Loi MRD du 4 février 2010, voire de la Loi organique des services de renseignement et de sécurité du 30 novembre 1998. Outre les recommandations concrètes qu'il a lui-même formulées ces dernières années (voir, ci-après, les points 1 à 7), le Comité n'a pas ressenti, ni dans son rôle de 'contrôleur' ni dans son rôle d' 'instance de contrôle des MRD', que la réglementation actuelle *« empêche[rait] parfois un recours rapide et efficace aux méthodes »* (Exposé des Motifs), ce qui nécessiterait certaines modifications proposées dans le projet.

289 Cette traduction a été réalisée en perspective du présent rapport d'activités.

En ce qui concerne les propositions que le Comité a lui-même formulées les années précédentes dans le cadre du fonctionnement MRD, les exemples suivants peuvent être cités. Le projet tient compte en grande partie de ces recommandations.

1. L'identification de l'abonné ou de l'utilisateur d'un moyen de communication électronique ou du moyen de communication utilisé pourrait être considérée comme une méthode ordinaire, vu l'impact limité sur la vie privée. Cette recommandation a été récemment concrétisée 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).

2. La loi devrait établir un cadre clair, uniforme et opérationnel pour la mise en oeuvre des méthodes particulières de recueil de données dans des situations d'extrême urgence (Comité permanent R, *Rapport d'activités 2011*, 78). Le projet répond à cette recommandation. Le Comité constate néanmoins que la réglementation prévue en ce qui concerne les méthodes exceptionnelles laisse une grande marge d'appréciation aux services. Le Comité fait également remarquer qu'il avait expressément recommandé qu'une sanction claire soit prévue si l'extrême urgence ne pouvait pas être démontrée par la suite. Dès lors, le Comité réitère cette recommandation.

3. L'article 13/1 § 2, alinéa 3 L.R&S donne à (l'ensemble de) la Commission BIM la possibilité d'accorder aux agents de renseignement l'autorisation expresse de commettre des infractions qui sont absolument nécessaires pour assurer l'efficacité d'une MRD ou de garantir leur propre sécurité ou celle d'autres personnes. Cependant, la loi n'a pas prévu de procédure d'extrême urgence. Le Comité est d'avis que lorsque la méthode particulière elle-même peut être mise en œuvre en extrême urgence, il faut en même temps prévoir que la compétence accessoire visée à 13/1 § 2, alinéa 3 L.R&S puisse être exercée en extrême urgence. Le projet va dans ce sens, voire un peu plus loin, en autorisant la commission d'infractions sans approbation préalable (voir point 28 ci-après).

4. Le Comité a indiqué que l'obligation de notification a été annulée par l'arrêt de la Cour constitutionnelle du 22 september 2011, ce qui a nécessité une nouvelle réglementation légale (Comité permanent R, *Rapport d'activités 2011*, 52-53). Le projet n'aborde pas cette problématique.

5. L'article 18/17 § 7 L.R&S prévoit que les données recueillies via une mesure d'écoute doivent être détruites dans un délai d'un an et deux mois. Le Comité avait recommandé à l'époque de supprimer cette limitation, entre autres parce que les services de renseignement travaillent sur du long terme et qu'une obligation d'effacer des renseignements pertinents – parce qu'ils ont été recueillis via une méthode exceptionnelle – va à l'encontre de ce travail sur le long terme. La proposition répond à cette recommandation. Le Comité attire néanmoins l'attention sur l'interdiction de reprendre dans la documentation les données qui ne sont pas utiles en termes de finalité de renseignement. Indépendamment de la manière dont elles ont été

recueillies, de telles données doivent dans tous les cas être détruites le plus vite possible.

6. La réglementation actuelle ne permet pas la mise en oeuvre de méthodes exceptionnelles en cas d'extrémisme et d'ingérence. Le Comité a proposé de lever cette interdiction. Le projet suit cette recommandation.

7. En 2013, le Comité avait recommandé que le législateur mène un débat sur la nécessité de permettre la mise en oeuvre de MRD à l'étranger. Plusieurs propositions sont émises dans le projet à cet égard (voir les points 23 et 24 ci-après).

Le Comité constate que l'avant-projet envisage d'apporter des modifications importantes à la Loi organique des services de renseignement et de sécurité du 30 novembre 1998, modifications qui vont plus loin que les dispositions qui ont été insérées en 2010 par la Loi MRD. Le Comité se réfère seulement aux exemples suivants :

8. La mission légale du SGRS et ses possibilités de collecte à l'étranger sont considérablement étendues (voir les points 18, 24 et 31 ci-après).

9. Le projet créé la possibilité d'instaurer une 'équipe d'intervention' tant au sein de la VSSE que du SGRS. Son objectif et sa nécessité réels n'ont jamais été abordés ou démontrés au Comité. Les membres de cette équipe d'intervention se voient octroyer des tâches et des compétences de police administrative, juste au moment où la mission de protection, comme tâche de police administrative, est retirée à la VSSE à la demande de celle-ci.

10. Les méthodes ordinaires existantes sont adaptées dans le sens que les services peuvent recevoir plus facilement des informations – surtout – de particuliers (voir ci-après).

11. Une disposition relative à l'archivage de documents des services de renseignement est introduite. Dans ce cadre, le Comité avait défendu, à l'époque, l'idée d'un système de caducité de plein droit des classifications après un certain temps (par exemple, 30 ans pour les documents revêtus de la mention 'secret' et 50 ans pour les documents revêtus de la mention 'très secret'), à moins d'un renouvellement explicite de celles-ci.

Le Comité tient à attirer l'attention sur plusieurs autres dispositions légales, qui ne sont pas reprises dans le projet, alors qu'elles sont perfectibles. Le Comité se réfère, dans ce cadre, aux exemples ci-dessous. Certains d'entre eux ont déjà l'objet d'une recommandation du Comité.

12. Le Comité permanent R a recommandé à maintes reprises que les articles 19 et 20 L.R&S soient précisés par le pouvoir exécutif, mais aussi par le pouvoir législatif. Ces dispositions essentielles régissent notamment la transmission d'informations (y compris les données à caractère personnel) à d'autres services (étrangers) et la coopération/assistance technique que les deux services belges peuvent prêter, par

exemple, aux autorités judiciaires ou à des homologues étrangers. Vu la coopération croissante entre tous les acteurs du milieu de la sécurité et vu la proposition d'extension des possibilités pour le service de renseignement militaire à l'étranger, le Comité recommande une fois encore de préciser les deux articles de loi, afin qu'il ne subsiste plus le moindre doute sur le rôle et les possibilités de chacun.

13. L'article 19/1 L.R&S prévoit une obligation de déclaration particulière si la mise en œuvre d'une méthode particulière révélait une infraction ; si c'est une méthode ordinaire qui fait apparaître la même infraction, c'est l'article 29 CIC qui est d'application. Le moment et la manière dont les infractions présumées doivent être communiquées diffèrent fondamentalement. En outre, la procédure à suivre n'est pas claire dans le cas où une infraction est mise au jour par le biais d'une méthode ordinaire et où des éléments complémentaires sont ensuite recueillis par le biais d'une méthode particulière. Le Comité permanent R recommande de réexaminer cette réglementation.

14. À l'époque, le Comité avait souligné la nécessité d'une réglementation plus détaillée du travail avec les informateurs. Le Gouvernement de l'époque avait décidé de s'en remettre au Comité ministériel du renseignement et de la sécurité, qui est devenu le Conseil national de sécurité. Rien n'a encore été fait en la matière, tout comme pour de nombreux autres aspects importants de la Loi organique des services de renseignement et de sécurité. Le Comité a été informé que le Conseil national de sécurité avait donné des instructions pour l'élaboration de directives si nécessaire. Le Comité reste toutefois d'avis que dans certains domaines, c'est au législateur qu'il revient de poser les jalons. En ce qui concerne le travail avec les informateurs, le Comité propose plus spécifiquement une interdiction explicite de recueillir des informations via des informateurs en contournant des dispositions qui invoquent une obligation de garder le secret ou en court-circuitant les garanties offertes par la Loi MRD.

15. La réglementation relative à la compétence du Comité comme organe juridictionnel doit être précisée pour que le Comité puisse également se saisir lorsqu'un service utilise une méthode qui, aux termes de la loi, doit être considérée comme une méthode particulière, sans en avoir reçu l'autorisation et pour laquelle il n'y a donc aucune décision ni autorisation formelle. Le Comité fait remarquer que l'application de mesures qui doivent être considérées comme des méthodes particulières de recueil de données, mais pour lequelles aucune autorisation n'a été accordée, peut constituer une infraction, avec toutes les conséquences qui en découlent.

16. Le droit de consultation octroyé aux personnes qui saisissent le Comité en sa qualité d'organe juridictionnel est tellement étendu que les opérations de renseignement en cours peuvent être mises en péril. Le Comité recommande une adaptation de cette réglementation, même si ce cas de figure ne s'est présenté qu'une seule fois à ce jour.

Le Comité est d'avis que l'évaluation de la réglementation actuelle a essentiellement porté sur l'efficacité des services de renseignement, ce qui s'est traduit par un projet axé

sur l'octroi de compétences et de possibilités légales supplémentaires (parfois utiles et nécessaires) aux deux services de renseignement. Mais le contrôle externe et les *checks and balances* nécessaires n'ont pas toujours fait l'objet d'une attention suffisante ; ce contrôle externe est même parfois ramené à un niveau antérieur.

En ce qui concerne les compétences, les tâches et les possibilités (de collecte) supplémentaires, le Comité se réfère, par exemple, aux propositions suivantes :

17. Il est proposé de créer une équipe d'intervention (voir point 9 *supra*)

18. La description des tâches du SGRS est considérablement étendue. La portée exacte des diverses modifications apportées à l'article 11 L.R&S requiert une étude appronfondie. Le Comité a l'impression que le spectre du SGRS s'est étendu au-delà du domaine 'militaire' (par exemple recueillir des renseignements en matière de politique de sécurité nationale et internationale). Le Comité est bien conscient de l'internationalisation croissante des problèmes de sécurité et de l'absence d'un service de renseignement civil étranger. Il fait néanmoins remarquer que cela signifierait une réorientation fondamentale au regard de la réglementation actuelle, ce qui nécessite une réflexion plus approfondie. À ce propos, il convient également de vérifier si le SGRS dispose des moyens pour accomplir ces nouvelles tâches et si un contrôle adéquat peut être exercé sur ces tâches.

19. L'article 13/2 proposé octroie aux agents de renseignement la possibilité d'utiliser un nom, une identité et une qualité fictives, et ce indépendamment de la mise en oeuvre d'une autre méthode. Cette réglementation – très sommaire – offre par exemple la possibilité d'infiltrer des groupements. Jusqu'à présent, les services prétendaient ne pas souhaiter utiliser cette technique. En revanche, s'ils veulent désormais l'utiliser, cela doit être mentionné explicitement, et la mesure doit être considérée comme une méthode particulière. Il convient par ailleurs de prêter l'attention nécessaire à la protection (légale) du personnel concerné.

20. Dans la foulée, le Comité se demande si la possibilité, telle que stipulée dans le nouvel article 13/4, doit également permettre de procéder à une infiltration civile. Il ressort de l'Exposé des Motifs que ce n'est pas le cas. Toutefois, le texte de ce projet d'article n'exclut pas cette possibilité. Si telle est l'intention, il est indiqué de réfléchir sérieusement à l'opportunité et à l'encadrement (légal).

21. L'article 14 précise que le secret professionnel ne fait pas obstacle, pour les autorités publiques telles qu'un CPAS, à la communication d'informations, sur demande, aux services de renseignement. Le Comité est en faveur de cette clarification, mais n'en constate pas moins que la possibilité pour ces autorités publiques de conclure des 'accords' ou d'établir des 'règles' est supprimée. Si l'intention du projet est de priver des autorités de leur compétence d'appréciation, une réflexion approfondie doit être menée à ce propos. En effet, il faut prendre en considération le fait que certains services publics sont en possession de données à caractère personnel très sensibles (par exemple des données médicales) qui sont recueillies dans un but bien défini.

22. La modification de l'article 16 prévoit en premier lieu que des personnes ou des organisations privées peuvent à tout moment communiquer des données à caractère personnel aux services de renseignement, même si ces acteurs privés sont en possession de ces données dans un but bien défini (modification du 'principe de finalité'). Deuxièmement, il semble que l'intention est qu'une éventuelle obligation de discrétion ou de secret du détenteur de certaines données ne s'applique pas dans sa relation avec un service de renseignement. Surtout en ce qui concerne ce second aspect, cette réglementation va très loin et nécessite de mettre en balance les divers intérêts en jeu (par exemple le secret médical d'un médecin, le secret professionnel d'un avocat ou le secret des sources d'un journaliste). Le Comité signale par ailleurs que de telles données pourraient également être transmises à la justice via l'article 19 L.R&S.

23. La mise en oeuvre de méthodes particulières de recueil de données en dehors du territoire belge est élargie pour les deux services. Une limitation est prévue pour la VSSE : les méthodes doivent être mises en oeuvre *depuis* le territoire. Ainsi, c'est manisfestement la possibilité de collecter des communications/informations digitales qui est surtout étendue. Mais cette réglementation signifie-t-elle, par exemple, que la VSSE peut intercepter des communications étrangères depuis la Belgique ? Il convient d'éclaircir ce point.

24. En ce qui concerne la mise en oeuvre de méthodes particulières de recueil de données en dehors de la Belgique, le SGRS n'est soumis à aucune restriction. Si, à l'époque, le Comité avait recommandé d'examiner si *certaines* MRD pouvaient aussi être utilisées à l'étranger, il est stipulé dans le projet actuel que ce service peut mettre en œuvre *toutes* les mesures spécifiques et exceptionnelles à l'étranger. En principe, le contrôle administratif de telles méthodes est du ressort de la Commission BIM, et le contrôle juridictionnel, du ressort du Comité permanent R (même si un grand point d'interrogation subsiste sur la manière dont cela devra se passer dans la pratique). Mais pour l'interception de certaines communications, la pénétration dans des systèmes informatiques et la réalisation de photos, une réglementation de contrôle spécifique (moins poussée) s'applique (voir ci-après au point 31). Enfin, le Comité fait remarquer que l'extention des possibilités des services de renseignement de mettre en oeuvre des méthodes particulières de recueil de données à l'étranger soulève les questions relatives à la problématique de la souveraineté d'autres États et à la punissabilité d'organisations établies à l'étranger auxquelles il est demandé de coopérer. Si de tels renseignements recueillis à l'étranger se retrouvent dans un dossier pénal, il convient d'examiner comment cela s'articule avec les traités d'entraide judiciaire et l'obligation de travailler avec des commissions rogatoires.

25. Le projet introduit une nouvelle méthode spécifique : la réquisition des données de transport et de voyage auprès d'acteurs privés. Le Comité comprend l'utilité d'une telle réglementation pour le fonctionnement des services de renseignement. Vu le caractère sensible de ce genre de données sur le plan du respect de la vie privée, le Comité estime que le recueil de celles-ci doit, en effet, être considéré comme une

méthode spécifique. Le Comité souligne que l'obtention de ces données doit *toujours* être considérée comme une méthode spécifique, et ce même si, à l'avenir, il est possible de les obtenir via une autorité publique, et donc via la méthode ordinaire visée à l'article 14 L.R&S (voir Projet de loi en matière de PNR).

26. Dans la foulée, le Comité estime de manière générale que le niveau de 'protection' offert dans la Loi MRD doit être lié à 'la nature des données' (plus ou moins sensible en termes de respect de la vie privée) et pas tant avec 'la manière dont elles sont recueillies' (par des moyens de collecte propres, par une requisition, par un accès direct à un fichier…). Sinon, on en arriverait à une situation où la collecte d'une même donnée sensible sur le plan du respect de la vie privée devrait être considérée tantôt comme une méthode ordinaire, tantôt comme une méthode spécifique. Cela reviendrait à laisser aux services la possibilité de choisir les méthodes comme bon leur semble. C'est la raison pour laquelle le Comité recommande également que l'article 18/15 L.R&S soit adapté, en ce sens que le recueil de certaines données financières constitue une méthode spécifique, qui peut notamment être mise en œuvre via une réquisition adressée à des institutions bancaires.

En ce qui concerne la problématique des *checks and balances*, le Comité reprend les exemples suivants :

27. Le projet apporte des changements à certains endroits : certaines méthodes spécifiques deviennent des méthodes ordinaires et des méthodes exceptionnelles deviennent des méthodes spécifiques. Il en résulte naturellement que le contrôle est moins poussé. Le Comité donne les exemples suivants :
    - L'ouverture d'objets fermés ne demeure une méthode spécifique que dans la mesure où ces objets sont 'verrouillés'.
    - Les caméras mobiles, comme les appareils photographiques, ne sont plus considérées comme un moyen technique, si bien que leur utilisation ne change pas la nature de l'observation. Cela signifie, par exemple, que filmer un *target* ne constitue pas une méthode spécifique, indépendamment de la durée et de la fréquence des observations. Le Comité n'a pas d'objection de principe, mais attire l'attention sur le fait que des observations longues et fréquentes d'un même *target* ou d'un même groupement peuvent être très intrusives et, partant, pourraient devoir être considérées comme une méthode particulière.
    - L'observation de ce qui se passe dans des dépendances peut constituer une méthode spécifique et non plus une méthode exceptionnelle. En introduisant une nouvelle catégorie dans le projet (c'est-à-dire « *des lieux non accessibles au public qui (ne) sont (pas) soustraits à la vue* »), les dépendances de domiciles (comme le jardin) sont moins protégées en fonction de la clôture installée par l'occupant. Jusqu'à présent, les dépendances bénéficiaient de la même protection que le domicile. L'introduction d'une nouvelle catégorie de ce genre ou d'une nouvelle notion juridique peut être une source de confusion et générer des problèmes d'interprétation. Le Comité n'a pas connaissance d'exemples où cette nouvelle réglementation pourrait répondre à un besoin opérationnel évident. En effet, ce qui se passe dans les dépendances peut déjà être collecté actuellement, mais en

recourant à une méthode exceptionnelle. Enfin, le Comité tient à attirer l'attention sur l'arrêt de la Cour constitutionnelle (n°178/2015), par lequel l'article 464/27 CIC relatif à l'enquête pénale d'exécution a été annulé. Les motifs de cet arrêt sont extrêmement pertinents au regard des modifications proposées ici.

- Le projet prévoit une réglementation spécifique pour les personnes qui sont reconnues comme journalistes professionnels mais qui, selon les services de renseignement, ne méritent pas d'être reconnues en cette qualité. Le Comité s'interroge sur la légalité et sur l'utilité d'une telle réglementation. Celle-ci représentera d'ailleurs un surcroît de travail pour les services, qui doivent démontrer qu'une personne n'est pas un journaliste professionnel.
- Dans le projet, il est proposé de tenir compte, lors de l'évaluation de la subsidiarité, des risques engendrés par l'exécution de la mission de renseignement pour la sécurité des agents des services et des tiers. La prise en compte des risques pour la sécurité physique n'est pas neuve : elle était déjà stipulée à l'article 18/9 § 3 L.R&S. Mais en transposant cette disposition à l'article 2, le service concerné peut désormais décider de la mise en oeuvre d'une méthode exceptionnelle (et donc de récolter des données très sensibles en termes de respect de la vie privée), parce que les méthodes ordinaires et spécifiques représentent un danger trop important. Si telle est bien l'intention du projet, il convient de veiller étroitement à ce que cette disposition soit utilisée avec précaution.

28. Le Comité se pose de sérieuses questions sur la réglementation en vertu de laquelle un agent de renseignement peut commettre une infraction qui ensuite – et par exemple en l'absence d'éventuelles personnes lésées – pourrait être 'couverte' par la Commission BIM. Le Comité est d'avis que cette réglementation doit être fondalement revue. Il estime que, dans les cas que le projet entend régir, on peut se baser sur les notions juridiques existantes (par exemple l'état de nécessité ou la légitime défense).

29. Le Comité ne peut absolument pas souscrire à la proposition de modification de l'article 43/5 § 4 L.R&S. La réglementation actuelle, qui a été introduite à l'époque sur proposition du Sénat, stipule que les agents de renseignement doivent communiquer *toutes* les informations au Comité lorsque celui-ci contrôle la légalité d'une méthode particulière. Cette réglementation s'applique également aux informations ou documents des services de renseignement qui sont couverts par le secret de l'enquête. Toutefois, le président du Comité doit, dans ce cas, se concerter avec le magistrat compétent. Il peut ainsi tenir compte de ses préoccupations. La même réglementation vaut d'ailleurs pour l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. La modification proposée pourrait avoir comme conséquence que le Comité, en sa qualité d'organe juridictionnel, doive évaluer la légalité de la méthode *sans* disposer de toutes les informations qui ont été recueillies ou élaborées par les services de renseignement. Le Comité insiste sur le fait qu'il n'a pas connaissance de cas où la réglementation actuelle se serait révélé problématique pour le secret de l'enquête. Le Comité souligne par ailleurs que de telles informations ne sont *jamais* partagées avec des tiers.

30. Comme cela a déjà été mentionné (voir point 4), le projet omet de prévoir une réglementation pour la notification des *targets* de l'utilisation de méthodes secrètes.

31. La réglementation qui permet au SGRS d'intercepter des communications à l'étranger a été élaborée à un moment où les signaux radio constituaient l'essentiel des interceptions. Depuis lors, la technologie a tellement évolué que le Comité avait déjà recommandé au législateur de revoir la réglementation. Les révélations d'Edward Snowden et l'intention du SGRS de procéder à du *cable-tapping* rend cette révision d'autant plus urgente. Le Comité constate que le domaine de compétence du SGRS est considérablement élargi (voir point 8) et que le service – à juste titre – se voit attribuer davantage de possibilités de collecte. Toutefois, ce double constat signifie pour le Comité qu'il convient de définir clairement ce qui peut être fait ou pas, et qu'un réel moyen de contrôle doit être prévu. Certains éléments doivent être de toute façon examinés, à savoir la mesure dans laquelle les interceptions doivent être ciblées ou non et à la demande de qui, le degré de précision du Plan d'écoutes annuel (par exemple, les sélecteurs au lieu de pays ou des termes génériques), la possibilité de procéder à du *datamining* en vrac et la question de savoir si les opérations SIGINT à l'étranger doivent toujours s'inscrire dans un conflit armé ou un dans un 'mandat international'. Le Comité estime que ces aspects ne sont pas suffisamment traités dans la réglementation proposée. Il rappelle que dans les faits, il est d'accord que les capacités réelles du SGRS au niveau SIGINT sont beaucoup trop limitées, mais que le projet actuel instaure une compétence générale d'interception sur toutes les compétences (élargies) du service, avec la collaboration obligatoire des opérateurs. Il en résulte que le SGRS peut surveiller en masse tous les moyens de communication depuis ou vers l'étranger. En revanche, la réglementation légale est sommaire, étant donné qu'elle ne prévoit que des moyens de contrôle limités. De l'avis du Comité, ceux-ci ne répondent pas aux exigences de la CEDH, par exemple. Toutes ces questions requièrent un débat parlementaire approfondi et documenté.

CONCLUSION

Vu les délais impartis, le Comité a dû se limiter aux modifications qui méritaient une attention critique. De manière générale, le Comité recommande que les propositions de modification qui sont reprises soient précisées quant à leur finalité et, dans certains cas, soient détaillées dans le projet. En outre, certaines options fondamentales doivent faire l'objet d'une réflexion approfondie. Le Comité recommande par ailleurs que le contrôle soit porté à un niveau adéquat. Ces considérations doivent s'inscrire dans le souci de répondre aux exigences fondamentales telles que celles qui découlent des normes juridiques nationales et internationales. Enfin, le Comité entend souligner que le projet, vaste, contient de nombreux éléments positifs, et ce tant sur le plan légistique que du point de vue des besoins opérationnels des deux services de renseignement.

ANNEXE F.
AVIS COMMUN N° 01/2016 DU 20 JUIN 2016 CONCERNANT LA DÉCLARATION PRÉALABLE DE LA BANQUE DE DONNÉES COMMUNE '*FOREIGN TERRORIST FIGHTERS*'[290]

L'Organe de contrôle de l'information policière (ci-après C.O.C.) et le Comité permanent de contrôle des services de renseignement et de sécurité (ci-après Comité R) ;

Vu la loi du 5 août 1992 sur la fonction de police (ci-après LFP), et plus particulièrement l'article 44/11/3*bis*, § 3 ;

Vu la demande d'avis des ministres de l'Intérieur et de la Justice, reçue par le C.O.C. le 30/05/2016 et par le Comité R le 14/06/2016 ;

Émettent, le 20 juin 2016, l'avis suivant :

A. OBJET DE LA REQUÊTE ET ASPECTS PROCÉDURAUX

1. Le 30 mai dernier, les ministres de la Justice et de l'Intérieur ont transmis au C.O.C. et au Comité R une demande d'avis, conformément à l'article 44/11/3*bis*, § 3 de la LFP. Cette demande porte sur la déclaration préalable de la banque de données commune 'Foreign Terrorist Fighters' (ci-après banque de données FTF). Conformément à l'article précité, le C.O.C. et le Comité R doivent émettre un avis commun endéans les trente jours.

2. L'article 44/11/3*bis*, § 4 de la LFP[291] impose néanmoins que pour chaque banque de données commune, un Arrêté royal fixe les règles relatives aux responsabilités en matière de protection de la vie privée, des organes, services et organismes qui traitent des données, les règles relatives à la sécurité du traitement ainsi que les règles d'utilisation, de conservation et d'effacement des données. Un tel Arrêté royal doit être soumis à l'avis de la Commission pour la Protection de la Vie Privée (ci-après CPVP).

3. À ce jour, il n'existe pas encore d'Arrêté royal fixant les règles pour la banque de données FTF. Conformément au courrier susmentionné des ministres de l'Intérieur et de la Justice, un projet d'Arrêté royal a été soumis à la CPVP. Il est possible que la CPVP émette des remarques (fondamentales) sur ce projet, et que celui-ci doive être, en conséquence, (drastiquement) modifié. Ceci a naturellement un impact sur la déclaration de la banque de données FTF et sur l'avis conforme du C.O.C. et du Comité R. En ce qui concerne les déclarations futures de banques de données

290 Le Comité permanent R a traduit librement le présent avis dans le cadre de son Rapport d'activités 2016.

291 Inséré par la Loi du 14 avril 2016 portant sur les mesures complémentaires en matière de lutte contre le terrorisme.

communes, le C.O.C. et le Comité R insistent dès lors pour que ces déclarations soient faites après la publication de l'Arrêté royal relatif à cette banque de données, et ce pour éviter que des déclarations prématurées ne doivent être modifiées par la suite et afin de permettre au C.O.C. et au Comité R d'émettre un avis portant sur la version et la structure définitives de la banque de données commune, ainsi que sur ses modalités de traitement.

4. Dans le courrier du 30 mai dernier émanant des ministres compétents, le projet d'Arrêté royal *relatif à la banque de données communes Foreign Terrorist Fighters et portant exécution de certaines dispositions de la section 1 bis «la gestion de l'information» du chapitre IV de la loi sur la fonction de police* (ci-après projet d'Arrêté royal) a été ajouté, ainsi qu'une note intitulée «*déclaration préalable des motifs de la banque de données commune Foreign Terrorist Fighters*» (ci-après 'déclaration préalable').[292] Cette déclaration préalable ne constitue cependant pas une déclaration pour le C.O.C. et le Comité R, en raison du manque d'informations fondamentales relatives à la banque de données.

5. Toutefois, le C.O.C. et le Comité R émettent ci-après, dans ce dossier, un avis provisoire concernant cette déclaration préalable, des modifications étant encore susceptibles d'être apportées au projet d'Arrêté royal (voir *infra* n° 7, 13, 15, 17). Ils se réservent néanmoins le droit de formuler un avis complémentaire après la publication de l'Arrêté royal sur la banque de données FTF, et après d'éventuelles déclarations complémentaires pour cette banque de données.

B. SUR LE FOND

6. Une analyse du document 'déclaration préalable' est développée ci-après. Cette analyse tient compte de la structure du document.

1. Finalité

7. Conformément à la déclaration, la banque de données FTF contribue à l'analyse, à l'évaluation et au suivi des *Foreign Terrorist Fighters* qui se trouvent dans une des situations telles que décrites au point 7 de la déclaration. Ces situations concernent tant des recruteurs et des propagandistes que des personnes ayant des intentions purement terroristes en Belgique, ce qui amène le C.O.C. et le Comité R à s'interroger. En effet, le rapport au Roi sur le projet d'Arrêté royal établit à la page 2 que «*Grâce à cette banque de données, une fiche de renseignements sur des personnes impliquées dans le phénomène des combattants qui se rendent dans des zones de combat djihadiste permet non seulement de pouvoir évaluer la menace potentielle que représentent ces*

292 Il convient de préciser que dans l'annexe du courrier du 30 mai 2016, envoyé par les ministres de la Justice et de l'Intérieur au Comité permanent R, il est question, dans la version néerlandaise, de «*voorafgaandelijke toelichting*», traduit en français par «*déclaration préalable*».

personnes mais surtout d'en assurer un suivi afin d'anticiper et d'empêcher de possibles actes terroristes de leur part». Dans la circulaire confidentielle COL 10/2015 du Collège des Procureurs généraux des Cours d'appel concernant l'approche judiciaire relative aux *Foreign Terrorist Fighters*, il est question d'une catégorie 6 'appui et recrutement'. La prise en compte de cette catégorie supplémentaire accroîtrait encore l'utilité opérationnelle de la banque de données FTF.

8. Si le but est effectivement de ne prévoir que les 5 catégories, dont il est question au point 7 de la déclaration, le C.O.C. et le Comité R veilleront, durant leur mission de contrôle, à ce que seules ces catégories de la banque de données FTF soient concernées. Ils ne prendront donc pas en considération la sixième catégorie, ni les personnes ayant des velléités terroristes et extrémistes en Belgique[293] (même si elles ont reçu ou exécuté des missions depuis l'étranger), ni les vecteurs radicalisants au sein de la société.

2. Base légale et réglementaire

9. On peut se référer ici aux remarques formulées au point 3. La déclaration préalable ne fait, jusqu'à présent, aucune référence à la publication d'un Arrêté royal. L'Arrêté royal relatif à une banque de données commune devra précéder une déclaration en la matière. Cet Arrêté royal pourra alors être repris dans la déclaration. Il est essentiel pour les organes de contrôle que tant la banque de données commune que son cadre juridique soient établis sans équivoque, avant de se prononcer définitivement sur les banques de données communes proposées.

3. Conseiller en sécurité et en protection de la vie privée

10. La déclaration ne fait aucune mention du conseiller en sécurité et en protection de la vie privée, qui doit être désigné par les ministres de l'Intérieur et de la Justice. Cette personne est cependant très importante dans le cadre des missions de contrôle du C.O.C. et du Comité R, étant donné que, conformément à l'article 44/3, § 1er/1 de la LFP, elle est chargée des contacts avec le C.O.C. et avec le Comité R. Cette personne devrait donc être reprise dans la déclaration. Il importe donc que le conseiller en sécurité et en protection de la vie privée soit impliqué dans la conception et dans le déploiement de la banque de données commune, et donc qu'il soit désigné le plus rapidement possible. La mention de ce dernier dans la déclaration aux organes de contrôle leur permettra d'avoir une vue sur le niveau d'indépendance de l'intéressé par rapport aux autorités, organes, organismes, services, directions ou de la commission tels qu'énoncés à l'article 44/11/3*ter* de la LFP.

5. Responsable opérationnel

11. L'Organe de coordination pour l'analyse de la menace (ci-après OCAM) est repris dans la déclaration en tant que responsable opérationnel. Pour faciliter les missions

293 Extrémisme pouvant mener au terrorisme (cf. art. 44/2, § 2 LFP).

de contrôle, il est recommandé de mentionner, dans la déclaration, les noms des responsables qui pourront être contactés par le C.O.C. et par le Comité R.

6. Gestionnaire

12. La Police fédérale est désignée en tant que gestionnaire. À nouveau, il peut être relevé que la déclaration doit au moins préciser quel est le service responsable au sein de la Police fédérale, et reprendre les noms de quelques personnes de contact au sein de ce service.

7. Personnes faisant l'objet d'un enregistrement dans la banque de données

13. Référence peut être faite ici aux remarques formulées aux points 7 et 8. En outre, la déclaration préalable, conformément à l'article 6, 3° du projet d'Arrêté royal, précise que seuls les renseignements non classifiés concernant ces personnes font l'objet d'un traitement. Cela induit qu'en pratique, la Sûreté de l'État, le SGRS et l'OCAM n'alimenteront probablement que très peu cette banque de données, étant donné qu'ils disposent de beaucoup d'informations qui sont classifiées. Cependant, la loi[294], à l'article 44/2 § 2 de la LFP, prévoit une obligation d'alimentation pour les différents services. L'article 44/11/3*ter* § 5 de la LFP prévoit une exception à cette obligation pour les services de renseignement et de sécurité, si le dirigeant juge qu'alimenter cette banque de données peut mettre en danger la vie d'une personne, ou s'il s'agit d'informations confidentielles émanant d'un service étranger. Aucune exception globale n'a été introduite en ce qui concerne les informations classifiées. Dès lors, la question se pose de savoir comment le projet d'Arrêté royal peut, à l'article 6,3° déroger à l'obligation d'alimentation telle que prévue dans la LFP, ou à tout le moins la réduire très fortement. Outre cette question purement juridique, se pose également et surtout la question opérationnelle de savoir s'il faut écarter toutes les informations classifiées de la banque de données FTF, d'autant plus que, conformément aux directives internes de la Police fédérale, tous les membres des services de police qui souhaitent avoir un accès à la banque de données FTF (au moins) doivent/devront disposer d'une habilitation de sécurité du niveau 'secret'. Cette exigence d'habilitation de sécurité du niveau 'secret' est également prévue à l'article 7 § 2 du projet d'Arrêté royal.

---

294 Voir aussi les travaux préparatoires de la loi relative à des mesures complémentaires en matière de lutte contre le terrorisme (*Doc. parl.*, Chambre 2015-2016, DOC 54, 1727/1, 21-22) : « *Ces données et informations relatives à différentes catégories de données ne sont en principe pas des données à caractère personnel ou des informations classifiées. Il convient en effet de permettre le partage assez large de données et d'informations sans mettre des barrières à leur traitement. Toutefois, s'il est absolument nécessaire que de telles données soient traitées dans ces banques de données afin de rencontrer les finalités pour lesquelles elles ont été créées, alors la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité est d'application. Dès lors, toute personne qui souhaite par exemple accéder à ces données et informations classifiées doit disposer de l'habilitation de sécurité appropriée* ».

14. Dans le prolongement de la question de savoir si les données classifiées ou les informations policières sensibles doivent ou non être reprises dans la banque de données commune, le C.O.C. et le Comité R renvoient à la problématique suivante : la Loi et le projet d'Arrêté royal (article 4) chargent l'OCAM de valider, *« sur base des données et informations qui figurent dans cette banque de données »*, si une personne peut être considérée comme FTF. Si une information essentielle concernant une personne n'est pas ajoutée à la banque de données commune en raison de sa classification ou de son caractère sensible, l'OCAM ne reprendra pas cette information dans son évaluation, alors qu'il disposera effectivement de cette information classifiée sur base de la Loi du 10 juillet 2006 relative à l'analyse de la menace.

8. Catégories et types de données personnelles et d'informations

15. Les données d'identification des utilisateurs de la banque de données FTF sont également reprises dans la banque de données. Conformément à l'article 7, § 3 du projet d'Arrêté royal, chaque service doit établir une liste des personnes disposant d'un accès et la transmettre au gestionnaire. Par dérogation à cet article, la liste des services de renseignement et de sécurité est tenue à la disposition de la seule CPVP. Ces listes ne devraient pas uniquement être transmises au gestionnaire, mais également aux organes de contrôle, c'est-à-dire le C.O.C. et le Comité R. En outre, la liste reprenant les services de renseignement et de sécurité devrait être mise à la disposition du Comité R et non de la CPVP. La CPVP n'a, en effet, aucune mission spécifique de contrôle dans le cadre de cette banque de données en ce qui concerne les services de renseignement et de sécurité. Il est dès lors recommandé de modifier le projet d'Arrêté royal en ce sens.

9. Services concernés et nature des accès

16. Conformément à la déclaration, trois services pourront utiliser la banque de données : les services de base, les services partenaires ou d'autres autorités publiques belges, d'autres organes ou organismes publics qui sont chargés, par la loi, de l'application de la loi pénale ou qui ont des missions légales de sécurité publique. Ceci concerne un certain nombre de services pour lesquels on peut se demander pourquoi ils doivent avoir accès à la banque de données FTF.[295] Conformément aux travaux préparatoires[296], un tel accès peut être nécessaire aux niveaux stratégique, tactique et opérationnel. Et les travaux préparatoires[297] d'indiquer que cela ne signifie pas que tous ces acteurs auront accès sans raison particulière à la banque de données commune, mais que seuls certains d'entre eux pourront y avoir accès, sur base des

295 Voir, dans le même ordre d'idées, l'avis n° 57/2015 de la CPVP relatif au projet de loi relative aux mesures complémentaires de lutte contre le terrorisme du 16 décembre 2015, plus spécifiquement le n° 77.

296 *Doc. parl.*, Chambre 2015-2016, DOC 54, 1727/1, 20 (Exposé des Motifs sur le projet de Loi portant sur des mesures complémentaires dans la lutte contre le terrorisme).

297 *Doc. parl.*, Chambre 2015-2016, DOC 54, 1727/1, 15.

finalités propres de la banque de données commune, de leurs compétences légales et en fonction de leur 'besoin d'en connaître' (*'need to know'*). Au sein des services partenaires, par exemple, on peut s'interroger sur le fondement d'un accès pour la Commission Permanente de la Police Locale (qui est un organe exclusivement stratégique). Le principe de base de l'accès à une telle banque de données opérationnelle (ou aux informations contenues dans celle-ci) doit être celui du *'need to know'* et non celui du *'nice to know',* qui plus est quand on veut éviter d'hypothéquer l'indispensable *'need to share'* entre les différents services. Par conséquent, tous les services qui ne satisfont pas au *'need to know'* devraient être exclus de tout accès à la banque de données ou avoir un accès limité à certaines informations. Bien entendu, cela ne veut pas dire qu'ils ne pourraient pas alimenter cette banque de données. On peut réfléchir à des systèmes permettant à un service donné de fournir des informations, sans pour autant disposer d'un accès à la banque de données FTF.

17. L'article 7, § 1er, dernier alinéa du projet d'Arrêté royal prévoit que l'accès pour, entre autres, les Maisons de Justice est limité aux données et aux informations personnelles sur les *Foreign Terrorist Fighters* pour lesquels le service est chargé d'un accompagnement judiciaire et d'une surveillance. La question est de savoir comment cela pourra être géré au niveau technique afin d'éviter que, au sein des Maisons de Justice, des recherches puissent être faites sur d'autres personnes que celles qui bénéficient d'un accompagnement. Une solution pourrait consister à mettre à la disposition du gestionnaire de la banque de données une liste mise à jour de manière permanente sur tous les dossiers en cours au sein des Maisons de Justice, c'est-à-dire les dossiers pour lesquels il existe un mandat judiciaire en matière de FTF. Dans tous les cas, il faudra examiner attentivement tous les accès à la banque de données FTF de la Maison de Justice et vérifier s'ils correspondent à un dossier concret. Une garantie supplémentaire pourrait être de limiter strictement les accès, pour chaque Maison de Justice, par exemple à un (ou quelques) assistant(s) de justice spécialement chargé(s) du suivi des dossiers FTF. D'autre part, il conviendrait également de désigner un conseiller en sécurité et en protection de la vie privée au sein des services ayant accès à la banque de données FTF. Le C.O.C. et le Comité R examineront si les accès (que ce soit un accès direct ou une interrogation directe) des services partenaires et des autres autorités publiques belges, autres organes ou organismes publics qui sont chargés par la loi de l'application de la loi pénale ou qui ont des missions légales de sécurité publique, sont conformes aux dispositions légales et conformes à la déclaration de la banque de données commune. Il est recommandé de prévoir explicitement la désignation d'un tel conseiller au sein des différents services concernés dans le projet d'Arrêté royal.

18. Dans le prolongement des points 16 et 17, le C.O.C. et le Comité R insistent sur le fait que dans la déclaration, il convient de mentionner clairement quel service et quelles fonctions ou personnes au sein d'un service ont accès (à la banque de données commune), à quelles catégories concrètes de données et avec quels objectifs concrets.

19. Les différents services sont responsables de la validation interne des données qu'ils transmettent. Ces règles de validation doivent être insérées dans la déclaration, et ce afin que le C.O.C et le Comité R puissent exercer leur mission de contrôle.

20. Pour un suivi effectif de leur mission de contrôle, il convient, selon le C.O.C. et le Comité R, de prévoir une possibilité de vérifier quel était l'état et le contenu d'une fiche d'informations donnée à un moment donné. Un historique des fiches de renseignements doit pouvoir être réalisé sur demande des organes de contrôle.

10. Modalités relatives au traitement des données

21. Conformément au point 10.4 de la déclaration, le système interne de validation est communiqué au responsable opérationnel par chaque service de base et par chaque service partenaire; le responsable opérationnel le transmettra au gestionnaire et au conseiller en sécurité et en protection de la vie privée. Comme déjà mentionné au point 19, ces règles internes de validation doivent également être transmises au C.O.C. et au Comité R, afin qu'ils puissent effectuer leur mission de contrôle. Le système de validation interne doit également prévoir que les données et les informations personnelles introduites par les services concernés soient pertinentes et non excessives conformément à l'article 44/2, § 2 de la LFP et à l'article 44/11/3*bis* § 2 de la LFP.

22. En ce qui concerne la transmission de données personnelles et d'autres informations d'une banque de données commune vers des services ou des organes étrangers de renseignement qui sont chargés de l'analyse de la menace, l'article 44/11/3*quinquies*, alinéa 3 de la LFP dispose que le Roi doit en déterminer les règles. L'article 15 § 3 du projet d'Arrêté royal stipule que ces communications doivent avoir lieu conformément à l'article 20 § 3 de la Loi du 30 novembre 1998 portant sur l'analyse de la menace.

23. L'article 20 § 3 de la Loi du 30 novembre 1998 stipule à son tour que les conditions de collaboration avec les services de renseignement étrangers doivent être précisées par le Conseil national de sécurité (précédemment le Comité Ministériel du Renseignement et de la Sécurité). Toutefois, le C.O.C. et le Comité R ne sont pas au courant d'éventuelles directives qui auraient été émises par le Conseil national de sécurité. Il est évidemment impossible pour un organe de contrôle de vérifier le respect d'éventuelles directives si celles-ci ne leur ont pas été communiquées. L'absence de directive et la non-communication de directives qui auraient été émises affaiblissent en même temps le contrôle parlementaire. Dans ce cadre, les organes de contrôle renvoient aux nombreuses recommandations formulées au cours des années précédentes par le Comité R en vue de régler ces dispositions de manière urgente.[298] Dès lors, le projet d'Arrêté royal doit lui-même fixer les règles qui sous-

[298] COMITÉ PERMANENT R, *Rapport d'activités 2006*, 4 et 132; *Rapport d'activités 2013*, 4 et 111; *Rapport d'activités* 2014, 112-113 et *Rapport d'activités 2015*, tbc ('Enquête de contrôle

tendent le partage des données avec l'étranger ; il ne peut pas simplement se référer à une obligation légale similaire, qui n'a pas encore été appliquée.[299] Ici encore, il conviendra de prêter davantage attention à la problématique des 'listes noires' de l'étranger, dans lesquelles des Belges peuvent se retrouver comme suite à un échange de données.[300]

24. En ce qui concerne l'article 8, 3° de la Loi du 10 juillet 2006, la même remarque est d'application : la définition des modalités par le Conseil national de sécurité en matière d'échange de données avec des services homologues fait défaut.

POUR CES RAISONS,
Le C.O.C. et le Comité R,

Émettent un avis temporaire et favorable sous réserve des remarques reprises aux points 3-5, 7, 10-12, 15-20 et 22-24.

Avis approuvé lors de la séance plénière commune de l'Organe de contrôle sur l'information policière et du Comité permanent R de contrôle sur les services de renseignement et de sécurité en date du 20 juin 2016.

Pour le C.O.C.,
Le Président,

Philippe ARNOULD

Pour le Comité permanent R,
Le Président,

Guy RAPAILLE

relative à la position sur l'information des deux services de renseignement portant sur le recrutement, l'envoi, le séjour et le retour de jeunes (de Belgique et d'autres nationalités résidant en Belgique) qui partent ou sont partis en Syrie ou en Irak et portant sur l'échange d'informations avec diverses autorités').

299 D'un point de vue strictement juridique, on peut s'interroger sur le fait que le projet d'article 15 § 3 est une application correcte de la délégation au Roi prévue à l'article 44/11/3*quinquies*, dernier alinéa de la LFP.

300 Voir 'Enquête de contrôle relative à la plainte d'un ressortissant tunisien résidant en Belgique déclarant avoir été suivi par les services de renseignement' (*Rapport d'activités 2015*, tbc). Dans le cadre des demandes d'informations émanant de services étrangers ou dans le cadre de l'insertion de personnes sur des listes, le Comité permanent R recommande aux services de s'assurer de l'exactitude de leurs renseignements et de s'assurer de la base juridique de la transmission d'informations, tant au niveau national qu'international, en gardant à l'esprit les conséquences éventuelles pour les personnes concernées. En outre, il est conseillé de tendre vers un équilibre entre, d'une part, les exigences de sécurité collectives et multilatérales et, d'autre part, les droits des citoyens qui figurent sur de telles listes.

AVIS COMMUN N° 02/2016 DU 1er DÉCEMBRE 2016 CONCERNANT LA DÉCLARATION PRÉALABLE DE LA BANQUE DE DONNÉES COMMUNE '*FOREIGN TERRORIST FIGHTERS*'

L'Organe de contrôle de l'information policière (ci-après C.O.C.) et le Comité permanent de contrôle des services de renseignement et de sécurité (ci-après Comité permanent R) ;

Vu la loi du 5 août 1992 sur la fonction de police (ci-après LFP), et plus particulièrement l'article 44/11/3*bis*, § 3 ;

Vu la demande d'avis des ministres de l'Intérieur et de la Justice, reçue le 3 novembre 2016 ;

Émettent, le 1er décembre 2016, l'avis suivant :

A. OBJET DE LA REQUÊTE ET ASPECTS PROCÉDURAUX

1. Le 3 novembre dernier, les ministres de la Justice et de l'Intérieur ont transmis, au C.O.C et au Comité permanent R, une demande d'avis, conformément à l'article 44/11/3*bis*, § 3 de la LFP. Cette demande porte sur la déclaration préalable de la banque de données commune 'Foreign Terrorist Fighters' (ci-après banque de données FTF). Conformément à l'article précité, le C.O.C. et le Comité permanent R doivent émettre un avis commun endéans les trente jours. Le *'User guide'* et le *'Manuel d'utilisation de la base de données dynamique FTF'* étaient joints au courrier susmentionné des ministres compétents.

2. Le C.O.C. et le Comité permanent R ont déjà rendu un avis commun provisoire sur une déclaration préalable de la banque de données FTF, avis dans lequel ils se réservaient le droit de formuler un avis complémentaire après la publication de l'Arrêté royal sur la banque de données FTF, et à la suite d'éventuelles déclarations complémentaires à cette banque de données. Aussi, émettent-ils ci-après un avis complémentaire sur la 'déclaration préalable' actuelle.

B. SUR LE FOND

3. Ci-après suit une analyse du document 'déclaration préalable', qui tient compte de sa structure. Seuls les points pertinents sont repris. On ajoutera au préalable que pour le C.O.C. et le Comité permanent R, ce qu'on entend par un 'jugement en cours' sous la rubrique 8, b) 'données judiciaires' n'est pas toujours clair, d'autant plus que l'existence d'une instruction en cours est reprise sous la rubrique 8, d) et chaque condamnation/acquittement est aussi repris(e) sous la rubrique 8, b). Peut-être cela signifie-t-il un non-lieu ou une ordonnance de renvoi par une juridiction d'instruction ?

En ce qui concerne le point 1. Conseiller en sécurité et en protection de la vie privée

4. La déclaration préalable ne fait pas mention du conseiller en sécurité et en protection de la vie privée, qui doit être désigné par les ministres de l'Intérieur et de la Justice. Cette personne est pourtant très importante dans le cadre des missions de contrôle du C.O.C. et du Comité permanent R, étant donné que, conformément à l'article 44/3, § 1er/1 LFP, il ou elle est chargé(e) des contacts avec le C.O.C. et le Comité permanent R. Cette personne doit donc être reprise dans la déclaration. En outre, il importe que le conseiller en sécurité et en protection de la vie privée soit impliqué dans la conception et dans le déploiement de la banque de données commune, et donc qu'il soit désigné dans les meilleurs délais. La mention de celui-ci dans la déclaration destinée aux organes de contrôle permettra à ceux-ci de se faire immédiatement une idée du niveau d'indépendance que l'intéressé doit avoir à l'égard des autorités, des organes, des organismes, des services, des directions ou de la commission, tels que visés à l'article 44/11/3*ter* LFP. L'importance de cette fonction a encore été soulignée à l'article 5 de l'AR 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 (ci-après abrégé comme suit : 'AR FTF') et dans le rapport au Roi relatif à cet article.

5. En revanche, la désignation d'un conseiller en sécurité et en protection de la vie privée est prévue dans les différents services (OCAM, Police intégrée, VSSE, SGRS, DG établissements pénitentiaires, Ministère public, CTIF et Office des étrangers) qui ont accès à la banque de données FTF, comme proposé dans l'avis commun n°01/2016 au point 17, dernière phrase. Le C.O.C. et le Comité permanent R rappellent qu'ils doivent être tenus informés de la désignation de conseillers supplémentaires pour les nouveaux services qui recevraient un accès à la banque de données FTF.

En ce qui concerne le point 9. Services concernés et nature des accès

6. Conformément à l'explication donnée dans la déclaration préalable, trois catégories de services pourront utiliser la banque de données : les services de base, les services partenaires et d'autres autorités publiques belges, d'autres organes ou organismes publics, qui, par la loi, sont chargés de l'application de la loi pénale ou qui ont des missions légales de sécurité publique. Le C.O.C. et le Comité permanent R rappellent que le principe de base de l'accès à une telle banque de données (et aux informations qu'elle renferme) doit être celui du '*need to know*', et non celui du '*nice to know*', d'autant plus si l'on veut éviter d'hypothéquer l'indispensable '*need to share*' entre les services concernés. Par conséquent, tous les services qui n'y satisfont pas doivent être exclus de tout accès à la banque de données ou voir leur accès limité à certaines données. Ce qui ne signifie évidemment pas qu'ils ne pourraient pas alimenter cette banque de données. On peut envisager des systèmes permettant que les informations soient fournies par un service déterminé, sans que celui-ci doive pour autant disposer d'un accès (complet ou non) à la banque de données FTF. À ce propos, le C.O.C. et le Comité permanent R se réfèrent aussi à l'avis commun n° 01/2016 du 20 juin 2016, point 17, concernant les Maisons de Justice.

7. Dans l'avis commun n° 01/2016 précité, le C.O.C. et le Comité permanent R avaient aussi évoqué le fait que dans la déclaration, il convenait de mentionner clairement quel service et quelles fonctions ou personnes au sein de ce service ont accès à cette banque de données commune, à quelle catégorie concrète de données, et avec quels objectifs concrets. Le point 9.2 de la déclaration préalable énumère les accès par service concerné (accès direct *et* interrogations directes). Les objectifs concrets sont toutefois souvent oubliés ; il est dès lors recommandé que les services concernés soient en mesure de les communiquer au C.O.C. et au Comité permanent R via leur conseiller en sécurité et en protection de la vie privée respectif. Enfin, en ce qui concerne l'accès direct des Maisons de Justice et de la 'Vlaams Agentschap Jongerenwelzijn', le C.O.C. et le Comité permanent R notent que les modalités pratiques seront définies dans une déclaration complémentaire.

8. Les différents services valident eux-mêmes, en interne, les données qu'ils fournissent. Afin de rendre possible un contrôle du C.O.C. et du Comité permanent R, il convient que ces règles de validation soient insérées dans la déclaration. Celles-ci sont reprises au point 10.4 de la déclaration préalable et sous le point 10 ci-après.

9. Enfin, selon le C.O.C. et le Comité permanent R, pour un suivi effectif de leur mission de contrôle, il convient de prévoir une possibilité de vérifier quel était l'état et le contenu d'une fiche d'information spécifique à un moment spécifique. Un historique des fiches d'informations doit pouvoir être réalisé sur demande des organes de contrôle. Ce point n'est pas abordé dans la déclaration préalable. Le C.O.C. et le Comité permanent R insistent pour que cette possibilité soit tout de même prévue, ou alors pour obtenir des explications sur une éventuelle impossibilité. La conservation d'un historique est en tout cas essentielle aux fins du contrôle. Sinon, il est toujours particulièrement problématique de pouvoir retrouver qui savait ou devait savoir quoi, à quel moment. Mais également en vue de la réalisation d'enquêtes, la conservation d'un tel historique semble pour le moins très utile. Il convient d'ailleurs de signaler que veiller à la traçabilité est une des missions du gestionnaire de la banque de données FTF, c'est-à-dire la Police fédérale (article 3, 2e tiret AR FTF du 21 juillet 2016 et le rapport au Roi à cet article). À juste titre, le rapport précité mentionne également à l'article 6 qu' « *enfin, les données à caractère personnel ou, en ce qui concerne les membres des services de renseignements et de sécurité, les codes d'identification des utilisateurs sont également enregistrées (logging) dans la banque de données F.T.F., ce qui est non seulement intéressant sur le plan opérationnel (savoir qui a ajouté telle donnée permet de renforcer la collaboration entre les différents partenaires) mais aussi sur le plan de la sécurité (qui a modifié, supprimé, quand, …)* ».

En ce qui concerne le point 10. Modalités relatives au traitement des données

10. Conformément au point 10.4, le système interne de validation, rendu obligatoire à l'article 8, § 1er, alinéa 1er de l'AR FTF (et qui, conformément à l'article 8, § 1er, alinéa 2 de l'AR FTF, doit être transmis au C.O.C. et au Comité permanent R), est inventorié pour les différents services : l'OCAM, la Police fédérale, le SGRS, la VSSE, la CTIF et l'OE, même si, dans de nombreux cas, cet inventaire est trop sommaire, voire

complètement inexistant (comme pour l'OE). En effet, dans le système interne de validation, il convient de veiller à ce que les données à caractère personnel et les informations que les services concernés introduisent dans le système soient adéquates, pertinentes en la matière, et qu'elles ne soient pas excessives à la lumière des objectifs définis à l'article 44/2, § 2 LFP et aux objectifs prévus à l'article 44/11/3*bis* § 2 LFP. Par conséquent, le C.O.C. et le Comité permanent R exhortent les services concernés à en tenir compte dans l'élaboration de leur système interne de validation, de sorte qu'il puisse être démontré (notamment au C.O.C. et au Comité permanent R, au moyen d'un document) que les données à caractère personnel et les informations que les services concernés introduisent dans le système sont adéquates, pertinentes en la matière et non excessives à la lumière des objectifs définis à l'article 44/2, § 2 LFP et aux objectifs prévus à l'article 44/11/3*bis*, § 2 LFP.

POUR CES RAISONS,
Le C.O.C. et le Comité permanent R,

Émettent un avis favorable sous réserve des remarques reprises aux points 4, 6-7 et 9-10.

Avis approuvé le 1er décembre 2016 par l'Organe de contrôle de l'information policière et le Comité permanent R de contrôle des services de renseignement et de sécurité.

Pour l'Organe de contrôle
Le président du C.O.C.,

(sign.) Philippe ARNOULD

Pour le Comité permanent R
Le président du Comité permanent R,

(sign.) Guy RAPAILLE

ACTIVITEITENVERSLAG 2016
RAPPORT D'ACTIVITÉS 2016

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.

ACTIVITEITENVERSLAG 2016

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

intersentia
Antwerpen – Cambridge

Voorliggend *Activiteitenverslag 2016* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 26 september 2017.

(*getekend*)
Guy Rapaille, voorzitter
Gérald Vande Walle, raadsheer
Pieter-Alexander De Brock, raadsheer
Wouter De Ridder, griffier

Activiteitenverslag 2016
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

ISBN 978-94-000-0897-7
D/2017/7849/129
NUR 823

INHOUD

LIJST MET AFKORTINGEN

ADCC	Algemene Directie Crisiscentrum
ADIV	Algemene Dienst Inlichting en Veiligheid
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
CCB	Centrum voor Cybersecurity België
CCIRM	*Collection coordination and intelligence requirements management*
CFI	Cel voor Financiële Informatieverwerking
CGVS	Commissariaat-generaal voor de Vluchtelingen en de Staatslozen
CHOD	Chief of Defence
CNCIS	*Commission nationale de contrôle des interceptions de sécurité*
CNCTR	*Commission nationale de contrôle des techniques de renseignement*
COC	Controleorgaan voor politionele informatie
COPPRA	*Community policing and prevention of radicalisation and terrorism*
CRIV	Compte Rendu Intégral – Integraal Verslag
CTG	*Counter Terrorism Group*
CTIVD	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten
DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
DGEPI	Directoraat-generaal Penitentiaire Instellingen
DGLV	Directoraat-generaal Luchtvaart
DGSU	Directoraat-generaal Uitvoering Straffen en Maatregelen
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*
GCHQ	*General Communications Headquarters*
IOCCO	*Interception of Communications Commissioner's Office*
Parl. St.	Parlementaire Stukken van Kamer en Senaat
Hand.	Handelingen
HUMINT	*Human intelligence*
ICT	Informatie- en communicatietechnologie
IMINT	*Image intelligence*
IOB	*Intelligence Outlook Bulletins*
IS	Islamitische Staat
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 van 10 juli 2006 betreffende de analyse van de dreiging
LTF	*Local task force*
M.B.	Ministerieel besluit
NRBC-wapens	Nucleaire, radiologische, chemische en biologische wapens
NSA	*National Security Agency*
NTF	Nationale Task Force
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open sources intelligence*
OVG	*Operation Vigilant Guardian*
PNR	*Passenger Name Record*
POC	*Point of contact*
POC	Parlementaire onderzoekscommissie
Privacycommissie	Commissie voor de bescherming van de persoonlijke levenssfeer
RFI	*Request for information*

SIGINT	*Signals intelligence*
SLA	*Service Level Agreement*
SOCMINT	*Social media intelligence*
Sv.	Wetboek van Strafvordering
Sw.	Strafwetboek
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
VWEU	Verdrag betreffende de werking van de Europese Unie
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.C&VM	Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
WEP	Wetenschappelijk en economisch potentieel
W.OCAD	Wet van 10 juli 2006 betreffende de analyse van de dreiging
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

De terreuraanslagen die voorbije jaren Europa teisterden hebben een grote impact. Het is dan ook niet verwonderlijk dat het thema 'veiligheid' een prioritaire bezorgdheid is geworden. Radicalisme en terrorisme zijn een dagelijkse realiteit geworden. Dat geldt evenzeer voor spionage en buitenlandse politieke inmenging. Ze kunnen leiden tot een ontwrichting van onze maatschappij en moeten dus bestreden worden. Immers, in veiligheid kunnen leven is een fundamenteel mensenrecht. En de overheid heeft de plicht die veiligheid te waarborgen.

De vele, nieuwe regelgevende initiatieven die ter zake werden genomen, werken diep in op het precaire evenwicht tussen enerzijds de rechten en vrijheden van de burgers en anderzijds de (tijdelijke) beperking daarvan om redenen van veiligheid.

Ook het Vast Comité I wordt met de zoektocht naar dit evenwicht geconfronteerd. Het Comité werd – net als andere dotatiegerechtigde instellingen[1] – opgericht om onafhankelijk én onpartijdig zijn controle-opdrachten te vervullen, onder meer om de burger te garanderen dat de hem bij (Grond)wet toegewezen rechten, gewaarborgd zijn en blijven. In de verhouding binnen de *trias politica* van een democratische rechtstaat is het van kapitaal belang dat de zogenaamde '*checks and balances*' op een correcte en efficiënte manier kunnen worden uitgevoerd. Daartoe behoort ongetwijfeld een Parlement dat, onder meer via het Vast Comité I, zijn toezichtstaak ook effectief kan uitoefenen. De kwaliteit van het werk dat deze dotatiegerechtigde instellingen kunnen 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.

Echter, in een veranderende samenleving waarin veiligheidsrisico's én middelen-beperkingen in stijgende lijn samengaan, wordt de opdracht om de fundamentele rechten van elke burger te vrijwaren, steeds moeilijker. Daarenboven heeft de uitvoerende en wetgevende macht de laatste jaren steeds

1 Het betreft het Vast Comité van Toezicht op de politiediensten, de Commissie voor de bescherming van de persoonlijke levenssfeer, het Controleorgaan voor de politionele informatie, de Federale Ombudsman, de Hoge Raad voor de Justitie, de BIM-Commissie en de Verenigde benoemingscommissies voor het notariaat. Deze instellingen brachten in 2017 gezamenlijk de Voorzitter van de Kamer van Volksvertegenwoordigers op de hoogte van de gevolgen van de budgettaire beperkingen.

meer (controle)opdrachten toegewezen aan het Vast Comité I. Voor deze nieuwe opdrachten werd evenwel niet in bijkomende middelen voorzien.[2]

Dotatiegerechtigde instellingen moeten omgaan met dit nijpend gebrek aan middelen. Dit geldt ook voor het Vast Comité I. Het laat zich raden dat enerzijds meer besparingen en anderzijds meer bevoegdheden een effect zullen hebben op de kwaliteit van de werking van het Vast Comité I. Het Comité is ervan overtuigd dat een debat over de schaarse middelen moet gevoerd worden. Echter, een dergelijk debat dient niet alleen te gebeuren in het kader van de toepassing van een aantal budgettaire normen, maar evenzeer in het kader van de broodnodige evenwichten die moeten kunnen spelen binnen een democratische rechtstaat.

Guy Rapaille,
Voorzitter van het Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

26 september 2017

2 Het Comité bracht 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 Vast Comité I moeten worden gecontroleerd.

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 OCAD en – in beperkte mate – van zijn ondersteunende diensten. De aanbevelingen die het Comité in 2016 formuleerde, zijn opgenomen in het laatste hoofdstuk van dit activiteitenverslag.

Traditiegetrouw worden in het eerste hoofdstuk 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.

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.[3]

Het Vast Comité I had zich voorgenomen 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*'.[4] Dit diende te gebeuren onder de vorm van boordtabellen.

Het Comité startte dit project in 2016 op. Echter, andere prioriteiten – niet het minst de opdrachten in het kader van de parlementaire onderzoekscommissies naar de aanslagen in Brussel en de totstandkoming van de verruimde minnelijke schikking in strafzaken – haalden de *timing* door mekaar zodat deze opdracht

---

3 VAST COMITÉ I, *Activiteitenverslag 2006*, 1-21 ('Hoofdstuk I. De eerdere aanbevelingen van het Vast Comité I en de Begeleidingscommissies').

4 *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.

niet kon worden gefinaliseerd. Wel werden halfweg 2016 op verzoek van de Voorzitter van de parlementaire onderzoekscommissie de toezichtonderzoeken van het Vast Comité I aangaande terrorisme en radicalisme en de gevolgen die hieraan werden gegeven, gezonden. Hierop wordt in Hoofdstuk V teruggekomen.

In de loop van 2017 werd de opdracht van de Begeleidingscommissie door het Vast Comité I hernomen en verfijnd: er zal worden bestudeerd welke aanbevelingen voor deze periode reeds werden gerealiseerd en de nog niet-gerealiseerde aanbevelingen zullen worden afgetoetst aan hun actualiteitswaarde en, indien nuttig en noodzakelijk, worden geherformuleerd. De rapportage is voorzien eind 2017.

HOOFDSTUK II
DE TOEZICHTONDERZOEKEN

In 2016 finaliseerde het Vast Comité I veertien toezichtonderzoeken, waarvan drie samen met het Vast Comité P (II.1 tot II.14). Verder opende het Vast Comité I in 2016 drie nieuwe toezichtonderzoeken, waarvan één gemeenschappelijk met het Vast Comité P. Dit laatste toezichtonderzoek werd geïnitieerd op verzoek van de Begeleidingscommissie; de twee andere onderzoeken werden ambtshalve opgestart. Eén van deze onderzoeken – met name dit naar de aanslagen in Zaventem en Maalbeek (II.4) – werd nog in 2016 afgerond. Een korte omschrijving van de twee andere opgestarte onderzoeken volgt in II.15.

In totaal ontving het Comité in 2016 29 klachten of aangiften. Er werd sinds dit jaar een aanvang genomen met een versoepeling, deformalisering en standaardisering van het werkproces 'klachten en aangiften'.[5] Na verificatie van een aantal objectieve gegevens wees het Comité alle 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 (het Vast Comité P, de Federale Politie, de procureur des Konings). Geen van de klachten uit 2016 gaf aanleiding tot het openen van een toezichtonderzoek, één klacht werd gevoegd bij een lopend informatiedossier.

II.1. DE PROBLEMATIEK VAN DE *FOREIGN TERRORIST FIGHTERS*

Sinds 2013 oefende het Syrische strijdtoneel een grote aantrekkingskracht uit op de zogenaamde *foreign (terrorist) fighters*[6] vanuit de hele wereld. Feit was dat daarbij – verhoudingsgewijs – veel strijders uit België kwamen.

---

5 In eerste instantie wordt de ontvankelijkheid/gegrondheid 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).

6 Het Comité sprak eerder over 'Syriëgangers'; personen die vertrokken naar of terugkeerden (*returnees*) uit Syrië of de buurlanden (jihadistische conflictzones) en deelnemen aan de gewapende strijd aan de zijde van terroristische groeperingen, ook *foreign fighters* genoemd. De Omzendbrief van de ministers van Binnenlandse Zaken en Justitie van 21 augustus 2015 en de

Vandaar dat het Vast Comité I in oktober 2014 besloot een toezichtonderzoek te openen naar 'de informatiepositie van de twee inlichtingendiensten (ADIV en VSSE) over de rekrutering, de zending, het verblijf en de terugkeer in België van jongeren (van Belgische en andere nationaliteiten die in België verblijven) die vertrekken of vertrokken zijn naar Syrië of Irak en aangaande de uitwisseling van inlichtingen met diverse overheden'. Daarbij waren verschillende thema's aan de orde: welke opdracht hadden de Belgische inlichtingendiensten in dit kader en op welke wijze werden zij aangestuurd? Hadden de diensten een kijk op de rekruterings- en vertrekfase? Konden zij zich een beeld vormen van de samenstelling van deze Syriëstrijders? Waren ze op de hoogte van de activiteiten die deze strijders ter plaatste ontwikkelden? Werd de evolutie in het buitenland vertaald naar mogelijke binnenlandse dreigingen, en zoja, welke? En wat met de opvolging en aanpak bij hun terugkeer naar België? Op welke wijze werd er samengewerkt (ADIV, VSSE, OCAD maar ook politie) in deze? Op welke wijze en aan wie werd gerapporteerd? …

Begin 2015 werd een eerste, tussentijds rapport opgesteld.[7] Het eindrapport dateert van februari 2016.

II.1.1. EEN VOORTDURENDE EVOLUTIE

De problematiek en de aanpak van de *foreign terrorist fighters* evolueerde voortdurend. Inlichtingendiensten pasten hun prioriteiten aan en voerden structurele en organisatorische wijzigingen door, het Parlement schetste het algemene kader en de regering preciseerde het regelgevend kader en nam allerhande initiatieven.[8]

De directie van de VSSE stelde reeds in 2014 belangrijke aanpassingen in zijn strategie en organisatie in het vooruitzicht. Ondertussen trof de regering een aantal beslissingen om de dienst te versterken en werden bijkomende middelen toegekend. Binnen de inlichtingenopdracht werd in het Actieplan 2015 'de strijd

---

COL 10/2015 van het College van Procureurs-generaal vulde dit aan tot *foreign 'terrorist' fighters*. Zowel de Omzendbrief als de COL 10/2015 definieerden daarbij zes categorieën, naargelang de status van de persoon: (1) vermoed in jihadistische conflictzone, (2) op weg naar jihadistische conflictzone, (3) in België, na in jihadistische conflictzone te zijn geweest (*returnees*), (4) in België, na op weg naar jihadistische conflictzone te zijn geweest, (5) waarvan er ernstige aanwijzingen bestaan dat hij zal vertrekken naar een jihadistische conflictzone en (6) steun en rekrutering.

7 Hierover: VAST COMITÉ I, *Activiteitenverslag 2015*, 21-25 ('II.4. De opvolging van Syriëstrijders door de twee Belgische inlichtingendiensten: een tussentijds verslag'). Daarin werd de impact van deze problematiek op de werking van de VSSE en de ADIV geduid en werd aangegeven welke middelen beiden in stelling hadden gebracht. Er werd tevens aandacht besteed aan de organisatorische problemen en risico's waarmee beide inlichtingendiensten werden geconfronteerd.

8 In dat licht verwees het Comité onder meer naar de 'Omzendbrief betreffende de informatie-uitwisseling rond en de opvolging van *foreign terrorist fighters* afkomstig uit België'.

tegen jihadistrijders' als één van de drie prioriteiten naar voor geschoven. Ook de structuur van de dienst werd in belangrijke mate gewijzigd.[9]

Van de nota's van de VSSE bleken vooral het Federaal Parket / de Federale Procureur bestemmeling te zijn, gevolgd door de Dienst Vreemdelingenzaken en het OCAD. Met de ADIV werd eerder weinig informatie uitgewisseld.[10] Het aantal strategische nota's was relatief klein. Het thema *foreign fighters* bleek sterk vertegenwoordigd bij de inzet van bijzondere inlichtingenmethoden: zowat 60% van alle door de VSSE ingezette BIM's – in hoofdzaak identificatie, lokalisatie… – tijdens de periode juni-oktober 2015, waren gelieerd aan deze problematiek.

Ook de ADIV rekende het tot zijn taak om vanuit de eigen specialismen (grotendeels gericht op het buitenland) en gelet op de specifieke collectemiddelen, aan verschillende instanties en in diverse overlegplatformen (zoals de *local task forces*) inlichtingen te verschaffen over zowel de bedreigingen ten aanzien van Belgen of Belgische belangen in het buitenland, als over de impact van buitenlandse fenomenen in België. Daartoe zette de ADIV een waaier van collectemiddelen in (HUMINT, SIGINT, IMINT, OSINT en SOCMINT).

Niet alleen de organisatie van de inlichtingendiensten, maar ook de ruimere samenwerkingsstructuren (bijvoorbeeld de nationale en de lokale *task forces*) werden hertekend en dit met het oog op een meer gerichte en gestroomlijnde benadering. Dat impliceerde dat de 'Taskforce foreign fighters' en het 'Platform returnees' vanaf 1 september 2015 ophielden te bestaan. Andere structuren uit het Plan R – de 'Nationale *Task Force* (NTF) en de lokale *task force* (LTF) – werden geactualiseerd. De Nationale Task Force werd uitgebreid met vertegenwoordigers van de gewesten en de gemeenschappen en er werd, onder de NTF, een 'werkgroep FTF' opgericht. De Lokale *task forces* bestaan op arrondissementeel niveau uit een strategische component en op lokaal niveau uit een operationele component.

De concrete aanpak van de FTF hield diverse aspecten in: de vaststelling van de aan- of afwezigheid van een *foreign fighter*, de verificatie en verrijking van de informatie, de individuele dreigingsevaluatie en de (gestandaardiseerde en gepersonaliseerde) opvolging. Voor alle betrokken diensten waren er op dat vlak duidelijk omschreven taken weggelegd. Om de informatie te beheren en te delen, werd beslist 2016 een 'dynamische databank' te installeren.[11]

---

9 Op het ogenblik van het onderzoek was het nog te voorbarig om na te gaan in hoeverre de nieuwe structuur effectief bijdroeg tot een betere informatiepositie ten aanzien van de *foreign terrorist fighters*. Wel werd duidelijk dat deze thematiek een grote invloed bleek te hebben op de werking en de werklast van de VSSE.

10 Ongeveer 60% van de officiële nota's aan de Belgische overheden (*notes aux autorités (NA)*) hadden het Federaal Parket of de Federale Procureur als bestemmeling, 17% de Dienst Vreemdelingenzaken tegenover slechts 6% de militaire inlichtingendienst.

11 Hierover: 'Hoofdstuk VI. De controle van gemeenschappelijke gegevensbanken'.

II.1.2. HET WETTELIJK KADER[12]

II.1.2.1. De Veiligheid van de Staat

Ingevolge de artikelen 7, 1° en 8, 1° b) en c) W.I&V, die betrekking hebben op extremistische en terroristische dreigingen, is de VSSE bevoegd om inlichtingen te verzamelen over eenieder die de intentie had om naar de jihadistische conflictzone in Syrië en Irak te vertrekken, zich ter plaatse bevond en terugkeerde. Personen die deelnamen aan deze strijd vormden een mogelijk of reëel gevaar voor de in- en externe veiligheid van het land.

De VSSE kon in deze al haar bevoegdheden aanwenden zowel in het kader van extremisme als in het kader van terrorisme (gewone, specifieke en uitzonderlijke methoden). Strikt genomen waren de uitzonderlijke methoden niet mogelijk in de strijd tegen een louter extremistische dreiging. Maar deze vaststelling moest worden genuanceerd in die zin dat de methoden wél mochten aangewend worden ter bestrijding van radicaliseringsprocessen. Daar waar de gewone inlichtingenmethoden in theorie ook mochten ingezet worden in het buitenland, gold dat niet voor de specifieke en uitzonderlijke methoden waarvan de toepassing beperkt moest blijven tot het Belgisch grondgebied (art. 18/1, 2° W.I&V).[13]

Of de VSSE gecollecteerde informatie mocht of moest doorgeven aan derden, verschilde naargelang de betrokken dienst en de aard van de informatie. Artikel 19 W.I&V laat de VSSE toe alle informatie en inlichtingen door te geven aan politiediensten en gerechtelijke overheden indien deze gegevens dienstig zijn voor hun opdrachten. Informatie die wees op een mogelijk misdrijf diende dan weer op basis van artikel 29 Sv. of artikel 19/1 W.I&V – en in dit laatste geval via de BIM-Commissie – aan de gerechtelijke overheden te worden overgezonden. Wat betreft het doorgeven van informatie aan buitenlandse diensten, wees het Vast Comité I er al meermaals op dat het wettelijk kader niet toereikend was, zeker wanneer het de transmissie van persoonsgegevens betrof.[14]

De artikelen 9, 11 § 3 en 20 W.I&V ten slotte dragen de inlichtingendiensten op om onderling maar ook bijvoorbeeld met andere administratieve overheden, politiediensten, gerechtelijke overheden (bijvoorbeeld onder de vorm van technische bijstand) en met buitenlandse inlichtingendiensten zo doeltreffend mogelijk samen te werken. Wat 'technische bijstand' aan het gerecht betrof, stelde het Comité reeds meermaals uitdrukkelijk dat een strikte lezing van deze bepaling de

---

12 Diverse aspecten werden na afloop van het toezichtonderzoek gewijzigd door de inwerkingtreding van 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* 28 april 2017. Hierdoor kwamen een aantal van onderstaande vaststellingen te vervallen.

13 Beide restricties werden weggewerkt met de Wet van 30 maart 2017 (*supra*).

14 Hieraan werd gedeeltelijk verholpen met een Richtlijn van de ministers van Justitie en Defensie 'aangaande de relaties van de Belgische inlichtingendiensten met buitenlandse inlichtingendiensten' d.d. 26 september 2016.

VSSE (en de ADIV) niet toeliet inlichtingenbevoegdheden te gebruiken voor gerechtelijke doeleinden.[15] Het Comité kon vaststellen dat de VSSE in de Syriëproblematiek steeds frequenter als expert op diverse vlakken technische bijstand verleende aan het gerecht. Het Comité kon niet vaststellen dat de wettelijke voorschriften daarbij niet werden gerespecteerd.

II.1.2.2. De Algemene Dienst Inlichting en Veiligheid

Wat de ADIV betreft, bood de Wet van 30 november 1998 drie aanknopingspunten voor het verzamelen en verwerken van gegevens inzake *foreign terrorist fighters*.[16] Vooreerst was er de '*vervulling van de opdrachten van de strijdkrachten*'; dit is '*elke uiting van het voornemen om de paraatstelling, de mobilisatie en de aanwending van de Belgische Krijgsmacht, van de geallieerde strijdkrachten of van intergeallieerde defensieorganisaties te neutraliseren, te belemmeren, te saboteren, in het gedrang te brengen of te verhinderen bij opdrachten, acties of operaties in nationaal verband, in het kader van een bondgenootschap of een internationaal of supranationaal samenwerkings-verband*'(art. 11 § 2, 3° W.I&V). De vrijwaring van de '*vervulling van de opdrachten van de strijdkrachten*' laat toe om elke '*activiteit*' (art. 11 § 1, 1° W.I&V) of beter '*elke uiting van het voornemen*' (art. 11 § 2, 3° W.I&V) op te volgen die dit belang in het gedrang kan brengen. In tegenstelling tot de VSSE, dient er dus niet noodzakelijk sprake te zijn van een dreiging (zoals extremisme of terrorisme).[17] De extremistische en terroristische activiteiten van personen die zich in het buitenland bevonden (*foreign fighters*) maar ook in het binnenland (bijvoorbeeld extremisten in het leger) vormden de basis voor de ADIV om zijn inlichtingenwerk te verrichten. Er diende wel benadrukt dat de ADIV – anders dan de VSSE – niet bevoegd was om fenomenen als 'extremisme' en 'terrorisme' op zich op te volgen. In die zin oordeelde het Vast Comité I reeds eerder dat '*de opvolging van het radicaal islamisme tot de bevoegdheden van de ADIV behoort in de mate waarin de militaire veiligheid in België en in het buitenland in brede zin in het gedrang is.*'[18] Een tweede aanknopingspunt was de veiligheid van Belgische onderdanen in het buitenland. Hierbij moest de ADIV aandacht hebben voor '*elke uiting van het voornemen om het leven of de lichamelijke integriteit van Belgen in het buitenland en van hun familieleden collectief te schaden door verwoesting, afslachting of plundering.*' Het toezichtonderzoek heeft ech-

15 Indien er in het kader van een gerechtelijk onderzoek bepaalde opsporingshandelingen dienen gesteld te worden, mag daarvoor geen beroep worden gedaan op bijzondere inlichtingenmethoden, maar dienen de geëigende gerechtelijke onderzoeksmethoden (zoals bijv. bijzondere opsporingsmethoden) te worden gehanteerd.

16 Ook de omschrijving van de bevoegdheden van de ADIV werd grondig gewijzigd bij Wet van 30 maart 2017 (*supra*).

17 Voor het eerste te verdedigen belang van de militaire inlichtingendienst geldt wél dat er een bepaalde dreiging moet aanwezig zijn vooraleer de dienst bevoegd is: er moet een '*middel van militaire aard*' worden ingezet (art. 11 § 2 1° W.I&V).

18 VAST COMITÉ I, *Activiteitenverslag 2007*, 30.

ter aangetoond dat de ADIV analyses opstelde die ruimer gingen dan de '*militaire veiligheid*' of de '*bescherming van Belgen in het buitenland*'. Een derde aanknopingspunt was de '*bescherming en het voortbestaan van de bevolking*' dat, gegeven de vele (pogingen tot) aanslagen, duidelijk in het gedrang werd gebracht met '*middelen van militaire aard*'.

De ADIV kon daarbij een beroep doen op de mogelijkheid om communicaties te intercepteren die verzonden waren vanuit het buitenland (art. 259*bis* Sw.).[19] Dergelijke intercepties waren mogelijk in het kader van de militaire operatie tegen IS (bijvoorbeeld door de aanwezigheid F16's), omwille van de bescherming van Belgen in het buitenland (vnl. in de betrokken regio) en van de Belgische bevolking in zijn geheel. De SIGINT-activiteiten konden in het kader van de Syriëproblematiek niet voor andere redenen worden uitgevoerd.

De inzet van gewone inlichtingenmethoden was toegelaten – ook in het buitenland – in de mate uiteraard waarin de collecte aan te knopen was bij een dreiging die door de ADIV mocht opgevolgd worden. Uiteraard kon de ADIV in het kader van de Syriëproblematiek specifieke of uitzonderlijke inlichtingenmethoden aanwenden indien er een dreiging was tegen een van de in de wet opgesomde te verdedigen belangen. Alleen diende de inzet van dergelijke methoden beperkt te blijven tot het Belgische grondgebied (art. 18/1, 2° W.I&V).[20]

Net zoals de VSSE, moest de ADIV zo doeltreffend mogelijk samenwerken met andere overheden, zonder dat ze daarbij methoden mocht aanwenden buiten zijn eigen bevoegdheidsdomein en dit louter ter ondersteuning van de missie van een andere dienst.

II.1.3. BEOORDELING VAN DE INFORMATIEPOSITIE VAN DE INLICHTINGENDIENSTEN

Met 'informatiepositie' wordt bedoeld het geheel van inlichtingen waarover een inlichtingendienst met betrekking tot een bepaald onderwerp, persoon, gebeurtenis … beschikt. Wat de Syriëproblematiek betreft, meldde de VSSE bij aanvang van het toezichtonderzoek in oktober 2014 te beschikken over een relatief goede informatiepositie. Toch werd onderlijnd dat de dienst bij ongeveer de helft van de 'Belgische' individuen (personen verblijvend in ons land, ongeacht de nationaliteit) geen zicht had op hun activiteiten in Syrië en Irak. De ADIV op zijn beurt stelde toen dat zijn inlichtingenpositie ontoereikend was om zijn ambitieniveau in te vullen. De ADIV leverde zijn bijdrage binnen het dossier Syrië, maar deze bijdrage moest duidelijk versterkt worden door een meer professionele ondersteu-

19 Gewijzigd door de inwerkingtreding van 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* 28 april 2017.

20 Gewijzigd met de Wet van 30 maart 2017 (*supra*).

ning van de analysecapaciteit en door gebruik te maken van nieuwe collectetechnieken. De dienst wees daarbij naar een aantal beperkingen.

Over de manier waarop de kwalitatieve beoordeling van de eindproducten en het beoordelen van de informatiepositie van een inlichtingendienst moet gebeuren, was weinig (objectiveerbaar) materiaal voorhanden. Het Comité evalueerde daarom de inlichtingenpositie niet *as such*, maar wel de inlichtingenprocessen die tot die positie hadden geleid. Deze werden getoetst aan een aantal formele elementen (hierna 'meetpunten') die op zich een procedurele garantie boden dat de informatiepositie op een kwaliteitsvolle manier tot stand kwam.[21] Deze benaderingswijze was tegelijkertijd ook een vorm van risicoanalyse: indien bepaalde procedures/werkprocessen niet gevolgd werden, kon dat er op wijzen dat de inlichtingenpositie op een wankele basis steunde.

II.1.3.1. Gegevensverzameling en bronnen

Het eerste meetpunt behelsde de gegevensverzameling en de bronnen. Wat de VSSE alsook de ADIV betrof, was het Comité de mening toegedaan dat er zich op dit vlak geen specifieke risico's stelden. Beide diensten deden voor wat betreft hun collectewerkzaamheden inzake FTF's beroep op diverse disciplines, methoden en bronnen. Bij de VSSE bleken vooral HUMINT en de BIM's daarbij bijzondere aandacht weg te dragen. De gegevens die *in fine* tot inlichtingen werden verwerkt waren – in de mate van het mogelijke en gegeven de omstandigheden – vrij compleet en precies; zij trachtten een antwoord te formuleren op de wie-, wat-, waarom-, wanneer- en waarvraag. Ook werd de informatie weergegeven zoals ze door of in de bron zelf was verwoord of naar voor kwam; ze was met andere woorden 'objectief'.[22] De wijze waarop de gegevens over de *foreign terrorist fighters* werd gecollecteerd, gebeurde dan ook relatief goed. Minstens wat procedures betrof, kon gesteld worden dat beide diensten maatregelen namen om hun informatiepositie zo goed mogelijk uit te bouwen.

II.1.3.2. Het data- en kennisbeheer

Een tweede meetpunt betrof de manier waarop de gegevens werden opgeslagen, geordend en beheerd (het data- en kennisbeheer).

Het databeheerssysteem bij de VSSE bood een solide basis voor het inlichtingenwerk, maar kon weliswaar verbeterd worden. Zo was er een gebrek aan standaardisatie en werd er redundantie vastgesteld.

---

21 Het Comité baseerde zich op de methodologie van DE VALK en koos ervoor om een uitgebreide steekproef uit te voeren. Zie: G.G. DE VALK, *Dutch Intelligence. Towards a Qualitative Framework for Ananlysis. With Cases Studies on the Shipping Research Bureau and the National Security Service (BND)*, Rijksuniversiteit Groningen, 2005.

22 Het Comité stelde echter vast dat de evaluatie van de bronnen bij de ADIV niet altijd systematisch gebeurde en er over de bron niet steeds voldoende geweten was.

Bij de ADIV vormde het databeheer een groot risico. De manier waarop de informatie bij de ADIV werd opgeslagen en beheerd, was eerder problematisch. Het opzoeken van informatie was niet alleen tijdrovend, maar tevens was er geen garantie dat de juiste en alle beschikbare informatie werd teruggevonden. Als het ging om verbanden te leggen (*connecting the dots*), liep de ADIV het risico dat bepaalde gegevens niet of onvoldoende snel naar boven kwamen, hetzij omdat de zoekmotor ze niet vond – bijvoorbeeld door de problematiek van de tussen de verschillende divisies afgescheiden *file-folders* – of omdat ze eenvoudigweg niet werden geüploaded (onvolkomen *input* in de databank). In het kader van de beoordeling van de wijze waarop de informatiepositie van de ADIV werd opgebouwd, was dit een problematiek die door de dienst al vele jaren werd meegesleept. Dit legde een belangrijke hypotheek op de kwaliteit van de informatiepositie.

II.1.3.3. Analyseprocessen

De wijze waarop de inkomende informatie geanalyseerd wordt om tot 'inlichtingen' te komen (de analyseprocessen) vormde een derde meetpunt. Het Comité onderzocht hoe de analysedocumenten over de Syriëproblematiek waren opgesteld en welke de methodologische onderbouw was. Het gebruiken van goed onderbouwde methoden is immers cruciaal om de kwaliteit van het eindproduct te garanderen.

Wat de VSSE betrof, moest worden vastgesteld dat de analysediensten weliswaar over een bepaalde *tool-box* beschikten, maar dat deze methoden niet op systematische wijze werden gebruikt. Dit werd, aldus de dienst, gecompenseerd door het feit dat een analist nooit alleen voor een probleem staat maar dat ook collega's en chefs erop toezagen dat er een goed product tot stand kwam.

Bij de ADIV stond de dienst CI/Homeland verder op het vlak van het gebruik van instrumenten en analysemethoden dan de Divisie I. Deze laatste haalde dezelfde argumenten aan als de VSSE, met name dat de geleverde kwaliteit niet alleen afhankelijk is van het gebruik van formele methoden (die soms tijdrovend en/of te theoretisch zijn), maar dat de kwaliteit ook wordt gewaarborgd door de wisselwerking tussen verschillende analisten en hun hiërarchie..

Voor zowel de VSSE als de ADIV gold dat er argumenten pro en contra te vinden zijn om het al dan niet rigoureus gebruik van methoden te bepleiten. Van belang is dat men hiermee bewust omgaat (risico-inschatting).

II.1.3.4. Gebruikersbehoefte en feedback

Een vierde meetpunt was de vraag of het product inspeelde op de behoefte van de gebruiker (*fit for use*) en de *feedback* aan de orde. Het Comité stelde daarbij een aantal lacunes vast die een negatieve invloed hadden op de inlichtingenprocessen, en dus mogelijk op de daaruit voortvloeiende producten. Het weze vermeld dat

deze lacunes niet noodzakelijk volledig aan de diensten zelf toe te schrijven waren.

Een eerste probleem betrof de manier waarop de klanten hun wensen en behoeften kenbaar maakten (of soms eerder niet kenbaar maakten) en *feedback* gaven. Het Comité stelde dat wanneer de klanten weinig of geen aanduidingen gaven omtrent wat zij nodig hebben of de *feedback* ontbrak, de diensten soms moeilijker in staat waren hun producten daar op af te stemmen.

Wat de vormelijke aspecten van de informatieverstrekking betrof, merkte het Comité op dat de diensten er wel degelijk aandacht aan besteedden om hun producten goed voor te stellen en duidelijke conclusies naar voor schoven.

In het algemeen werd getracht de nota's zo op te stellen dat de klanten ze nuttig konden gebruiken. Bij de ADIV, althans de Divisie I, bestond zelfs een formele richtlijn die bepaalde hoe een document moest worden opgesteld. Dit bood een bepaalde kwaliteitsgarantie, minstens wat de vorm betrof. Ook andere elementen, zoals de *Service Level Agreements* (SLA's), de distributielijst en het bestaan van de functie van *production support* vormden na te volgen voorbeelden.

II.1.3.5. Het voorspellende karakter van het inlichtingenwerk

Het vijfde meetpunt betrof het voorspellende karakter van het inlichtingenwerk. Het Vast Comité I stelde vast dat beide inlichtingendiensten vooral beschrijvende en verklarende inlichtingen verschaften, en minder voorspellende. De *Intelligence Outlook Bulletins* (IOB) van de Divisie I van de ADIV vormde hierop een uitzondering. Voor zover de bevoegde (gerechtelijke, politionele, politieke) overheden van de inlichtingendiensten mogelijke scenario's en onderbouwde hypotheses zouden willen aangereikt krijgen om op die manier bepaalde acties in gang te zetten, dan waren de door de diensten verschafte inlichtingen daarvoor doorgaans minder geschikt.

II.1.3.6. Design of planning van de inlichtingeninspanning

Het design of de planning van de globale inlichtingeninspanning in de Syriëproblematiek betrof een zesde meetpunt. Dit heeft tot doel zowel de collecte- als de analyse-inspanningen en methoden te beschrijven en er wordt getracht tussen beide verbanden te leggen.

Het vormde bij beide inlichtingendiensten een belangrijk werkpunt. Bij de VSSE en de ADIV waren wel een aantal bouwstenen aanwezig, maar deze dienden beter te worden geïntegreerd en uitgewerkt dan op het ogenblik van het toezichtonderzoek het geval was. De individuele inlichtingenprocessen werden door dit gebrek weliswaar niet fundamenteel verstoord, maar de globale resultaten van de inlichtingeninspanning (naar efficiëntie en coördinatie) zouden worden verbeterd indien hieraan meer aandacht werd besteed. Wat de eigenlijke collecte-aanpak betrof, en de breedte ervan, sprak het voor zich dat bepaalde gegevens de

diensten konden ontgaan. Het Vast Comité I was van mening dat de collecteaanpak van beide diensten voldoende gediversifieerd en breed was en de nodige garanties bood opdat de informatiepositie op een goede manier tot stand kwam. Dit sloot opnieuw aan bij het eerste meetpunt.

II.1.3.7. Besluitend

De inlichtingendiensten sloegen erin bij het uitbouwen van hun informatiepositie aangaande de Syriëproblematiek diverse risico's die aan de meetpunten verbonden zijn, te beperken. Toch manifesteerden zich een aantal risico's die voor het Comité dienden te worden aangepakt; daarbij was de problematiek van het databeheer, zeker voor de ADIV, prioritair.

II.1.4. INLICHTINGENDIENSTEN EN DE *LOCAL TASK FORCES*

Inzake de samenstelling, de organisatie en de invulling die aan de verschillende lokale *task forces* (LTF) werd gegeven, werden onderling belangrijke verschillen vastgesteld. Op zich hoefde dit niet geen probleem te zijn, aangezien de plaatselijke situaties konden verschillen. Niettemin bleek dat hoe groter de LTF, des te meer dit woog op de efficiëntie.

Er kon worden vastgesteld dat de verschillende deelnemers aan de LTF (politie, inlichtingendiensten, parket…) elk met verschillende verwachtingen en taken naar de vergaderingen kwamen ('inlichtingenwerk' versus 'politiewerk'). Voor de inlichtingendiensten golden daarbij ook een aantal beperkingen (bijvoorbeeld inzake classificatie, *need to know*, regel van de derde dienst) die de manier waarop zij aan de LTF meewerkten, beïnvloedden.

Vanuit het standpunt van de inlichtingendienst vormde de kwestie van de veiligheidsmachtigingen een belangrijke struikelblok: het betrof een rem op de informatie-uitwisseling, terwijl die door de andere actoren niet steeds ten volle in rekening werd gebracht of geapprecieerd. Deze problematiek vond (deels) zijn oplossing in de Omzendbrief FTF nu beslist werd dat alle deelnemers aan de LTF's dienen te beschikken over een veiligheidsmachtiging niveau GEHEIM. Het Vast Comité I meende dat dit een stap vooruit was. Dit impliceerde weliswaar dat voortaan alle deelnemers over bepaalde geclassificeerde informatie zullen beschikken die ze niet zomaar kunnen delen met personen of overheden die geen drager zijn van een veiligheidsmachtiging.

Ook in dit verband meende het Comité dat er moest worden nagedacht over de vraag welke informatie precies moest worden geclassificeerd. In dat kader pleitte de administrateur-generaal voor meer openheid vanuit de VSSE.

Er rezen verder twijfels en vragen over wat van de medewerkers van zowel de VSSE als de ADIV in de *local task forces* verwacht werd. De 'oorspronkelijke'

Omzendbrief FF bleef daarbij teveel aan de oppervlakte: de opdrachten werden weliswaar beschreven, maar er werden geen taken 'toegekend'. De deelnemers bleven met een aantal vragen zitten: werden de LTF's opgericht met het oog op de uitwisseling van informatie – en zo ja, welke soort van informatie – of betrof het eerder organen om aan netwerking en sensibilisering te doen? En welke was dan – afhankelijk van de doelstelling – de meest aangewezen samenstelling? Zo werd bijvoorbeeld gesuggereerd om (soms) ook een analist naar de LTF te sturen. Op die manier zou de VSSE naast louter 'operationele' informatie ook een bredere contextualiserende rol kunnen invullen. Het toezichtonderzoek kon vaststellen dat de leden van de VSSE ter zake sturing vanuit het hoofdbestuur wenselijk achtten. De verwachtingen van het terrein werden niet volledig ingelost.

Ook hier bood de nieuwe Omzendbrief (*supra*) soelaas: de concrete aanpak van de *foreign fighters* werd ingedeeld in diverse deelaspecten (vaststelling van de aan- of afwezigheid van de FTF, verificatie en verrijking van de informatie, de individuele dreigingsanalyse en de gestandaardiseerde en gepersonaliseerde opvolging) met voor eenieder een duidelijk afgelijnd takenpakket.

II.1.5. SAMENWERKING MET DE GERECHTELIJKE AUTORITEITEN

Geen enkele van de ondervraagde diensten stelde vragen bij het wettelijk kader van de samenwerking, dat voldoende leek en aangepast was aan de behoeften van de strijd tegen de *foreign (terrorist) fighters* en de *returnees*. Alle ondervraagde diensten benadrukten de goede samenwerking tussen de inlichtingendiensten, de politie en het Federaal Parket[23] in het kader van de Syrische problematiek. Die samenwerking was verbeterd sinds de komst van de nieuwe directie van de VSSE.

Het Comité stelde echter vast dat de VSSE en de ADIV er een verschillend informatiebeleid ten aanzien van de gerechtelijke overheden op na hielden en dat ook weinig gebruik werd gemaakt van artikel 19/1 W.I&V. In concrete dossiers kon de bescherming van de bronnen van de inlichtingendiensten problematisch blijken, ook al had de tussenkomst van het Federaal Parket het mogelijk gemaakt om moeilijkheden te voorkomen.

Ook de verschillende actoren beoordeelden de rechtstreekse samenwerking tussen de inlichtingendiensten en de politiediensten als positief. Het werd echter wenselijk geacht de rol die elke dienst rekening houdend met de eigen deskundigheid, op operationeel vlak kon vervullen, *in concreto* te omschrijven.

---

[23] Voor de periode van 1 oktober 2014 tot 31 maart 2015 kreeg de VSSE 132 verzoeken om technische bijstand (art. 20 § 2 W.I&V), waarvan de meeste verband hielden met dossiers van internationaal terrorisme. Voor de periode maart-april 2015 ontving de ADIV 60 verzoeken om technische bijstand waarvan 90% in verband met de problematiek van de *foreign fighters* en waaraan de dienst gunstig gevolg gaf.

Een delicaat probleem dat de politiediensten ter sprake brachten, was dat van de (cultuur van) classificatie en de veiligheidsmachtigingen. Hierbij erkenden de politiediensten dat ze intern met verbeteringen moesten verschijnen.

II.2. DE INFORMATIEPOSITIE VAN DE VSSE EN DE MISLUKTE AANSLAG IN DE THALYS

II.2.1. DE FEITEN

Op 21 augustus 2015 was de Thalys tussen Amsterdam en Parijs het doelwit van een terroristische aanval door een individu. Hij kon evenwel snel worden overmeesterd door enkele treinreizigers. De dader werd geïdentificeerd als Ayoub El Khazzani en was afkomstig uit Marokko. Hij zou in Brussel in de Thalys zijn gestapt met wapens die hij in België zou hebben gekocht.[24] Het Vast Comité I opende, in het verlengde van zijn toezichtonderzoek naar de *foreign terrorist fighters* (II.1), een aanvullend onderzoek. Dit onderzoek had alleen betrekking op de VSSE. De ADIV verklaarde immers geen informatie te bezitten met betrekking tot Ayoub El Khazzani voorafgaand aan de feiten.

II.2.2. WAS DE DADER GEKEND BIJ DE VSSE?

Ayoub El Khazzani was sedert 2012 bij de VSSE gekend: zijn naam dook, samen met die van zijn broer Imram, voor het eerst op in een rapport dat de VSSE in juni 2012 opstelde na een vergadering met een buitenlandse partnerdienst. De broers werden in verband gebracht met een vooraanstaand lid van een buitenlandse jihadistische cel. Deze laatste zou naar België zijn gevlucht en de schakel vormen in een groter netwerk dat betrokken was bij het uitsturen van strijders naar Syrië. Hun identiteit werd opgenomen in de database van de VSSE.

In de daaropvolgende maanden werden inlichtingen en foto's uitgewisseld en werd de VSSE gevraagd om informatie te verifiëren, wat de dienst ook deed. Verificaties bij de Dienst Vreemdelingenzaken leverden geen resultaat op. In oktober 2012 nam de VSSE deel aan een vergadering met de partnerdienst in verband met de jihadistische cel en de aanwezigheid van sommige leden ervan op Belgische bodem. De inlichtingendienst kreeg er te horen dat in ons land een gerechtelijk onderzoek was geopend met betrekking tot de bewuste cel. Het

[24] De dader werd door de Parijse procureur officieel in verdenking gesteld voor poging tot moord gelieerd aan terrorisme en wapenbezit. Hij wacht zijn proces af.

Vast Comité I vond geen sporen van communicatie waaruit zou blijken dat de Federale Politie en de VSSE hieromtrent informatie zouden hebben uitgewisseld.[25]

In april 2013 werd El Khazzani op een internationale lijst geplaatst, waarschijnlijk door de partnerdienst, waarna het even stil werd rond de broers.

Op 11 mei 2015 stuurde de correspondent opnieuw een document naar de VSSE met daarin informatie over Ayoub El Khazzani. De partnerdienst liet weten belang te stellen in de betrokkene, zijn contacten met Belgische extremistische kringen en zijn mogelijke rol als verbindingspersoon in het kader van de netwerken die ook via België liepen. In dit document wordt nergens verwezen naar enige aankoop van wapens of een plan om een terroristische aanval te plegen. Evenmin stuurde de partnerdienst een foto door van Ayoub El Khazzani of werd een graad van dringendheid toegevoegd. Twee dagen later werd het document intern doorgestuurd naar de Analysedienst en de centrale dienst van de Buitendiensten. Dezelfde dag nog stuurde de centrale dienst het document door naar de bevoegde provinciepost met de vermelding 'voor onderzoek'.[26] De provinciepost verklaarde een controle in het Rijksregister te hebben verricht en op 30 juni 2015 naar de Lokale Politie te zijn gegaan. Het Comité stelde vast dat de VSSE zelf niet het initiatief nam om bij de politie- of de partnerdienst een foto van de betrokkene te verkrijgen. Er werd geen antwoord verzonden naar de buitenlandse correspondent. Dit is niet ongebruikelijk als de dienst niet over informatie beschikt (de zgn. *silent answer*).

Op 17 augustus 2015 ontving de VSSE van de partnerdienst bijkomende informatie. Deze laatste liet opnieuw weten belang te stellen in Ayoub El Khazzani en vroeg tevens om drie GSM-nummers te identificeren. De informatie werd op 18 augustus 2015 (dit is drie dagen voor de mislukte aanslag) meegedeeld aan de Analysedienst en de Buitendiensten. Op 19 augustus voerde de Analysedienst het verzoek in het informaticasysteem in ter bestemming van de bevoegde provinciepost. Op 22 augustus 2015, d.w.z. na de mislukte aanslag, ging de VSSE over tot de door de partnerdienst gevraagde identificatie. De VSSE stelde een document op met informatie over de ondertussen gearresteerde Ayoub El Khazzani alsook met de identificatie van de drie mobiele telefoonnummers.

---

25 Op te merken viel dat de VSSE geen rechtstreekse toegang had tot de databanken van de politie. De VSSE verklaarde slechts informatie te krijgen wanneer de politie daartoe zelf het initiatief nam of wanneer zij er uitdrukkelijk om vroeg. Krachtens artikel 14 W.I&V mag de VSSE echter eender welk type informatie opvragen bij de politiediensten.

26 Dit was ook de enige maal dat gebruik werd gemaakt van de daartoe voorziene ICT-tool in de databank van de VSSE om een bericht te verzenden. Omdat het onderzoek destijds niets opleverde met betrekking tot El Khazzani, liet de betrokken provinciepost de taak in de databank open zodat ze deze, naar eigen zeggen, later opnieuw zou kunnen opnemen.

II.2.3. DE CONTEXT VAN HET DOSSIER

Om de gebeurtenissen in hun context te plaatsen, onderzocht het Comité hoe de VSSE destijds de aanvragen van buitenlandse correspondenten beheerde.

Documenten die naar de VSSE worden verzonden, passeren in eerste instantie via een uniek ingangspunt. Ten tijde van de aanslag in de Thalys, gold de procedure dat deze documenten vervolgens naar zowel de Analyse- als de Buitendiensten – en dit binnen de grenzen van hun respectieve bevoegdheden – werden gestuurd. Sinds de herstructurering van de VSSE in september 2015 werden wijzigingen aangebracht aan deze procedure. De binnenkomende informatie passeert nog steeds via het unieke ingangspunt, maar wordt daarna doorgestuurd naar de bevoegde afdeling van de Analysedienst. Deze dienst bepaalt of en welke van de Buitendiensten in kennis wordt gesteld en vraagt zo nodig verder onderzoek te voeren.

In augustus 2015[27] ontving de VSSE circa 1200 documenten afkomstig van buitenlandse correspondenten. Een kwart daarvan werd doorgestuurd naar de afdeling die onderzoek voert naar de radicale islam.[28] Iets meer dan 40 van deze documenten bevatte informatieaanvragen die een actie vanwege de VSSE vereisten.[29] Slechts enkele daarvan hadden betrekking op de identificatie van telefoongegevens. Het verzoek met betrekking tot Ayoub El Khazzani was het enige waaraan – evenwel na de aanslag – gevolg werd gegeven.

Wat betreft de verzoeken van buitenlandse correspondenten om telefonieidentificatie (art. 18/7 W.I.&V.) te verrichten, bestudeerde het Vast Comité I ook de cijfers die betrekking hadden op de periode januari-augustus 2015. Hieruit bleek dat de VSSE in deze tijdspanne 130 identificaties uitvoerde op verzoek van een buitenlandse dienst.[30] Bijna tien van deze methoden – gevraagd voor de periode van 1 juli tot 21 augustus 2015 – hadden betrekking op het extremistisch ter-

---

27 De maand waarin de partnerdienst zijn verzoek tot identificatie van telefoonnummers verzond, maar ook de maand van de mislukte aanslag in de Thalys.

28 Het Vast Comité I deed opmerken op dat het aantal tijdens de maand augustus 2015 ontvangen documenten door de afdeling belast met 'radicale islam' niet representatief was voor de gewone stroom aan binnenkomende documenten. Zo ontving de betrokken afdeling ongeveer 850 documenten afkomstig van buitenlandse correspondenten in september 2015 en zowat 1050 in oktober van datzelfde jaar.

29 Er was geen eenvormigheid in de manier waarop de vragen van buitenlandse correspondenten in het ICT-systeem werden ingevoerd. Ze werden afwisselend omschreven als 'verzoeken', '*requests for information*' (RFI), 'vragen' of nog 'vragen naar sporen'. De VSSE verklaarde dat ze slechts beperkte invloed kan uitoefenen op de keuze van titels door haar correspondenten. Dat kan afhankelijk zijn van de taal van de correspondent, de keuzes van gemaakte vertalingen, de standaardprocedures die bij de correspondenten van kracht zijn … Bovendien vermeldden de vragen van de buitenlandse correspondent geen dringendheidsgraad (routine, dringend, *flash*). Deze vaststelling geldt enkel voor de documenten die het Comité in het kader van dit onderzoek raadpleegde. Als gevolg daarvan was het niet eenvoudig om de prioriteit van onderzoeksopdrachten te bepalen.

30 Deze 130 methoden hebben betrekking op alle door de VSSE op te volgen materies. Dit geeft een gemiddelde van 16 identificaties per maand.

rorisme. In die dossiers waar de VSSE overging tot een identificatie, schommelde de termijn tussen de vraag van de buitenlandse dienst en het gevolg dat eraan werd gegeven, tussen 6[31] en 64 dagen. In het specifieke kader van het verzoek om identificatie van de telefoonnummers van Ayoub El Khazzani verliepen drie dagen.[32] Het Comité concludeerde dan ook dat feit dat er geen uitvoering van identificatie binnen de drie dagen was geweest, op zich niet uitzonderlijk was.

Tot slot viel op te merken dat de gevraagde telefonie-identificatie, achteraf gezien, niet doorslaggevend was geweest, aangezien de nummers afkomstig waren van vooraf betaalde en bijgevolg 'anonieme' kaarten. Het daaropvolgende onderzoek van de VSSE naar de nummers in kwestie liet evenwel toe personen te identificeren met wie Ayoub El Khazzani in België contact had gehad.

II.2.4. VASTSTELLINGEN EN BESLUITEN

De VSSE verrichtte haar werkzaamheden op basis van de inlichtingen die ze uit het buitenland kreeg. Deze informatie was niet zeer gedetailleerd. Het Comité diende vast te stellen dat er geen optimale opvolging van het beheer van de vragen van de buitenlandse correspondent was:

- het dossierbeheer was routinematig. Zo heeft de VSSE geen pogingen ondernomen om bijkomende informatie over het dossier te verkrijgen, met als doel het onderzoek te doen vorderen;
- er was een gebrek aan leiding op het niveau van de centrale afdelingen;
- de VSSE noch de buitenlandse correspondent hebben een graad van dringendheid of belang aangegeven voor de verwerking van de informatie in de zaak-El Khazzani. Er werd evenmin melding gemaakt van een precieze dreiging;
- de informatie van mei 2015 werd verwerkt via het daartoe voorziene ICT-systeem, maar de onderzoeksopdrachten, de herinnering van de Analysedienst en de (zelfs negatieve) resultaten werden niet opgenomen in het systeem. Het Vast Comité I was van mening dat de niet-aanwending van het ICT-systeem het beheer van de informatie verzwakte;
- de resultaten van de in mei 2015 uitgevoerde onderzoeksopdrachten, zelfs al waren die negatief, werden door de Buitendiensten niet doorgegeven aan de Analysedienst en er werd geen antwoord gegeven aan de buitenlandse correspondent. De resultaten van voornoemde onderzoeksopdrachten hebben het evenmin mogelijk gemaakt het dossier af te sluiten of nieuwe hypothesen te openen.

---

31 Op te merken valt dat deze vrij korte termijn betrekking heeft op een vraag om identificatie door een partnerdienst en in het kader van een dossier in verband met de cel van Verviers.

32 Bij deze termijn dienen twee dagen te worden bijgeteld als er rekening wordt gehouden met de termijn voor toezending van het document door de verbindingsofficier van de partnerdienst.

Het Vast Comité I heeft geen informatie-uitwisseling vastgesteld tussen de VSSE en de Federale Politie.

De broers El Khazzani stonden op een internationale lijst. Het Vast Comité I betwistte het nut van een dergelijke lijst niet, maar onderstreepte dat er tal van zowel nationale als internationale lijsten bestaan waarvan de relevantie en de actualiteit niet steeds zijn gewaarborgd. De VSSE verleende ook zijn medewerking aan deze lijst, maar verklaarde niet over de middelen te beschikken om elke naam op deze lijst (meer dan 2500) te volgen en te controleren indien ze niet meer aanwijzingen kreeg betreffende de context en de bedreiging die het individu vertegenwoordigde. Volgens de VSSE zouden de inlichtingendiensten een systeem van risicobeheer moeten ontwikkelen dat gekoppeld is aan potentiële jihadi's.[33] Dankzij een dergelijk systeem zou het voor de diensten mogelijk moeten zijn de betrokkenen te rangschikken volgens graad van gevaarlijkheid.

Meer algemeen merkte het Vast Comité I op dat de actiemiddelen van de inlichtingendiensten die de opdracht krijgen opzoekingen te verrichten naar personen die een bedreiging vormen, beperkt zijn. Het gemak waarmee de betrokkenen zich binnen en zelfs buiten Europa konden verplaatsen, allerlei soorten communicatiemiddelen kunnen gebruiken en anoniem in regio's en landen verblijven zonder dat ze werden ontdekt, vertegenwoordigt een grote uitdaging voor de inlichtingen- en veiligheidsdiensten.

II.3. DE INFORMATIEPOSITIE VAN DE TWEE INLICHTINGENDIENSTEN VOOR DE AANSLAGEN IN PARIJS

II.3.1. DE GEBEURTENISSEN KORT SAMENGEVAT

Op 13 november 2015 grijpen in Parijs bijna gelijktijdig meerdere aanslagen plaats. Even na 21 uur zijn er drie explosies in de buurt van het *Stade de France*, waar op dat ogenblik een voetbalwedstrijd wordt gespeeld tussen Frankrijk en Duitsland. In de omgeving van het stadion blazen drie zelfmoordterroristen zichzelf op met een bommengordel. Er valt naast de daders nog één slachtoffer. Amper een kwartier later volgen schietpartijen nabij terrassen van cafés en restaurants in de Parijse binnenstad. Daarbij vallen tientallen doden en gewonden. In de nabijgelegen concertzaal Bataclan ten slotte, worden 90 mensen op brutale wijze gedood. Ook hier komen de drie daders om.

In totaal vallen die avond 130 dodelijke slachtoffers te betreuren alsook meer dan 400 gewonden. De terreurbeweging Islamitische Staat eist de aanslagen op in een officiële mededeling.

[33] Intussen hebben er daarover tussen de inlichtingendiensten besprekingen plaatsgevonden.

Vrijwel onmiddellijk na de bloedige aanslagen opende het Vast Comité I een '*toezichtonderzoek over de informatiepositie van de twee inlichtingendiensten, voorafgaand aan 13 november 2015 's avonds, over de individuen of groepen die de aanslagen te Parijs hebben uitgevoerd of hierbij betrokken waren*'.[34] Er bleek immers snel dat er heel wat linken waren met België: zo waren vijf terroristen afkomstig van of woonden in België, waren de voertuigen die gebruikt werden bij de aanslagen in België gehuurd, waren er Belgische onderduikadressen, werden de bommengordels waarschijnlijk in een appartement in Schaarbeek geassembleerd…

Het Vast Comité I ging vooreerst na wat de VSSE en de ADIV voorafgaand aan de aanslagen wisten over de daders en welke collectemiddelen ze daarbij inzetten. Daarnaast werd onderzocht hoe deze diensten met andere nationale en internationale autoriteiten samenwerkten voor en na de aanslagen in Parijs. Verder werd bestudeerd op welke wijze de betrokken overheden (regering, parket…) op de hoogte werden gebracht van nakende dreigingen zodat deze tijdig de nodige maatregelen konden treffen. Ten slotte ging het Comité na op welke wijze de twee inlichtingendiensten in termen van 'organisatiebeheer' reageerden op de gebeurtenissen en welke structurele problemen en risico's zich aandienden. Vooraf wees het Comité echter op de snel evoluerende juridische context waarin de strijd tegen terrorisme en extremisme verloopt.

II.3.2. DE SNEL EVOLUERENDE JURIDISCHE CONTEXT

Sinds de aanslagen in New York (2001), Madrid (2004) en Londen (2005) beschikken vele Europese landen over een bijzonder uitgebreide waaier aan preventieve – maar vooral repressieve – maatregelen tegen terrorisme. Dit kon de aanslagen in Parijs en later ook Brussel evenwel niet voorkomen. De omvang van het probleem en de specifieke dreiging die ervan uitgaat, vraagt om een gerichte en gestroomlijnde aanpak. De inlichtingendiensten vormen daarbij één schakel in de ketting van de rechtshandhaving in het algemeen en de strijd tegen het radicaal islamisme en de *foreign fighters* en *returnees* in het bijzonder.

---

[34] Het onderzoek werd afgesloten in juli 2016 (Beperkte verspreiding – 47 pagina's). Voordien werden er ten behoeve van de Begeleidingscommissie in de Kamer reeds twee tussentijdse verslagen opgesteld. Het eerste verslag van 24 februari 2016 (Beperkte verspreiding – 41 pagina's) was vooral beschrijvend en kwantitatief van aard. Het tweede verslag van 22 april 2016 (Beperkte verspreiding – 22 pagina's) bevatte twee onderdelen. In een eerste onderdeel werd nagegaan welke de toegevoegde waarde was van de collectemiddelen HUMINT, SOCMINT en SIGINT bij het opbouwen van de informatiepositie en de wijze waarop de informatie werd gedeeld. Een tweede onderdeel had betrekking op een aantal structurele elementen inzake de manier waarop de Belgische inlichtingendiensten de collecte en analyse organiseren en de risico's die daaraan verbonden zijn. De resultaten van beide tussentijdse verslagen werden verwerkt in voorliggende samenvatting.

Zeker na de aanslagen in Parijs werden op diverse beleidsniveaus zeer veel maatregelen genomen. Het Comité stelde zich de vraag of dit voldoende gecoördineerd verliep en of de noodzaak van elke maatregel kon worden aangetoond. Het Comité verwees in dit verband naar de conclusie van een onderzoek naar de effectiviteit van de sinds 2001 in Europa genomen maatregelen tegen terrorisme waarin gesteld werd dat een grondige evaluatie van de maatregelen harder nodig is dan de invoering van wéér nieuwe maatregelen.[35]

II.3.3. DE INFORMATIEPOSITIE VAN DE DIENSTEN EN DE INBRENG VAN DE DIVERSE COLLECTEMIDDELEN

Het Comité stelde voor de belangrijkste personen die rechtstreeks of onrechtstreeks betrokken waren bij de aanslagen[36] een tijdslijn op met daarop de op hen betrekking hebbende informatie die vóór 13 november 2015 beschikbaar was bij de VSSE en de ADIV en dit los van de aard (briefwisseling, analysenota…) en de bron (eigen collecte, buitenlandse dienst, andere Belgische overheid…) van de informatie. Daarna werd de informatiepositie en de totstandkoming ervan kort omschreven aan de hand van volgende vragen: Wanneer kwam elk van hen voor het eerst in beeld? Wat wist men over deze persoon (wie, wat, wanneer, waarom en waar)? Werden er al dan niet BIM-methoden ingezet? Welke informatie werd uitgewisseld met buitenlandse diensten en hoe was de wisselwerking met de Belgische diensten en autoriteiten? Welke eventuele relaties legden de inlichtingendiensten tussen de betrokken personen?

II.3.3.1. De informatiepositie

De VSSE had de meeste protagonisten – sommigen relatief lang, anderen eerder kort – in het vizier en kende ze hetzij als criminelen, hetzij als geradicaliseerde personen. Enkel van Abdelhamid Abaaoud, die als een van de leiders van het moordcommando wordt beschouwd, was duidelijk dat hij erg gevaarlijk was. Van geen van de anderen waren er indicaties voorhanden dat ze tot actie zouden overgaan. Evenmin kon worden afgeleid dat ze een operationele cel vormden.

De ADIV beschikte vóór de aanslagen alleen over informatie met betrekking tot Abaaoud. Hij was in 2013 in beeld gekomen in de marge van een ander onder-

35 B. HAYES en C. JONES, *Report on how the EU assesses the impact, legitimacy and effectiveness of its counter-terrorism laws*, Statewatch, SECILE-project, 2015, 59 p.

36 Aanvankelijk ging het om tien personen die ten tijde van het onderzoek van het Comité als (mede)dader werden aangeduid door diverse bronnen. In een latere fase van het toezichtonderzoek werd dit getal eerst uitgebreid naar veertien personen en in het laatste deel van het onderzoek teruggebracht tot acht personen.

zoek.[37] Wanneer Abaaoud begin 2014 IS vervoegt, probeert de ADIV meer over zijn activiteiten in het buitenland te vernemen. Vanaf het oprollen van de cel in Verviers in januari 2015, vormde hij een prioriteit voor de ADIV. De dienst richtte meerdere *Request's for Information* (RFI) tot zijn correspondenten. Dit leverde echter geen nuttige inlichtingen op. In november 2015 vernam de ADIV via zijn eigen collectemiddelen dat IS de vaste wil had om in Europa aanslagen te plegen. De dienst had echter geen concrete informatie over datum of plaats. De ADIV oordeelde in dit geval dat deze informatie zeer belangrijk was en verspreidde ze *quasi* onmiddellijk naar de gerechtelijke autoriteiten, zijn buitenlandse correspondenten en de Nationale Veiligheidsraad.

II.3.3.2. De inzet van de diverse collectemiddelen

Wat betreft de door de VSSE en de ADIV ingezette collectemiddelen (HUMINT, BIM's, SIGINT en SOCMINT) kan in dit publieke verslag melding worden gemaakt van de hierna volgende vaststellingen.

Wat betreft *human intelligence* (HUMINT):

- de VSSE beschikte met betrekking tot sommige van de onderzochte personen over fragmentaire informatie afkomstig uit menselijke bronnen. Ook al werden sommige van die bronnen omschreven als 'van hoge toegevoegde waarde', toch bracht geen enkele ervan concrete informatie bij in verband met de nakende aanslagen;
- sommige van deze bronnen werden samen met een buitenlandse partnerdienst beheerd;
- in het kader van de strijd tegen terrorisme zijn goedgeplaatste menselijke bronnen schaars. Het was dan ook zo dat een heel beperkt aantal menselijke '*high value*' bronnen aan de basis lagen van het gros van de informatie waarover de VSSE beschikte;
- de VSSE stelde dat personeelsgebrek tot beperkingen voor de bronnenwerking leidde in de zin dat te weinig tijd kon besteed worden aan het onderhouden van de contacten en het zoeken naar nieuwe bronnen;
- de ADIV rekruteerde menselijke bronnen in het kader van geradicaliseerde islamistische milieus in België en in het buitenland.[38] Als gevolg daarvan kan deze dienst vaker samenwerken en meer informatie uitwisselen met bepaalde buitenlandse partners;
- voor het beheer van deze bronnen – maar ook voor het opsporen en analyseren van informatie via OSINT en SOCMINT (*infra*) – is talenkennis en kennis

[37] Het betreft de zaak rond Zerkani die in 2016 werd veroordeeld voor terroristische misdrijven (zie ook II.3.4.4).

[38] De ADIV beschikte voor de aanslagen van 13 november 2015 over geen HUMINT aangaande voormelde protagonisten, tenzij over Abaaoud. De HUMINT-informatie over betrokkene was niet recent, weinig volumineus noch specifiek.

van allochtone milieus essentieel. De VSSE en de ADIV zouden daarom de diversiteit binnen hun diensten moeten bevorderen;
– er dringt zich een betere coördinatie op tussen de verschillende onderdelen die binnen de ADIV de menselijke bronnen beheren.

Wat betreft social media intelligence (SOCMINT):
– in 2015 werd binnen de VSSE een cel SOCMINT opgericht. Ze had als opdracht het monitoren en opzoeken van de sites, profielen en personen. Maar ze kon ook haar medewerking verlenen aan BIM's en aan de sectie HUMINT;
– de SOCMINT-informatie over de (mede)daders heeft weinig bijgedragen tot de informatiepositie van de VSSE, met uitzondering van de informatie over Abaaoud. Uit de gegevens kon wel worden opgemaakt dat bepaalde personen (sterk) geradicaliseerd waren, zonder dat er aanwijzingen waren voor concrete plannen om aanslagen te plegen;
– het Comité heeft kunnen vaststellen dat het belang van SOCMINT als collecte-instrument alsmaar toenam. SOCMINT is echter arbeidsintensief en moeilijk te beheersen qua volume aan informatie en qua techniciteit;
– het Comité stelde vast dat de capaciteit die zowel de VSSE als de ADIV besteedden aan SOCMINT eerder beperkt was, zeker gelet het feit dat deze diensten niet enkel op het fenomeen van het terrorisme moesten focussen. Om hieraan te verhelpen is een vergaande samenwerking noodzakelijk.

Wat betreft *signals intelligence* (SIGINT)[39]:
– via de sectie SIGINT heeft de ADIV toegang tot informatie die afkomstig is van andere landen die beschikken over meer vergaande SIGINT-capaciteiten. Zij kan op die manier ook voordeel halen uit het delen van internationale bronnen;
– alhoewel de SIGINT-afdeling van de ADIV voornamelijk beschikt over (meta)data die vaak niet gekoppeld zijn aan een geïdentificeerde persoon, beschikte deze afdeling over documenten die konden gelieerd worden aan twee individuen die voorkwamen op de lijst van de door het Comité geselecteerde namen;
– de SIGINT-afdeling beschikt over een unieke capaciteit met betrekking tot buitenlandse telefoonnummers. Nochtans deed de VSSE zelden een beroep op deze afdeling. Het Comité was van oordeel dat er op dit vlak een structurele samenwerking zou moeten worden opgezet.

[39] In deze wordt verwezen naar de bevoegdheid om in het buitenland uitgezonden communicaties te onderscheppen. Alleen de ADIV heeft deze bevoegdheid. Dergelijke intercepties zijn wettelijk mogelijk in het kader van de militaire operatie tegen IS (bijvoorbeeld door de aanwezigheid F16's), omwille van de bescherming van Belgen in het buitenland (vnl. in de betrokken regio) en van de Belgische bevolking in zijn geheel.

Wat betreft de bijzondere inlichtingenmethoden (BIM's):
- het Comité stelde vast dat de VSSE op passende wijze gebruik maakte van BIM's;
- op drie van de acht door het Comité geselecteerde targets werden door de VSSE vóór 13 november 2015 bijzondere inlichtingenmethoden ingezet (op de betrokkene zelf of op zijn omgeving).[40] Deze hebben geen afdoende informatie opgeleverd om de gebeurtenissen te voorkomen. De informatie afkomstig van de BIM's was wel nuttig om informatie afkomstig van andere collectiemiddelen te bevestigen of te ontkrachten, om andere denkpistes aan te reiken of om onderzoekhypotheses uit te werken of uit te sluiten;
- de ADIV zette voor de aanslagen geen BIM's in ten aanzien van de geselecteerde personen;
- het komt zeer vaak voor dat het afluisteren van telefoongesprekken werd opgestart als gevolg van een vraag van een buitenlandse correspondent, vaak in het kader van een meer algemene samenwerking;
- personen die gevolgd werden in het kader van terrorisme, leken vaak te beseffen dat zij het voorwerp uitmaakten van een opvolging en ontwikkelden hiertegen contra-strategieën om de opvolging te ontlopen.

Het Comité was van oordeel dat er aan de VSSE geen gebrek aan inzet kon verweten worden. De dienst heeft zich heel wat inspanningen getroost om te trachten inlichtingen in te zamelen.

Het Comité formuleerde wel een opmerking met betrekking tot de mogelijkheid om de informatiepositie te verbeteren aan de hand van gerechtelijke informatie. Het was immers zo dat de VSSE op systematische wijze verzocht werd om technische bijstand te verlenen bij gerechtelijke dossiers van het Federaal Parket. Hierdoor kreeg de dienst toegang tot die dossiers hetgeen eveneens een bron van informatie kon zijn. Het Comité vroeg zich af of de VSSE systematisch gebruikt maakte van deze collecte-mogelijkheid of opportuniteit.

II.3.3.3. De (in- en externe) informatiedoorstroming

Het aantal bij de inlichtingendiensten inkomende gegevens alsook de hoeveelheid eigen gecollecteerde informatie, lag enorm hoog. Het risico bestond daarbij dat bepaalde stukken aan de aandacht ontsnapten en/of bij de verdere behandeling en rapportering naar buiten toe niet voldoende op de voorgrond kwamen. Dit kon een inhoudelijk kwaliteitsverlies tot gevolg hebben.[41]

---

40 Uiteraard werden er onmiddellijk na de aanslagen zeer veel BIM-methoden ingezet. Het Comité heeft deze ook onderzocht.

41 Het Comité kon vaststellen dat er in een bericht dat de VSSE midden 2015 ontving uit het buitenland omtrent de mogelijke terreurplannen van IS, sprake was van contacten die de *foreign fighters* in 'Molenbeek' hadden, terwijl in het rapport aan het parket daaromtrent de meer algemene vermelding 'Brussel' werd meegegeven. Eveneens stelde het Comité vast dat

Het Vast Comité I onderzocht dit gegeven aan de hand van enkele casussen: de via HUMINT gecollecteerde inlichtingen ten aanzien van Abdelhamid Abaaoud en Mohammed Abrini bij de VSSE en de SIGINT-informatie van de ADIV.

Wat betreft de VSSE, vond het Vast Comité I weinig of geen verlies inzake precisie en volledigheid tussen enerzijds de inzake Abaaoud gecollecteerde HUMINT-informatie en anderzijds de nota's bestemd voor andere overheden. Wat door de bronnen werd gerapporteerd, vond zijn weg naar buiten, weliswaar met variabele snelheid.

Wat betreft Abrini, kwam een ander beeld naar voor. HUMINT-bronnen brachten heel wat informatie aan, maar de VSSE stelde hieromtrent geen externe nota's op. De HUMINT-informatie bleef binnenskamers, wat uiteraard niet impliceert dat de VSSE er niets mee deed.

De informatie die door de SIGINT-afdeling van de militaire inlichtingendienst gecollecteerd werd, had drie bestemmelingen: de ADIV zelf, Belgische partnerdiensten en buitenlandse SIGINT-partners. De SIGINT-documenten bestemd voor intern gebruik bleken in de regel heel gedetailleerd. De documenten voor de VSSE en/of de gerechtelijke autoriteiten waren in het algemeen veel minder gedetailleerd en volledig.[42] Er was dus sprake van een verlies aan volledigheid en precisie van de doorgezonden inlichtingen. Maar *in casu* kon het Vast Comité I niet vaststellen dat het cruciale informatie betrof. Aangezien SIGINT-informatie in principe nooit in brute vorm wordt doorgezonden naar externe partners, vereist dit een bewerking én dus een zekere tijd. Maar indien cruciale informatie volledig en snel naar een partnerdienst moet verzonden worden, kan hieraan tegemoet worden gekomen.

II.3.3.4. De analyse van de gecollecteerde informatie

De analyse vormt een essentiële component van het inlichtingenwerk. Er bestaan diverse methodologieën om de analyse te structureren. De diensten deden er evenwel onvoldoende hun voordeel mee. Het Vast Comité I benadrukte dat dit de diensten niet heeft belet om op belangrijke momenten de nodige waarschuwingen uit te zenden.

---

een rapport dat de ADIV in de zomer van 2015 ontving, niet verder doorstroomde. Daarin was sprake van een militaire eenheid die ingezet was in het kader van de bijstand aan de politie, die Abaaoud had menen op te merken in de Brusselse regio, terwijl iedereen er op dat ogenblik van uitging dat hij in Syrië was. Het rapport werd weliswaar door de betrokken militaire eenheid ook aan de politie overgezonden.

42 Eind oktober 2015 bijvoorbeeld, werd voor intern gebruik een document opgesteld over twee medestanders van Abaaoud, met daarin heel wat details. De nota die hieromtrent naar de VSSE werd verzonden, was veel minder expliciet. Hiervoor werden een aantal redenen aangehaald die te maken hebben met de specifieke SIGINT-werkingsregels die bijvoorbeeld vereisen dat de brute informatie wordt ontdaan van gegevens die een zicht kunnen geven op de bron van de informatie.

Een belangrijke methode is het opstellen van mogelijke scenario's en het stellen van hypotheses die kunnen bevestigd of ontkracht worden. Zo bijvoorbeeld hanteerde de VSSE lang de hypothese dat de FTF van plan waren zich definitief in het op til zijnde Kalifaat te vestigen of daar te sterven en ze niet de bedoeling hadden terug te keren. Hierdoor werd de weerslag van het fenomeen op Europese bodem aanvankelijk in het algemeen onderschat, hoewel de VSSE aanvankelijk wel, weze het heel kort, van een *worst case*-scenario uitging. Dergelijke scenario's zijn belangrijk omdat ze een houvast bieden om nadien via indicatoren te bepalen welke kant het scenario uitgaat. Ze vormen belangrijke methodologische instrumenten die meer zouden kunnen worden toegepast.

Het Vast Comité I meent echter dat dergelijke scenariovorming bij voorkeur multidisciplinair gebeurt. Een terrorisme-scenario heeft immers meerdere componenten – zowel burgerlijke als militaire – zodat de VSSE en de ADIV ter zake hadden kunnen samenwerken. Dit had tot betere resultaten kunnen leiden. Het is met andere woorden niet omdat de ADIV zich in eerste instantie ten aanzien van de 'civiele' FTF grotendeels onbevoegd achtte, dat zij in deze geen nuttige bijdrage had kunnen leveren.

Ten slotte stelde het Comité dat er een verband moet bestaan tussen de collecte en de analyse: beiden moeten mekaar voeden en in evenwicht zijn. Vandaar dat het Comité het belang onderstreepte van een 'overkoepelend inlichtingendesign' voor een bepaald fenomeen of een concrete dreiging of *target*. In principe zou dit design niet enkel binnen elke dienst moeten bestaan, maar ook rekening houden met – en idealiter gebruik maken van – collecte- en analysecapaciteiten van andere diensten. De na de aanslagen opgestelde *Memory of Understanding* (*infra*) gaat die richting uit.

II.3.4. DE SAMENWERKING OP NATIONAAL VLAK

II.3.4.1. De samenwerking in het kader van de local task forces

Wat betreft de werking van *local task forces* deed het Comité volgende vaststellingen:

- de deelnemers aan de LTF moeten elkaar goed informeren over eenieders noden, behoeften, mogelijkheden en beperkingen. Op die manier is er wederzijds begrip mogelijk over wat de LTF al dan niet kan opleveren;
- wat specifiek de VSSE betrof, bleek dat het voor de deelnemers niet altijd duidelijk was welke informatie kon worden gedeeld. Het Comité beval aan dat hierover intern de diensten duidelijkheid zou worden gecreëerd en dat vertegenwoordigers uit de provinciale diensten die aan de vergaderingen deelnamen, daarbij vanuit het centrale bestuur actief zouden worden ondersteund en gestuurd;

– de inlichtingendiensten moesten steeds nagaan welke het gepaste classificatieniveau was van een bepaalde informatie en dat aangezien ten tijde van het toezichtonderzoek niet alle LTF-deelnemers over de vereiste veiligheidsmachtiging beschikten;
– de ADIV nam minder dan de VSSE aan de LTF deel. De dienst haalde als reden de krappe personeelsbezetting aan. De ADIV stelde voor om zich in de LTF door de VSSE te laten vertegenwoordigen. Het Comité was van oordeel dat deze werkwijze kon worden overwogen, mits de wederzijdse verwachtingen en de procedures bij de uitwisseling van informatie naar behoren zouden vastgelegd worden;
– aangezien de protagonisten van de aanslagen zich hoofdzakelijk in Brussel bevonden, hebben de LTF's in andere arrondissementen weinig informatie kunnen bijdragen.

II.3.4.2. De samenwerking in het kader het Plan Radicalisme (Plan R)

Wat de werking van het Plan R betrof, wees het Comité in eerste instantie op de *Joint Information Box* (JIB). De Vaste Comités I en P voerden reeds een onderzoek naar deze door het OCAD beheerde lijst van radicaliserende vectoren. Het onderzoek toonde vooral aan dat het JIB in de onderzochte periode weinig performant was en in de regel vooral (en meestal enkel) tot een politiesignalement leidde.[43]

Naast de JIB-lijst werd tevens melding gemaakt van de diverse thematische en *ad hoc* werkgroepen die werden opgericht binnen het kader van het Plan R. De VSSE en de ADIV maakten deel uit van (de meeste van) deze werkgroepen. Gelet op het tijdsbestek waarbinnen het onderzoek diende afgerond te worden, kon het Comité niet nagaan welke de bijdrage was die vanuit deze groepen kwam in het kader van het opvolgen van de FTF.

II.3.4.3. De samenwerking tussen de VSSE en de ADIV

Er dient een optimale en doeltreffende samenwerking tussen beide inlichtingendiensten te bestaan. Eerder kon het Comité vaststellen dat de samenwerking voor verbetering vatbaar was en deed het meerdere aanbevelingen in die zin.[44] De resultaten van voorliggend onderzoek deden vermoeden dat de situatie voor en ten tijde van de aanslagen in Parijs nog steeds kon verbeterd worden. Het Comité deed immers volgende vaststellingen:

---

43 Het Comité verwees in deze naar dat onderzoek en naar de destijds geformuleerde aanbevelingen. VAST COMITÉ I, *Activiteitenverslag 2015*, 7-11 ('II.1. Gemeenschappelijk toezichtonderzoek naar de Joint Information Box van het OCAD') en 100-101 (IX.2.1. Aanbevelingen met betrekking tot de *Joint Information Box*).

44 VAST COMITÉ I, *Activiteitenverslag 2014*, 116 ('IX.2.2. Nauwere samenwerking tussen beide inlichtingendiensten').

- de bilaterale ontmoetingen tussen de VSSE en de ADIV met het oog op operationele informatie-uitwisseling waren weinig talrijk. Uiteraard waren er wel contacten mogelijk bij andere gelegenheden (bijvoorbeeld in het kader van LTF-vergaderingen);
- er werd met betrekking tot de strijd tegen het terrorisme slechts een beperkt aantal documenten uitgewisseld tussen de inlichtingendiensten;
- de ADIV had moeite om zijn rol bij de strijd tegen het terrorisme af te lijnen, wat tot gevolg had dat de verschillende partners niet goed wisten wat ze konden verwachten;
- tot slot wees het Comité op het feit dat de bij de ADIV vastgestelde problemen inzake informatiebeheer[45] de samenwerking met zijn partners, en dus ook met de VSSE, in de weg stond.

II.3.4.4. De samenwerking met de gerechtelijke overheden en de politie[46]

Wat de samenwerking betreft met politie en justitie, stelde het Comité het volgende vast:

- alhoewel er wel degelijk veel contacten en vormen van informatie-uitwisseling tussen de diensten bestonden (in het bijzonder tussen de VSSE en de Federale Politie), leverde dit voor de onderzochte personen weinig concrete resultaten op;
- inzake de observatie van één van de protagonisten, werkten de VSSE en de politie in de herfst van 2015 goed samen met als doel een welbepaalde inlichting te verifiëren;
- zoals verder (II.3.6.1) blijkt, stuurde de VSSE op bepaalde momenten belangrijke waarschuwingen uit, ook naar de gerechtelijke autoriteiten en de politie;
- wat betreft de ADIV noteerde het Comité vooral de rol van deze dienst in het opstarten en het behandelen van het gerechtelijk dossier-Zerkani.[47] Het was

---

45 VAST COMITÉ I, *Activiteitenverslag 2010*, 105 ('IX.2.12. Een performant informatie-beheerssysteem voor de ADIV') en *Activiteitenverslag 2011*, 12-13 en 106-107.

46 Er bestaan heel wat normen over de samenwerking en informatie-uitwisseling tussen inlichtingendiensten en politionele en gerechtelijk overheden: artikel 29 Sv., artikelen 19, 19/1 en 20 § 2 W.I&V, COL 9/2005 van het College van Procureurs-generaal betreffende de gerechtelijke aanpak inzake terrorisme, COL 9/2012 van het College van Procureurs-generaal houdende regeling van de inlichtingen- en veiligheidsdienst – samenwerking tussen VSSE/ADIV en de gerechtelijke overheden, COL 10/2015 van het College van Procureurs-generaal betreffende de gerechtelijke aanpak inzake *foreign terrorist fighters*, Omzendbrief van de ministers van Justitie en Binnenlandse Zaken van 21 augustus 2015 met betrekking tot de uitwisseling van informatie en het opvolgen van *foreign terrorist fighters* die afkomstig zijn uit België. Na de aanslagen in Parijs werd daarenboven een *Memorandum of Understanding* opgesteld tussen de ADIV, de VSSE, het OCAD en de Federale Gerechtelijke Politie van Brussel. Daarin wordt in regelmatig en structureel overleg voorzien in het kader van de strijd tegen het terrorisme om zo tot een gemeenschappelijke informatiepositie te komen.

47 Deze persoon werd samen met een aantal anderen veroordeeld bij arrest van het hof van beroep te Brussel van 14 april 2016. Hij behoort evenwel niet tot de in het toezichtonderzoek weerhouden protagonisten.

immers een nota van de ADIV die de gerechtelijke autoriteiten voor het eerst op de hoogte bracht van de aanwezigheid van een groep geradicaliseerde personen in Molenbeek;
– het Comité stelde vast dat de ADIV sinds 2015 doorgaans een gunstig gevolg verleende aan de verzoeken om technische bijstand vanwege de Federaal Procureur. De ADIV verklaarde dit te doen om toegang te verkrijgen tot het dossier en aldus zijn kennis over de *foreign terrorist fighters* te verbeteren.

II.3.4.5. De samenwerking met het OCAD

Ingevolge artikel 6 W.OCAD zijn de VSSE en de ADIV, als ondersteunende diensten, '*verplicht ambtshalve of op vraag van de directeur van het OCAD alle inlichtingen waarover zij in het kader van (haar) wettelijke opdrachten (beschikt) en die relevant zijn voor het vervullen van de in artikel 8, 1° en 2°, bepaalde opdrachten aan het OCAD mee te delen*'. Het weze opgemerkt dat de VSSE deze verplichting steeds in die zin heeft geïnterpreteerd dat er geen ruwe informatie dient te worden overgezonden, maar alleen verwerkte inlichtingen.

Zowel de VSSE[48] als de ADIV hebben permanent twee experten afgevaardigd bij het coördinatieorgaan. Deze treden ook op als verbindingsofficier.

II.3.4.6. De samenwerking met de Dienst Vreemdelingenzaken, het Commissariaat-generaal voor de Vluchtelingen en de Staatlozen en Fedasil

De samenwerking tussen de VSSE en deze diensten bestond reeds langer en is niet beperkt tot terrorisme. De VSSE heeft een vaste verbindingsofficier bij de drie diensten. Deze functies kregen een bijzonder belang door de massale migratieproblematiek gedurende de zomer van 2015, moment waarop aan de VSSE gevraagd werd een *screening* uit te voeren van alle personen die asiel aanvroegen.[49]

Ook de ADIV onderhoudt sedert geruime tijd contacten met de drie diensten. Recent duidde de ADIV een contactpersoon aan om de uitwisseling van informatie te centraliseren.

---

48 Om de stroom van informatie met het OCAD te optimaliseren, heeft de VSSE na de gebeurtenissen in Parijs intern een contactpersoon aangeduid die dicht bij de directie staat en regelmatige contacten onderhoudt met de naar het OCAD gedetacheerde expert.

49 Tussen 7 september 2015 en 11 mei 2016 maakten 17.643 personen het voorwerp uit van een screening. 82 onder hen waren gekend in de databank van de VSSE, waarvan 15 personen voor radicalisering. Er werden nauwelijks zes onderzoeken geopend naar personen die konden worden gelinkt aan IS, maar geen enkel van deze onderzoeken toonde een band met de daders van de aanslagen van Parijs. Volgens de VSSE leverde deze – nochtans vrij belangrijke investering – slechts een beperkt resultaat op.

II.3.4.7. De samenwerking met de Algemene Directie Penitentiaire Instellingen

Het Vast Comité I had reeds een onderzoek verricht naar de samenwerking tussen de VSSE en de penitentiaire instellingen.[50] Daarin werd vastgesteld dat de VSSE midden 2015 een cel 'GP' ('Gevangenissen/Prisons') had opgericht. Deze cel verwerkt veel informatie in het kader van radicalisering en terrorisme.[51]

II.3.4.8. De samenwerking met de operationele eenheden van Defensie

Specifiek wat de ADIV betrof, wees het Comité op banden tussen de inlichtingendienst en de operationele eenheden van het leger die tot taak hadden om, in ondersteuning van de politie, voor de openbare veiligheid te zorgen. Aangezien deze eenheden ruim ontplooid waren, konden zij uiteraard informatie op het terrein oppikken en rapporteren (bijvoorbeeld verdachte gebeurtenissen waarvan ze getuige waren). Zo meldde een operationeel detachement de eventuele aanwezigheid van Abaaoud in België in de zomer van 2015. Deze informatie werd gemeld aan de politie, en via de militaire keten ook aan de ADIV.

Gelet op het beperkte tijdsbestek kon het Vast Comité I geen onderzoek voeren naar deze informatiestroom en naar de wijze waarop de ADIV haar primaire taak in het kader van de *force protection* van de op het terrein ontplooide legereenheden uitvoerde (zie II.4.3.3).

II.3.4.9. De samenwerking met de Algemene Directie Crisiscentrum

De VSSE en de ADIV hadden ten slotte ook tarlijke contacten met het Crisiscentrum. Deze contacten hadden weliswaar niet exclusief betrekking op terrorisme maar ook bijvoorbeeld op de algemene openbare veiligheid (manifestaties). De VSSE heeft een vaste verbindingsofficier bij de ADCC.

II.3.5. DE SAMENWERKING OP INTERNATIONAAL VLAK

Artikel 20 W.I&V bepaalt dat de inlichtingendiensten zorg dragen voor de samenwerking met hun buitenlandse homologen. Hieronder wordt de wijze waarop de VSSE en de ADIV uitvoering gaven aan deze bepaling, samengevat weergegeven.

---

50 Zie 'II.5. De VSSE en het Protocol met de Strafinrichtingen' van dit activiteitenverslag.

51 Ten tijde van het onderzoek stelde het Vast Comité I vast dat, door de massa aan informatie, niet alle gegevens verwerkt konden worden.

II.3.5.1. De internationale samenwerking van de VSSE

De VSSE maakt deel uit van verschillende multilaterale samenwerkingsplatforms (Club van Bern, *Terrorism Group*…) en werkt daarin zowel op operationeel vlak (bijvoorbeeld informatie-uitwisseling) als op analytisch vlak met andere diensten samen. Ook worden er soms beleidskeuzes voorbereid op het gebied van (inter)nationale veiligheid in brede zin. Hoewel de operationele samenwerking doorgaans op bilateraal niveau verloopt, werd wat de strijd tegen terrorisme betreft op het terrein ook in multilateraal verband intens samengewerkt.

Daarnaast zijn er ook fora die niet specifiek gericht zijn op inlichtingendiensten maar die wel een belangrijke rol spelen in de strijd tegen terreur (bijvoorbeeld Europol, NAVO…). In sommige fora heeft de VSSE een vaste verbindingsofficier.

De VSSE onderhield ten tijde van het onderzoek bilaterale contacten met diensten uit meer dan zeventig verschillende landen. De intensiteit en de frequentie van de samenwerking liep sterk uiteen. In het kader van de strijd tegen de FTF waren de meest intense relaties deze met onze buurlanden en met sommige niet-Europese landen dicht bij de conflictregio.

Een doorgedreven vorm van bilaterale samenwerking is de uitwisseling van liaisonofficieren. Wat de relaties met de Franse zusterdienst betreft, werd deze vorm van samenwerking door de VSSE reeds geruime tijd betracht, maar kwam ze pas effectief tot stand na de aanslagen in Parijs.

De VSSE maakte ook deel uit van een werkgroep van Europese en niet-Europese partners die kort voor de aanslagen was opgericht specifiek om te werken rond Abaaoud. De werkgroep kwam voorafgaand aan de aanslagen nooit samen.

De gelijklopende hypotheses over plannen tot aanslagen in Europa waarin hij een hoofdrol zou spelen, mobiliseerden vijftien buitenlandse diensten, die gecombineerd over heel wat middelen beschikten. De VSSE ontving in dit kader heel veel inlichtingen. Wel bleken de personen die niet gekend waren door de VSSE, ook grotendeels onbekend voor de vele andere buitenlandse diensten.

De VSSE verspreidde ook informatie waarover hij beschikte, of bevroeg de partners om zijn eigen gegevens te vervolledigen. De internationale inspanningen leverden in de zomer van 2015 een (beperkt) resultaat op: er werden in drie verschillende landen drie terroristen aangehouden uit wiens verhalen duidelijk bleek dat de dreiging naar Europa toe zeer ernstig was.

Vanaf midden augustus 2015 is er druk internationaal berichtenverkeer: de VSSE ontvangt veel nota's met inlichtingen of vragen om inlichtingen. De VSSE gaf of vroeg zelf heel wat informatie aan de partnerdiensten.

Uit het bovenstaande kon worden afgeleid dat er wel degelijk een intense informatie-uitwisseling plaatsvond en er geen aanduiding was dat de VSSE bepaalde gegevens niet deelde.

II.3.5.2. De internationale samenwerking door de ADIV

Ook de ADIV is lid van diverse multilaterale samenwerkingsplatformen. Zo nam de dienst sinds augustus 2015 deel aan een platform dat de opvolging garandeerde van de activiteiten op de sociale media van leden en sympathisanten van IS. De ADIV nam ook deel aan internationale groepen die werkten rond een *counter narrativ* met het oog op het neutraliseren van de IS-propaganda die via het internet en de sociale media verspreid werd.[52]

II.3.6. WANNEER EN HOE BRACHTEN DE INLICHTINGENDIENSTEN DE BEVOEGDE OVERHEDEN OP DE HOOGTE VAN DE DREIGING?

In de loop van de zomer van 2015 ontvingen de diensten een aantal belangrijke signalen die duidelijk maakten dat er een groeiende terroristische dreiging was die zich specifiek naar Europe richtte. Het Comité onderzocht of en op welke wijze de VSSE en de ADIV de bevoegde autoriteiten hiervoor waarschuwden. Maar het ging ook na hoe de diensten de jaren voordien handelden. Er werden vier perioden onderscheiden.

In november 2012 vertrekt de eerste gekende Belgische onderdaan naar de Syrische regio. In die periode ontstaat ook de Islamistische Staat in Irak en de Levant (ISIL, later IS).

Een nieuwe periode dient zich aan vanaf het najaar van 2013; op dat ogenblik was er sprake van de eerste *returnees*. Zonder dat er specifieke aanwijzingen zijn, was duidelijk dat zij een bedreiging kunnen vormen.

De aanslag in mei 2014 op het Joods museum in Brussel, het uitroepen van het Kalifaat door IS in juni 2014 en de oproep om aanslagen te plegen, luidde alweer een nieuwe periode in. Op dat moment zal België ook toetreden tot de internationale coalitie waarbij militairen werden ontplooid tegen IS.

Een vierde en laatste periode startte vanaf de aanslag tegen Charlie Hebdo en de ontmanteling van de terreurcel in Verviers in januari 2015. Deze cel werd (deels) aangestuurd vanuit het buitenland (met Abaaoud als centrale figuur). Deze periode kenmerkte zich door het feit dat kandidaat-terroristen die door IS waren opgeleid, Europa infiltreerden. Een aantal onder hen werd opgepakt; ze onthulden plannen tegen Frankrijk, België en Duitsland. Net voor de aanslagen in Parijs (augustus 2015) was er nog de mislukte aanslag op de hogesnelheidstrein Thalys.

---

52 De ADIV ontwikkelde in de dagen volgend op de aanslagen van Parijs en Brussel een nauwe bilaterale samenwerking met een aantal Europese en niet-Europese partners. Het Comité stelde daarbij vast dat de ADIV zowel samenwerkt met burgerlijke als met militaire inlichtingendiensten.

II.3.6.1. De Veiligheid van de Staat

Het Comité kon vaststellen dat de VSSE de groeiende terroristische dreiging had gedetecteerd en op sleutelmomenten waarschuwingen had uitgestuurd.

In de eerste periode, waarin vooral sprake was van vertrekkers naar Syrië, was de respons van de VSSE eerder afwachtend. Dit betekende evenwel niet dat de dienst geen aandacht had voor het probleem. Integendeel, reeds in oktober 2012 werd een nota aan de politieke overheid gericht om het fenomeen van de Syriëgangers onder de aandacht te brengen. Toen reeds werd ervoor gewaarschuwd dat strijders zouden kunnen terugkeren om aanslagen te plegen. De dienst dacht daarbij eerder aan *lone wolfs* dan aan georganiseerde groepen.

In de overgang van de tweede naar de derde periode stuurde de VSSE in toenemende mate waarschuwingen uit naar de bevoegde ministers. Er werden ook briefings georganiseerd waarin de problematiek van de *returnees* aan bod kwam, zonder dat reeds expliciet sprake was van mogelijke aanslagen in het Westen.

Op het einde van de derde periode – de dreiging wordt inmiddels reëel – werden echter weinig of geen nota's aan de (nieuwe) ministers gezonden. De VSSE verklaarde dit doordat heel wat dossiers na de operatie in Verviers onder gerechtelijke leiding werden voortgezet.

In de periode voorafgaand aan de aanslagen stuurde de VSSE twee belangrijke waarschuwingen uit, waarbij sprake was van mogelijke aanslagen in Frankrijk, België en Duitsland.

Het Vast Comité I besloot dan ook dat de VSSE gepoogd had adequaat te reageren op de komende dreiging. De VSSE besefte op een sleutelmoment dat de dreiging reëel werd (eerst vertrekkers, nadien de dreiging van de *returnees*) en uitte meermaals waarschuwingen.

II.3.6.2. De Algemene Dienst Inlichting en Veiligheid

Ook voor de ADIV ging het Comité na of op het juiste moment de juiste waarschuwingen werden uitgezonden. Hierbij moet uiteraard rekening worden gehouden met het gegeven dat de ADIV niet onmiddellijk betrokken was bij de problematiek van de (burgerlijke) Syriëgangers. In principe was de dienst enkel bevoegd voor dreigingen waarbij (ex-)militairen betrokken waren, of indien er militaire belangen mee gemoeid waren (zoals de bescherming van troepen of van militaire installaties).

Het islamitisch terrorisme vormde reeds langer een aandachtspunt voor de divisie SI van de ADIV. Sinds 2011 werd het een prioriteit en werd er bijzondere aandacht geschonken aan individuen die, in België of in het buitenland, aan deze problematiek gelinkt werden en die een dreiging konden inhouden tegen Belgische militaire belangen.

In de eerste periode bleef de rapportering van de ADIV beperkt tot het verschaffen van inlichtingen binnen de militaire keten voor wat betreft *force protection* in binnen- en buitenland.

In mei 2013 richtte de ADIV een dienst Joint Terro op. Pas na Verviers omschreef de ADIV naar aanleiding van een vergadering met de Nationale Veiligheidsraad zijn bevoegdheid ruimer en begaf de dienst zich ook op 'burgerlijk' terrein. Vanaf dat ogenblik zond de ADIV een aantal belangrijke waarschuwingen uit. De bedoeling was om niet alleen zicht te hebben op het radicalisme binnen het leger in België zelf, alsook op de terroristische dreiging tegen troepen in operatietheaters (Afghanistan en Libanon), maar eveneens om de islamistische extreme netwerken en fenomenen in een veel bredere regio en context in kaart te brengen. Dit vanuit het besef dat het terrorisme niet noodzakelijk in Syrië zou blijven. Het Vast Comité I meende dat dit een terechte reactie vormde.

In februari 2015 gaf de ADIV een briefing aan de Nationale Veiligheidsraad betreffende de dreiging vanwege IS voor België.

Een week voor de aanslagen in Parijs verspreidde de ADIV nog een zeer belangrijke inlichting over een nakende aanslag.

II.3.7. HOE REAGEERDEN DE DIENSTEN OP DE EVOLUERENDE DREIGING?

Het Vast Comité I zocht een antwoord op de vraag hoe de twee inlichtingendiensten als organisatie reageerden op de groeiende terroristische dreiging en of ze hun structuren of werkprocessen aanpasten. Het Comité bekeek de problematiek aan de hand van de vier voornoemde periodes.

II.3.7.1. De Veiligheid van de Staat

Met de oprichting van de 'Taskforce Syrië' in het voorjaar 2013, richtte de VSSE de focus op de problematiek van de *foreign fighters*. Het operationele werk bleef nog aftastend, gelet op het feit dat de dreiging zich nog maar net begon af te tekenen en alleszins ver van België situeerde. De VSSE nam ook deel aan een nieuw opgerichte internationale werkgroep.

Vanaf de tweede periode werden de interne procedures aangepast in de zin dat er in de strijd tegen het extremisme en het terrorisme een nauwere samenwerking tot stand kwam tussen de collecte- en de analysediensten. Vanaf eind 2013 bleek ook uit de BIM-cijfers dat de aandacht van de dienst verschoof naar Syrië-gerelateerd terrorisme.

Op het einde van de derde periode werden plannen gemaakt voor een grondige reorganisatie. Deze structurele aanpassingen maakten deel uit van het in het voorjaar 2014 opgestelde ontwerp van Actieplan 2015 waarin de strijd tegen het terrorisme als belangrijkste prioriteit werd aangemerkt. In diezelfde periode werd

ook gewerkt aan een verbetering van de samenwerking met de gevangenisadministratie en aan een versterking van de SOCMINT-capaciteit.

In de periode voorafgaand aan de aanslagen in Parijs werd het Actieplan 2015, dat in juni door de Nationale Veiligheidsraad was goedgekeurd en waarvoor de regering middelen had vrijgemaakt, geïmplementeerd. Deze reorganisatie nam uiteraard tijd in beslag, mede omdat de hervorming werd doorkruist door de gebeurtenissen in Verviers en de mislukte aanslag op de Thalys. In de laatste periode zette de VSSE veel middelen in in zijn zoektocht naar terroristische elementen, maar zonder doorslaggevend succes.

II.3.7.2. De Algemene Dienst Inlichting en Veiligheid

Wat de ADIV betreft, was het Vast Comité I van mening dat er, gelet op haar beperkte bevoegdheid ter zake, aanvankelijk geen nood was aan belangrijke structuurwijzigingen.

Bij de start van de tweede periode – wanneer het duidelijk werd dat de *returnees* wel degelijk een gevaar konden vormen – voerde de ADIV een structurele aanpassing door. Na Verviers werden nieuwe doelstellingen vastgelegd en de bevoegdheid ruimer omschreven (*supra*). Het Vast Comité I was van mening dat dit een terechte reactie vormde, al bleef de uitvoering een moeilijk punt, gelet op de beperkte middelen.

In de derde periode paste de ADIV zijn prioriteiten aan en versterkte ook de internationale samenwerking op SIGINT-vlak. Eind 2014 werd voorgesteld meer collectemiddelen in te zetten om op permanente wijze inlichtingen te kunnen inwinnen over het jihadistisch terrorisme. In diezelfde periode besliste België om deel te nemen aan de internationale coalitie tegen IS. Door deze deelname kreeg de ADIV toegang tot informatie afkomstig van andere partners in de conflictzone.

De vierde periode vormde voor de ADIV een sleutelmoment. De eigen bevoegdheid, die tot dan toe 'militair' was, werd breder geïnterpreteerd. De ADIV zou zich voortaan ook richten op bedreigingen met 'militaire middelen' ook als ze door niet-militairen uitgevoerd of tegen niet-militaire doelen gericht waren. De ADIV zette ook in op een versterkte internationale samenwerking, daarbij gebruik makend van de opportuniteiten geboden door de internationale militaire ontwikkelingen.

II.3.8. ENKELE STRUCTURELE PROBLEMEN EN RISICO'S

Het Vast Comité I wees op enkele structurele problemen die zich bij de diensten voordeden en die bepaalde risico's met zich meebrachten. Voor de VSSE ging het om de toename van de werkdruk; wat de ADIV betreft werd andermaal gewezen op de problematische situatie van het databeheer.

II.3.8.1. De toegenomen werkdruk en de onvoltooide reorganisatie bij de VSSE

Het Comité noteerde in de loop van zijn onderzoek een sterke toename van de werkdruk binnen de VSSE, en dit uiteraard voornamelijk in de strijd tegen terreur: er werden meer gegevens verwerkt, de urgentie was groter, de dreiging nam toe… Daartegenover stond het feit dat de dienst in 2015 over 15% minder medewerkers beschikte dan in 2010.[53] Kwam daarbij de problematiek van de overuren en de niet-opgenomen vakantiedagen en het gegeven dat het absenteïsme wegens ziekte weliswaar een dalende trend vertoonde, maar nog steeds hoger lag dan het federale gemiddelde. Het Comité drong daarom aan op een snelle overdracht van de Dienst Persoonsbescherming van de VSSE naar de Federale Politie.[54] Hierdoor zouden immers een twintigtal inspecteurs vrijkomen voor inlichtingenwerk.[55] Vanuit dezelfde bekommernis wees het Comité op problemen die de aanwerving van nieuw personeel bemoeilijkten.

Het Vast Comité I kon vaststellen dat de interne hervorming bij de VSSE op het niveau van de collectediensten was afgerond. Dat was ten tijde van het onderzoek nog niet zo voor de analysediensten. Dit betekende dat er geen parallelisme was tussen de collecte – die materiegericht tewerk ging – en de analyse – die nog geografisch gericht was. Dit bemoeilijkte de samenwerking. Ook het fysiek samenbrengen van collecte- en analysediensten om zo de onderlinge communicatie te verbeteren, werd daardoor niet volledig tot stand gebracht en bemoeilijkte de samenwerking.

II.3.8.2. Het informatiebeheer bij de ADIV

Het Vast Comité I wees bij herhaling op het gegeven dat het informatiebeheer bij de ADIV problematisch was.[56] Ook het Commando van de ADIV zelf had dit reeds meerdere malen aangekaart.

Uit onderzoek was gebleken dat de eigen productie van de ADIV ten aanzien van de protagonisten van de aanslagen in Parijs klein was. Dit werd verklaard door het gegeven dat de ADIV zich in de eerste plaats richt op militaire bedreigingen of bedreigingen waarbij militairen betrokken zijn en dat de daders in eerste instantie niet binnen deze categorieën vielen.[57] Maar er was ook een andere verklaring. Het Comité stuitte bij zijn onderzoek namelijk op informatie die wel beschikbaar was binnen de dienst, maar die niet onmiddellijk terug te vinden

---

53 Begin 2016 was er opnieuw een personeelsstijging merkbaar dankzij de beslissing van de regering in de loop van 2015 om nieuwe inspecteurs en analisten aan te werven.

54 VAST COMITÉ I, *Activiteitenverslag 2014*, 44 e.v.

55 Deze overdracht werd gerealiseerd.

56 VAST COMITE I, *Activiteitenverslag 2011*, 12-13 en 106-107.

57 Pas na de feiten in Verviers trad daarin een verandering op: het werd duidelijk dat de inlichtingendiensten te maken kregen met personen die zich inschreven in de 'militaire strategie' van de terreurgroep IS. Vanaf dat moment werd, in het bijzonder Abaaoud, ook voor de militaire inlichtingendienst duidelijk een legitiem doel.

was. Het Comité moest dus opnieuw vaststellen dat het informatiebeheer binnen ADIV problematisch was. Het systeem liet immers niet toe om met zekerheid de totaliteit van de beschikbare gegevens terug te vinden.

De ADIV beschikte weliswaar over een eenvoudig en modern systeem dat relaties tussen gegevens weergaf en dat de nodige mogelijkheden bevatte om de stroom aan informatie binnen een inlichtingendienst te beheren, maar door gebrek aan personeel om de nodige encodering door te voeren en door gebrek aan opleiding om met het betreffende systeem om te gaan, werd het niet of nauwelijks gebruikt. Samengevat concludeerde het Comité dat het beheer van de informatiestromen een risico inhield voor het gehele inlichtingenproces bij de ADIV.

II.3.9. ALGEMENE CONCLUSIES

De inspanningen van de inlichtingendiensten hebben niet geleid tot de tijdige detectie van een cel die banden had met België en die in staat was grootschalige aanslagen te plegen. Bovendien kon Abaaoud niet tijdig worden opgespoord, ook al werd er intensief samengewerkt tussen bijna twintig Europese en niet-Europese diensten.

Hiertegenover staat dat het Vast Comité I geen manifeste gebreken kon vaststellen in de manier waarop de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs hun eigen taak probeerden te vervullen. Er was geen aanduiding dat bepaalde informatie was achtergehouden voor de (buitenlandse) partners.

Dit neemt niet weg dat het Comité – net zoals in het onderzoek naar de opvolging van de FTF (zie II.1) – van oordeel was dat er heel wat zaken voor verbetering vatbaar waren (zie XI.1 en XI.2.1).

II.4. DE INFORMATIEPOSITIE VAN DE TWEE INLICHTINGENDIENSTEN VOORAFGAAND AAN DE AANSLAGEN TE ZAVENTEM EN MAALBEEK

II.4.1. DE FEITEN SAMENGEVAT

Sinds het uitbreken van de burgeroorlog in Syrië in 2011 hebben honderden Belgen deelgenomen aan dit conflict. België had daarmee op een gegeven ogenblik in Europa het grootste aantal buitenlandse Syriëstrijders per inwoner. Maar sinds 2015-2016 verschoof het strijdtoneel. IS voerde wereldwijd terreuraanslagen uit.

Ook België werd daarbij geviseerd. In januari 2013 berichtte de media over Brusselaars die naar Syrië vertrokken en werd er gedreigd met een aanslag in de

hoofdstad. Op 24 mei 2014 schiet Mehdi Nemmouche vier mensen dood in het Joods museum in Brussel. Hij is een teruggekeerde Syriëstrijder. Daarna volgen Charlie Hebdo, Lyon, Parijs … allen met een duidelijke link met België.

Na de aanslagen in Parijs wordt er een (internationale) klopjacht georganiseerd op de resterende daders waarbij alle politie- en inlichtingendiensten betrokken zijn. Een van de daders is Salah Abdeslam. Hij zou gepoogd hebben het *Stade de France* binnen te dringen met een bommengordel, maar zou zich hebben bedacht. Hij vluchtte richting België waar hij spoorloos verdween. Het dreigingsniveau stond op niveau 3: de dreiging was ernstig, mogelijk en waarschijnlijk. Sommige bioscopen sloten de deuren, in terreurmiddens bestond er aandacht voor kerncentrales…

Op 15 maart 2016 voert de anti-terrorisme-eenheid van de Federale Politie in het kader van het onderzoek naar de aanslagen in Parijs een huiszoeking uit in Vorst. De agenten verwachtten een lege woning aan te treffen, maar ze worden onmiddellijk beschoten. Er vallen vier gewonden. Tijdens de inval van de speciale eenheden wordt een verdachte in het bezit van een Kalasjnikov gedood. Achteraf bleek het om Mohamed Belkaid te gaan, die voorheen enkel gekend was onder zijn schuilnaam Samir Bouzid. Twee andere verdachten sloegen op de vlucht. Uit sporen ter plaatse aangetroffen, kon men afleiden dat het mogelijks ging om Salah Abdeslam en Amine Choukri, die ook nog een vals Syrisch paspoort had op de naam van Ahmed Monir Alhay. Het onderzoek loopt dag en nacht verder.

Drie dagen later, op 18 maart, wordt Salah Abdeslam gearresteerd in een onderduikadres in Molenbeek. Samen met hem wordt ook Amine Choukri aangehouden, wiens ware naam Soufiane Ayari bleek te zijn.

Op 22 maart 2016 blazen zelfmoordterroristen Ibrahim El Bakraoui en Najim Laachraoui (alias Soufiane Kayal) zichzelf op in de vertrekhal van de luchthaven Brussels Airport. Er is nog een derde terrorist aanwezig: Mohamed Abrini laat zijn trolley met explosieven achter en verlaat te voet de luchthaven.

Drie kwartier later filmde een bewakingscamera Khalid El Bakraoui – broer van Ibrahim – en Osama Krayem (alias Naïm El Hamed) aan de ticketmachine van het Brusselse metrostation Petillon. Het ondergrondse treinstation Brussel-Nationaal-Luchthaven werd ondertussen afgesloten. Het dreigingsniveau werd opgetrokken tot niveau vier: de dreiging is zeer ernstig en nabij. Omstreeks 9u werd opdracht gegeven de Brusselse metrostations alsook de vijf treinstations te ontruimen. De federale fase van het crisisbeheer werd afgekondigd, het nationaal noodplan voor een terroristische aanslag geactiveerd. Dit kon evenwel niet verhinderen dat zelfmoordterrorist Khalid El Bakraoui zichzelf om 9u11 opblies in een metrostel dat was vertrokken vanuit station Maalbeek richting Kunst-Wet.

In beide gevallen ging het om zelfmoordaanslagen, waarbij de daders, gewapend met zelf vervaardigde explosieven (nagelbommen verstopt in reiskoffers),

zichzelf opbliezen in de menigte. De gevolgen zijn enorm: 35 mensen kwamen om het leven, en vielen meer dan 300 gewonden.

Sommige daders waren teruggekeerde *foreign terrorist fighters* (FTF) en gelieerd aan de terreurgroep Islamitische Staat (IS), dat de verantwoordelijkheid voor de aanslagen dezelfde dag nog opeiste en daarvoor later diverse redenen aanhaalde (hoofdstad van de Europese Unie, deelname aan aanvallen in Syrië, gevangenhouden van Malika El Aroud en Salah Abdeslam, het verbod op dragen van de hijab…).

Er blijkt snel een link met de aanslagen in Parijs: Najim Laachraoui werd gesignaleerd in het gezelschap van Salah Abdeslam; zijn DNA werd gevonden op de bommengordel die werd gebruikt in de Parijse concertzaal Bataclan. Meteen na de aanslagen stelde de VSSE dat het alsmaar duidelijker werd dat de aanslagen in Brussel als het ware het verlengstuk waren van de aanslagen in Parijs. Immers, in beide gevallen ging het om aanslagen die door IS werden opgeëist, die deels door dezelfde personen waren voorbereid en uitgevoerd en waarvan de voorbereiding (en uitvoering) volgens gelijkaardige patronen was verlopen.

Mohamed Abrini, die sinds de aanslagen in Parijs werd gezocht, werd op 8 april 2016 in Anderlecht aangehouden. Dezelfde dag nog wordt Osama Krayem in Laken gearresteerd. Ook de Rwandees Hervé Bayingana-Muhirwa werd die dag gearresteerd. Hij werd ervan verdacht Abrini en Krayem te hebben geholpen bij het onderduiken na de aanslagen. Ook Bilal El Makhouki – in 2015 nog veroordeeld tijdens het Sharia4Belgium-proces – werd in hechtenis genomen.

Op 11 april 2016 werd Ibrahim Farisi aangehouden, samen met zijn broer Smail. Ibrahim Farisi was de huurder van het appartement in Etterbeek van waaruit de daders van de aanslagen in de Brusselse metro vertrokken zijn. Hij gebruikte de flat om een OCMW-uitkering te krijgen, maar leende ze uit aan Khalid El Bakraoui.

Verder werden ook Ali El Haddad Asufi, die een logistieke functie zou hebben gehad bij de voorbereiding van de aanslagen, en Youssef El Ajmi, een jeugdvriend van Khalid El Bakraoui en Ali El Haddad Asufi gearresteerd. Onderzoek leidde eveneens tot de aanhouding van Jawad en Mustapha Benhattal en Samir Chahjouani op 17 juni 2016.

Enkele maanden na de aanslagen kwam ook Oussama Atar (alias Abou Ahmad), neef van de broers El Bakraoui, in het vizier als mogelijk brein achter de aanslagen. Atar werd eerder in Abu Ghraib opgesloten. Hij verbleef tot 2012 in Iraakse gevangenissen, maar kwam vervroegd vrij nadat Amnesty International en de Belgische overheid op grond van humanitaire redenen aan Irak had gevraagd om Atar naar ons land over te brengen. Sindsdien was Atar spoorloos. Hij zou een voortrekker zijn van de Syriëgangers.[58]

[58] Ook de naam van Yassine, de jongere broer van Atar, dook op. Hij werd gearresteerd en er zouden sporen van explosieven zijn aangetroffen op zijn vingers.

II.4.2. OPZET VAN HET TOEZICHTONDERZOEK

Het onderzoek volgde hetzelfde stramien als dat naar de aanslagen in Parijs (II.3).[59] Het Vast Comité I noteerde onmiddellijk na de feiten de namen van personen die betrokken waren bij de aanslagen als (vermeende) dader of medeader.[60] Vooreerst werd de informatiepositie geschetst voorafgaand aan de aanslagen in Brussel ten aanzien van deze geselecteerde personen. Vervolgens werd nader ingegaan op de verschillende 'collectedisciplines' (HUMINT, SOCMINT, SIGINT en BIM). Ook kwam de samenwerking van de diensten met hun partners en correspondenten, zowel nationaal als internationaal, aan bod. Ten slotte werd beschreven welke activiteiten de VSSE ontplooide in de periode onmiddellijk voorafgaand aan de aanslagen.

II.4.3. DE INFORMATIEPOSITIE VAN DE INLICHTINGENDIENSTEN

II.4.3.1. De Veiligheid van de Staat

Het Comité stelde vooreerst een overzicht op van het aantal documenten in het bezit van de VSSE waarin de naam (of de alias) van de (geselecteerde) (mede) daders in voorkwamen en dit vanaf de aanslagen in Parijs tot de aanslagen in Brussel. De cijfers varieerden van enkele tot vele honderden documenten. Het Comité noteerde ook wanneer een (mede)dader voor het eerst door de VSSE werd opgemerkt en wanneer de dienst voor het laatst (en dit voorafgaand aan 22 maart 2016) informatie over hem verkreeg of verwerkte. Het Comité stelde daarnaast een tijdslijn op voor elk van de (mede)daders die de informatiestromen weergaven en gaf een beschrijving van de informatiepositie en de evolutie hiervan. Tevens werd aandacht besteed aan de 'bron' van de informatie (eigen collecte, bijvoorbeeld via BIM, informatie van Belgische of buitenlandse diensten…).

---

59 Het toezichtonderzoek '*over de informatiepositie van de twee inlichtingendiensten, voorafgaand aan 22 maart 2016 's morgens, over de individuen of groepen die de aanslagen te Brussel en Zaventem hebben uitgevoerd of hierbij betrokken waren evenals naar de individuen of groepen die Salah Abdeslam hebben toegelaten zich in de clandestiniteit op te houden tot zijn arrestatie op 18 maart 2016*' werd geopend op 20 juli 2016. Het eindrapport dateert van 4 november 2016. Gelet op de beperkte tijd kon het Comité in dit onderzoek niet alle aspecten van de problematiek bestuderen. Het Comité dacht hierbij aan volgende thema's: welke *leads* werden door de inlichtingendiensten mogelijks gemist, hoe gebeurde de aansturing van de diensten door hun respectieve directies, hoe verliep de samenwerking tussen de betrokken politie- en inlichtingendiensten, hoe verliep de werking rond crisisbeheer bij de VSSE in de praktische aanpak van de aanslagen van 22 maart.

60 Andere mogelijkse betrokkenen werden pas later bekend: het betreft onder meer Ali El Haddad Asufi, Youssef El Ajmi, Jawad en Mustapha Benhattal, Samir Chahjouani en Oussama en Yassine Atar.

Uit de onderzoeken van het Vast Comité I bleek dat sinds de aanslagen in Parijs grote inspanningen werden verricht om Abrini en Abdeslam op te sporen. Zowel nationaal als internationaal werden belangrijke middelen ontplooid: ten aanzien van Abdeslam onderhield de VSSE met 27 buitenlandse diensten op vier continenten contact en wisselde informatie hieromtrent uit; ten aanzien van Abrini waren 12 buitenlandse diensten betrokken. De tijdslijn maakte duidelijk dat de intensiteit van de informatiestroom gaandeweg afnam vanaf februari 2016.

Wel werden er ten aanzien van Abrini nog bijzondere inlichtingenmethoden ingezet tot net voorafgaand aan de aanslagen. Achteraf gezien zou, op basis van gekende contacten van Abdeslam die in verband stonden met de aanslagen in Brussel, tot de conclusie kunnen worden gekomen dat het mogelijk was om, voorafgaand aan de aanslagen, de namen van de betrokkenen aan mekaar te verbinden. Dit lag evenwel niet voor de hand. Veel van de (mede)daders maakten immers gebruik van schuilnamen en konden pas laat (of pas na de aanslagen) worden geïdentificeerd. Bij wijze van voorbeeld was men, in een concreet geval, in de veronderstelling dat men met twee verschillende individuen te maken had, terwijl het in werkelijkheid om één en dezelfde persoon ging. De opbouw van een gedegen informatiepositie werd hierdoor in grote mate bemoeilijkt.

Laachroui en Belkaid genoten de aandacht van de VSSE omdat ze in september 2015 werden opgemerkt samen met Salah Abdeslam. Op dat ogenblik was het binnen de internationale inlichtingenwereld (én bij de VSSE), duidelijk dat zij deel uitmaakten van éénzelfde netwerk. Ze waren toen evenwel nog niet gekend onder hun ware identiteit. Najim Laachraoui had valse identiteitspapieren op naam van Kayal. Belkaid had een valse identiteitskaart op naam van Bouzid. Ze konden al de tijd ondergedoken leven.

De broers El Bakraoui waren sinds december 2015 bij de VSSE gekend, maar in eerste instantie met een louter crimineel profiel. Pas na de inval in Vorst veranderde dit toen bleek dat Khalid het *safehouse* onder een schuilnaam had gehuurd.

Osama Krayem – alias Naïm al Hamed – was diegene met de rugzak die contact had met El Bakraoui kort voor die zich opblies in de metro in Maalbeek. Hij was eveneens betrokken bij de voorbereiding van de aanslag in Zaventem. Hij kwam onder zijn valse identiteit als Syrisch vluchteling via Griekenland in Europa binnen. Krayem was onder zijn ware identiteit onbekend bij de VSSE en dit tot aan de inval in Vorst, omdat er valse papieren van hem werden aangetroffen.

Voorafgaand aan de aanslagen van 22 maart 2016 waren Farisi, Bayingana Muhirwa, Ayari[61] en El Makhouki voor de VSSE geen prioritaire doelwitten. Wel bleek dat enkelen onder hen hand- en spandiensten hadden verleend. Zo heeft Farisi actief deelgenomen in het helpen verwijderen van sporen uit een *safehouse* en verleende Bayingana Muhirwa onderdak aan voortvluchtigen. Welke de speci-

[61] Wat betreft Soufiane Ayari wist de VSSE voorafgaand aan de aanslagen dat hij door Salah Abdeslam werd opgehaald in een ander Europees land. Ook hier werden valse identiteiten gebruikt.

fieke rol van de andere personen was, was op het ogenblik van het afsluiten van het toezichtonderzoek niet bekend.

II.4.3.2. De Algemene Dienst Inlichting en Veiligheid

De ADIV kende in zijn bestanden de namen van slechts vier van de (mede)daders, te weten Salah Abdeslam, Mohammed Abrini, Najim Laachraoui et Khalid El Bakhraoui.[62] Het Comité stelde daarenboven vast dat de militaire inlichtingendienst wat betreft deze vier personen over geen enkele informatie beschikte afkomstig van de eigen collecte (*infra*). De beschikbare informatie was afkomstig van nationale en internationale partners en van de (inter)nationale pers. Het merendeel van de beschikbare informatie was SIGINT-informatie van buitenlandse partners. Deze informatie had in hoofdzaak betrekking op de aanslagen in Parijs.

Gelet op de schaarse informatie – die bovendien slechts vier (mede)daders betrof – dient te worden gesteld dat de ADIV over een slechte informatiepositie beschikte.[63] Het Vast Comité I verwonderde zich hierover gelet op het feit dat de ADIV de opvolging van het jihadistisch terrorisme als een prioriteit heeft beschouwd en gelet op de rol die de dienst te vervullen had/heeft[64] in het kader van de *force protection* ten aanzien van de militairen die, naast de politie, bewakingsopdrachten vervullen in Belgische steden.

II.4.3.3. Een bijzondere informatiestroom binnen defensie: de Operation Vigilant Guardian

Sinds januari 2015 patrouilleren militairen voor een reeks strategische gebouwen. Hun aantal evolueerde in functie van het dreigingsniveau van 150 tot meer dan 1800 eenheden. Deze *Operation Vigilant Guardian* (OVG) heeft tot doel de Federale Politie te ondersteunen.

Net zoals bij operaties waarbij troepen in het buitenland worden ontplooid, komen bij deze binnenlandopdracht ook bepaalde inlichtingenaspecten aan bod. Naast bewakings- en beveiligingsactiviteiten, vervullen de ingezette militairen de rol van 'sensor': zij nemen evenementen en incidenten waar en brengen er rapport over uit. Deze 'inlichtingenactiviteit' verloopt normaliter als volgt: de betrokken

---

62 De andere mede(daders) komen slechts onder de aandacht van de ADIV ná de aanslagen van Brussel.

63 De Chef ADIV uitte zich in dezelfde termen in zijn rapport dat werd opgesteld voor en geadresseerd aan de parlementaire onderzoekscommissie 'aanslagen'. Ten aanzien van het Comité stelde de ADIV dat de dienst zich grotendeels kon vinden in de conclusies van zijn rapport. De dienst wees eens te meer op een schrijnend personeelsgebrek.

64 Uit eerder onderzoek kon worden vastgesteld dat de Wet op de inlichtingen- en veiligheidsdiensten drie aanknopingspunten bood voor het verzamelen en verwerken van gegevens inzake *foreign terrorist fighters*. Hierover: 'Hoofdstuk II.1.2.2. De Algemene Dienst Inlichting en Veiligheid'.

militairen krijgen vooraf een al dan niet gedetailleerde briefing over de omgeving, wat hen te wachten staat en waarvoor ze aandachtig moeten zijn. Belangrijk is dat ze tijdens of na afloop van de missie ook binnen de militaire keten rapport uitbrengen bij daartoe speciaal aangeduide officieren ('G2') binnen hun eenheid. Vandaar gaat de informatie naar de ADIV. De in het kader van OVG opgemaakte procedures zijn evenwel verschillend. De ingezette militaire detachementen, dewelke op het terrein onder de operationele leiding van de Federale Politie staan, rapporteren in de eerste plaats aan de politie.[65] De informatie wordt weliswaar gelijktijdig gerapporteerd naar de Defensiestaf (C-Ops), die alle operaties coördineert en opvolgt. Echter, in tegenstelling tot wat gebeurt bij buitenlandse operaties, wordt de informatie binnen de operationele eenheden (in hoofde van hun officieren 'G2'), noch op centraal niveau (C-Ops) inhoudelijk behandeld. Vanuit C-Ops gaat de informatie in kopie naar de ADIV, die deze registreert. In principe hebben de ADIV-analisten er vanaf dat ogenblik toegang toe.

Het Vast Comité I nam alle rapporten door die door de in Brussel en Zaventem ontplooide militaire detachementen tussen 13 november 2015 en 22 maart 2016 werden opgemaakt. Het betrof 24 documenten. Het Comité kon daarbij vaststellen dat de ADIV deze rapporten door tussenkomst van C-Ops wel ontving, maar ze niet inhoudelijk verwerkte.[66] De militaire inlichtingendienst was de mening toegedaan dat de verantwoordelijkheid voor de verwerking van deze rapporten bij de Federale Politie lag. Het Vast Comité I was het niet eens met deze zienswijze: de ADIV wordt er niet van ontslaan om te verifiëren of in de toegestuurde documenten desgevallend informatie zit die de dienst kan aanbelangen. De ADIV stelde ook niet te zijn betrokken bij de voorbereiding van de militairen op hun opdracht in de OVG en geen zicht te hebben op de kwaliteit van de rapporten.

Uit drie casussen kon het Vast Comité I afleiden dat de informatiestroom vanuit het terrein in het kader van de OVG vragen opriep, in de zin dat de informatie niet tot in alle geledingen en mogelijks betrokken diensten was doorgedrongen.

Zo werd begin maart 2016 in twee rapporten melding gemaakt van de mogelijke aanwezigheid op de luchthaven van Zaventem van een van de latere daders. Aan de basis van een van deze rapporten lagen militairen van een bataljon dat gespecialiseerd is in inlichtingengaring.[67] In een eerder verslag van november 2015 werd melding gemaakt van een persoon die vanuit een wagen een veilig-

65 Defensie heeft bij de Federale Politie een liaisonofficier ingezet, die onder andere tot taak heeft om ten behoeve van de politie een syntheseverslag te maken van de in het kader van de OVG opgestelde informatierapporten. Of de politie een bepaalde bestemming geeft aan deze syntheserapporten of aan de initiële rapporten vanuit het terrein, en op welke manier, kon het Vast Comité I niet onderzoeken. Dit gaat zijn bevoegdheid te buiten.

66 De ADIV stelde dat hij aan de Defensiestaf zou voorstellen om de te volgen procedure in de desbetreffende operatieplan van de Chief of Defence (CHOD) in te schrijven.

67 De militairen baseerden zich daarbij op een lijst met namen en foto's van personen die verdacht werden van betrokkenheid bij de aanslagen in Parijs. Ook toen de ADIV werd gevraagd deze lijst te evalueren, antwoordde de dienst dat dit niet tot zijn bevoegdheid behoorde.

heidsdispositief van de militairen filmde; betrokkene had daarbij zijn aangezicht bedekt. Geen van deze drie verslagen werd door de ADIV behandeld of toegezonden naar de VSSE[68] of het OCAD.[69]

Het Vast Comité I is van mening dat vanuit het standpunt van de inlichtingengaring de OVG-detachementen zonder twijfel een waardevolle bijdrage kunnen leveren. De ingezette militairen zijn niet alleen leverancier van informatie, maar ze hebben ook zelf inlichtingen nodig om hun taak naar behoren te vervullen en om zichzelf adequaat te kunnen beschermen. Ook hier ligt een bevoegdheid voor de ADV in het kader van de *force protection*.

II.4.4. DE COLLECTEMIDDELEN

II.4.4.1. De Veiligheid van de Staat

Het Comité kon uit de stijging van het aantal opgestelde rapporten duidelijk afleiden dat de VSSE haar bronnen (HUMINT) had geactiveerd na de aanslagen van Parijs.

Als reactie op de aanslagen hebben de inlichtingendiensten en de Federale Politie de werkgroep binnen het Plan R rond sociale media geheractiveerd. Deze werkgroep die de SOCMINT-cellen van de politie, de ADIV en de VSSE groepeert, heeft tot doel om de samenwerking te verbeteren.

In de periode tussen beide aanslagen stelde de cel SOCMINT van de VSSE 15 rapporten op met betrekking tot de (mede)daders. Deze informatie leverde geen enkele aanwijzing op die wees op een nakende aanslag te Brussel. Wel bleek dat sommige (mede)daders elkaar op één of andere manier kenden.

Het Comité heeft per (mede)dader de ingezette bijzondere inlichtingenmethoden (BIM's) geanalyseerd die werden uitgevoerd tussen 13 november 2015 en 22 maart 2016. De conclusies van deze analyses liepen gelijk met deze naar aanleiding van het toezichtonderzoek aangaande de aanslagen te Parijs (zie II.3.2.2). De ingezette BIM's hebben het onderzoek naar de aanslagen van Parijs vooruitgeholpen. De BIM's gaven weliswaar geen indicatie van wat er nadien nog stond te gebeuren in Zaventem en Maalbeek. Het Comité kon vaststellen dat het gebruik van communicatiemiddelen door de terroristen steeds gesofisticeerder werd, wat tot gevolg had dat de diensten verplicht waren het aantal BIM's op te drijven.

Het Comité stelde vast dat in het kader van de gerechtelijke onderzoeken naar de (mede)daders van de aanslagen van Parijs, een zekere taakverdeling werd

---

68 Het Vast Comité I ging na of de VSSE deze informatie desgevallend via de Federale Politie had verkregen: in de databank van de VSSE was daarvan geen spoor.

69 In het onderzoek naar de aanslagen in Parijs werd hetzelfde probleem vastgesteld (zie 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voor de aanslagen in Parijs'.

bepaald door het Federaal Parket, dit onder meer om te vermijden dat de onderzoeksmethoden van de inlichtingendiensten de methoden zouden verstoren die werden ingezet op gerechtelijk niveau.

Het Comité kon echter ook vaststellen dat in de dagen volgend op de aanslagen in Parijs en Brussel de VSSE talrijke inlichtingenmethoden heeft uitgevoerd waarvan de inlichtingenfinaliteit niet steeds duidelijk was. De VSSE erkende dat er in de crisis volgend op de aanslag, een verdeling van targets en van selectoren plaatsvond tussen de VSSE en de Federale gerechtelijke Politie. De dienst was er zich van bewust dat het gebeurde, in precieze omstandigheden, dat er werd gewerkt voor de gerechtelijke overheden. Als reden werd aangehaald dat de gerechtelijke politie over onvoldoende manschappen beschikte. Het Vast Comité I is er zich van bewust dat het beheer van dergelijke crisissen een grote mate van souplesse vereisen vanwege alle betrokken actoren. Het Comité was evenwel van oordeel dat er moest worden gezocht naar oplossingen om deze taakverdeling optimaal te laten verlopen.[70]

II.4.4.2. De Algemene Dienst Inlichting en Veiligheid

De ADIV heeft zijn bronnen geactiveerd op vraag van een andere Belgische dienst, en meer specifiek betreffende twee targets. Geen enkele bron verstrekte concrete informatie.

Het Vast Comité I kon vaststellen dat de SOCMINT-sectie van de ADIV vóór 22 maart 2016 geen enkele actieve collecte over de vier door de ADIV gekende targets heeft uitgevoerd. Het was pas op 21 april 2016 dat er een lijst werd rondgedeeld met twintig op te volgen personen. Deze sectie werd nochtans hervormd in oktober 2015. In die periode wou de directie van de ADIV haar uitrusten met een analytische capaciteit en wou ze het personeel een *ad hoc*-opleiding geven. Het Vast Comité I heeft vastgesteld dat de sectie slechts vanaf 25 april 2016 duidelijke instructies ontving omtrent de doelwitten die zij moest opvolgen. Volgens het personeel van de sectie waren ze echter met onvoldoende personen om alle doelwitten op te volgen.

Enkel de ADIV beschikt over een SIGINT-capaciteit om communicaties in het buitenland te onderscheppen (art. 44*bis* W.I&V). Dit collectemiddel werd niet ontplooid in dit kader. Wel kreeg SIGINT-sectie van de ADIV van buitenlandse SIGINT-partners informatie betreffende drie (mede)daders. Er was sprake van één geval waarin relevante inlichtingen zeer kort voor de aanslagen in het bezit kwam van de SIGINT-afdeling, die deze informatie zowel intern als extern (onder meer met de VSSE, het OCAD en het Federaal Parket) deelde. Het Vast Comité I deed dezelfde vaststelling in het onderzoek naar de aanslagen in Parijs (II.3).

---

70 Na het toezichtonderzoek werden overlegplatformen opgericht om de te volgen targets te verdelen. Het Comité heeft deze overlegplatformen nog niet aan een evaluatie kunnen onderwerpen.

Betreffende de personen die (mede)daders bleken te zijn van de aanslagen in Brussel, werd door de ADIV geen enkele specifieke of uitzonderlijke inlichtingenmethode opgestart.

Het Comité merkte op dat ADIV geen eigen onderzoekpistes had uitgewerkt na de aanslagen van Parijs. Zij baseerde zich dus op de vaststellingen van de VSSE. Wel verleende de dienst bijstand aan de VSSE op het vlak van schaduwing en stelde zijn agenten die specifieke talen machtig zijn, ter beschikking.

II.4.5. DE SAMENWERKING OP NATIONAAL VLAK

II.4.5.1. De Veiligheid van de Staat

Bijkomend aan de vaststellingen die het Comité deed in het kader van het onderzoek naar de aanslagen in Paris (II.1), konden volgende elementen worden toegevoegd.

De inlichtingendiensten en de Federale Politie beslisten om een inlichtingen-*fusion*-cel op te richten. In de periode tussen beide aanslagen ontving de VSSE 200 berichten over de (mede)daders van de Federale Politie. Het OCAD stuurde 33 berichten naar de VSSE, waaronder de *updates* van de geconsolideerde Syriëlijst en van de inlichtingenfiches, een aantal rapporten op basis van sociale media en een aantal punctuele gegevens. De ADIV leverde slechts zeven inlichtingen aan, in hoofdzaak van SIGINT-aard. De VSSE was tevens bestemmeling van de '*CI-weekly security situation*'-rapporten opgesteld door de ADIV.

Tussen november 2015 en maart 2016 stuurde de VSSE 61 nota's naar Belgische autoriteiten (Federaal Parket, OCAD, Federale Politie, minister van Justitie, Nationale Veiligheidsraad, DVZ, CFI, DG EPI, ADIV) waarin één of meerdere namen van de (mede)daders vermeld waren. Sommige van deze nota's werden naar meerdere diensten en autoriteiten tegelijk gezonden.

II.4.5.2. De Algemene Dienst Inlichting en Veiligheid

Het Vast Comité I nam kennis van de diverse '*CI weekly*'-rapporten die de ADIV vanaf midden november 2015 tot net voor de aanslagen in Brussel opstelde. Het betreft een quasi-wekelijkse, vertrouwelijk geclassificeerde publicatie (17 in totaal in de beschouwde periode) die gestuurd werd naar verschillende bestemmelingen (CHOD, VSSE, OCAD, Federale Politie, Crisiscentrum en andere (inter)nationale militaire instanties). De publicatie heeft tot doel informatie te verschaffen over de veiligheidssituatie en de bedreigingen ten aanzien van militaire belangen, maar het betreft – in voorkomend geval – ook de veiligheid van Belgen in het buitenland (dit behoort ook tot de taakstelling van de ADIV). De *CI-weekly* is goed gestructureerd en bevat een *abstract*, een *assesment* en een *general threat analysis*.

De dag voor de aanslag in Parijs op 13 november 2015 publiceerde de ADIV een *CI weekly*. Daarin werd gesteld dat de Belgische deelname aan de coalitie

tegen IS weliswaar het risico op vergeldingsaanvallen tegen ons land verhoogt, maar dat er op dat moment geen concrete aanduidingen waren van mogelijke aanvallen tegen militaire belangen in België of elders. Niettemin werd vermeld dat de dreiging tegen Westerse belangen – inclusief Belgische – als ernstig werd beschouwd. Belangrijk was ook dat de ADIV waarschuwde voor de mogelijke infiltratie van IS-agenten via de vluchtelingenstroom vanuit het Midden-Oosten en Afrika. De ADIV had reeds voorafgaand aan de aanslagen in Parijs kunnen afleiden dat er IS-bewegingen van individuen in Europa waren. De dienst heeft die informatie ook gedeeld met de VSSE eind oktober 2015.

De ADIV deelde ook operationele informatie met de Belgische autoriteiten. Zo zond de dienst SIGINT-gegevens die betrekking hadden op personen die in Brussel een rol zouden spelen, naar de VSSE. De ADIV kon vooral kort na de aanslagen in Parijs een bijdrage leveren, maar de informatie droogde midden januari 2016 op.

Pas na de inval in Vorst, kon de ADIV terug met succes zijn netwerk activeren. De dienst stuurde op 18 maart 2016 een vraag naar zijn internationale partners en kreeg één dag voor de aanslagen van een internationale SIGINT-partner informatie over één van de (mede)daders. Deze informatie kon voorafgaand aan de aanslagen in Brussel echter niet meer verder worden verspreid.

Ten slotte deelde de ADIV andere informatie: op 3 maart 2016 werd aan de VSSE een mogelijke dreiging in maart 2016 gemeld alsook tussen april en juni 2016 (weliswaar in hoofdzaak tegen doelen in de militaire sfeer). Naast tien andere Europese steden, werd ook Brussel vernoemd. De ADIV had deze informatie van een van zijn partners gekregen. De dienst merkte op dat hij geen elementen had om de informatie te bevestigen of de ontkrachten, en uitte twijfel over de *modus operandi* die in het bericht beschreven was. Het Vast Comité I meende te kunnen stellen dat het bericht – als er al enige waarheid in zat – alleszins geen concrete informatie opleverde over de aanslagen in Brussel van een drietal weken nadien.

II.4.6. DE SAMENWERKING OP INTERNATIONAAL VLAK

II.4.6.1. De Veiligheid van de Staat

In de beschouwde periode ontving de VSSE van circa 30 buitenlandse correspondenten meer dan 200 berichten (*supra*). Bijkomend aan de vaststellingen uit voorgaand onderzoek (II.3) noteerde het Comité volgende elementen:

– de VSSE legde de nadruk op de belangrijke rol die in België geaccrediteerde verbindingsofficieren spelen op het vlak van de uitwisseling van informatie;
– de VSSE wenste zelf over verbindingsofficieren te kunnen beschikken in het buitenland met het oog op het optimaliseren van de uitwisseling van informatie;

– de internationale samenwerking in de inlichtingenwereld was aan een grote evolutie onderhevig; er werd gestreefd naar meer efficiëntie en een snellere uitwisseling door het oprichten van een permanente samenwerkingsstructuur binnen de *Counter Terrorism Group* (CTG).

II.4.6.2. De Algemene Dienst Inlichting en Veiligheid

Eerder werd aangegeven dat het grootste deel van de informatie waarover de ADIV beschikte, afkomstig was uit internationale bronnen (bijvoorbeeld de SIGINT-informatie). Wat betreft de internationale platformen waarvan de ADIV lid is, formuleerde het Comité volgende opmerkingen:
– deze platformen zijn van strategisch en politiek niveau; informatie van operationele of tactische aard wordt hier niet gedeeld;
– de ADIV bracht in mei 2016 een aantal homologe buitenlandse diensten samen om operationele informatie over IS uit te wisselen;
– tussen 2014 en medio 2016 werden ongeveer 200 bilaterale vergaderingen gehouden tussen de ADIV en buitenlandse partnerdiensten, met als onderwerp de terroristische dreiging;
– vanaf 2015 tot medio 2016 nam het diensthoofd van de ADIV deel aan 20 internationale werkvergaderingen met als onderwerp de terroristische dreiging.

II.4.7. DE WEKEN VOORAFGAAND AAN DE AANSLAGEN, VANUIT HET STANDPUNT VAN DE VSSE

Het Vast Comité I ging in het bijzonder na welke activiteiten de VSSE ontplooide in de periode onmiddellijk voorafgaand (vanaf 1 maart 2016) aan de aanslagen van Brussel en op welke wijze de autoriteiten hiervan op de hoogte werden gebracht.[71]

II.4.7.1. De operationele targetlijsten van de VSSE

In zijn 'operationele targetslijsten' geeft de VSSE per week weer welke de prioritaire onderzoeksobjecten of -sporen zijn en de wijze waarop men hierover informatie tracht te verzamelen. Tevens wordt aangeduid welke de betrokken collectedienst is en welke analist instaat voor de opvolging.[72]

---

71 Het Comité had geen inzage in de gerechtelijke onderzoeken die op dat moment liepen en waarin de VSSE als expert was aangeduid (en waar de dienst eventueel bepaalde informatie of inlichtingen kon uit puren).

72 De creatie van deze lijsten – die na de aanslagen in Parijs als werkinstrument werden geformaliseerd en verder verfijnd– sluiten aan bij eerdere aanbevelingen van het Vast Comité I in verband met het opmaken van een overkoepelend 'collecte- en analysedesign' (weze het *in casu* toegepast op de materie van counterterrorisme).

Op de lijst van 7 maart 2016 werden meer dan zestig individuen vermeld. Met uitzondering van één persoon waren alle latere (mede)daders erin opgenomen. Ze vormden dus prioritaire doelwitten. De lijst gaf ook aan welke HUMINT-bronnen verder moesten worden verworven en er werd een opsomming gegeven van de punctuele dreigingsinformatie die de VSSE van buitenlandse correspondenten had verkregen. Deze informatie verwees niet naar de feiten die zich in Zaventem en Maalbeek zouden afspelen.

De targetlijst van 15 maart 2016 was grotendeels identiek aan de vorige. Wel werd het aantal mogelijke dreigingen tegen of in België uitgebreid. Maar het Comité stelde vast dat ook deze nieuw toegevoegde meldingen niets te maken hadden met de aanslagen kort nadien.

II.4.7.2. De werkzaamheden in de eerste weken van maart 2016

De activiteiten en de aandachtspunten van de VSSE in de laatste weken voorafgaand aan de aanslagen konden het best worden gekarakteriseerd aan de hand van vergaderingen waarop een of meerdere latere (mede)daders aan bod kwamen.

In de periode tussen 4 en 21 maart 2016 nam de VSSE deel aan minstens negen vergaderingen waarin één of meerdere van de latere (mede)daders van de aanslagen in Brussel vermeld werden. Bij zeven vergaderingen waren buitenlandse partners betrokken. De aanslagen in Parijs en wat eraan voorafging, maakte de kern uit van de gesprekken. De diensten trachtten de voorbereiding van de aanslag in Parijs te reconstrueren. De (mede)daders werden nog steeds als 'gevaarlijk' omschreven en in staat om nog andere aanslagen te plannen of plegen. Er was echter geen indicatie van een concrete en/of imminente dreiging specifiek tegen België.

De inval door de speciale eenheden in het appartement in Vorst op 15 maart was een belangrijk moment omdat de terreurverdachten (achteraf bleek slechts deels) uit hun schuilplaatsen werden verjaagd. Na de inval volgden de vergaderingen zich op. De VSSE trachtte samen met twee partnerdiensten nog steeds details te achterhalen van de reis die Salah Abdeslam in het najaar van 2015 ondernam en waarbij hij een aantal mensen naar Brussel bracht (één ervan werd immers in Vorst gedood). Op dezelfde dag werd ook een vergadering gehouden met het Federaal Parket en de Federale Politie waarin de gebeurtenissen besproken werden en mogelijke pistes bekeken.

Op 17 en 18 maart 2016 werd – onder meer met een Noord-Europese dienst – vergaderd over de persoon die in Vorst werd gedood. Dit leidde tot diens identificatie (Belkaid).

Naast de vergaderingen waarin gegevens werd uitgewisseld, werd er ook schriftelijke informatie uitgewisseld met Belgische diensten. Dit leverde vooral punctuele, operationele informatie op, onder meer over de mogelijke *whereabouts* van Abdeslam.

II.4.7.3. De inval in Vorst en de arrestatie van Abdeslam in Molenbeek

De inval in Vorst op 15 maart 2016 vormde een scharniermoment. Belkaid werd gedood, twee anderen ontsnapten: Salah Abdeslam en de man die zich bediende van de naam Amine Choukri (later geïdentificeerd als Ayari). Over de inval in Vorst maakte de VSSE een omstandige nota op voor de minister van Justitie waarin de stand van zaken werd geschetst en waarin de dienst meldde welke pistes hij had gevolgd.

Na de inval in Vorst en het oppakken van Abdeslam in Molenbeek, werden spoedvergaderingen georganiseerd door de Nationale Veiligheidsraad.

Op 21 maart 2016 – de vooravond van de aanslagen – wordt een nota aan de minister van Justitie gericht. Daarin worden een aantal onderzoekspistes naar aanleiding van de aanhouding van Salah Abdeslam uitgewerkt. Het Comité noteerde dat:

- bij de inval in Vorst werden geen aanwijzingen aangetroffen die wezen op nakende aanslagen in Zaventem of Maalbeek;
- de VSSE was niet op de hoogte van eventuele verkenningen door mogelijke daders in Brussel of elders met het oog op aanslagen (zoals eerder wel gebeurde in Parijs en later in Nice)[73];
- de VSSE kreeg kort na de feiten in Vorst inzage van een steekkaart die werd toegeschreven aan IS (en waarin details – onder meer *suicide bomber* – over Belkaid voorkwamen). Het document maakte deel uit van een reeks soortgelijke documenten die begin maart 2016 in de openbaarheid kwamen. De vraag waar de betrokkene zichzelf had willen opblazen – indien de informatie op de fiche juist zou geweest zijn – bleef onbeantwoord;
- Abdeslam bleef in de dagen na zijn arrestatie zwijgen.

II.4.7.4. In hoofdzaak operationele informatie

De informatie die nationaal en internationaal werd uitgewisseld was vooral van operationele aard. Datzelfde gold voor de nota's die de VSSE opmaakte en aan de autoriteiten zond: het ging om feiten, onderzoekspistes… Het Comité trof geen nota's aan met meer uitgesponnen analyses of formeel uitgewerkte hypotheses/scenario's over hoe de gebeurtenissen moesten worden geïnterpreteerd of wat er zou kunnen uit volgen en/of nota's die de autoriteiten waarschuwden voor imminente dreigingen. Hierover bevraagd, verklaarde de VSSE dat dergelijke vragen en bekommernissen wel voortdurend leefden. Het Vast Comité I meende dat de VSSE in de nasleep van Vorst/Molenbeek, in het operationele werk werd meegesleurd. Het Comité herhaalde het belang van formele hypothese/scenariovorming en van 'voorspellende' inlichtingen. Uiteraard dienen daar de nodige mensen en middelen voor worden uitgetrokken, een methodologie opgezet en informatie uitgewisseld. Ook wees het Comité er op dat hierbij ook voor andere diensten een

[73] Zoals hoger gezegd (II.4.3.3), werden de observaties van de OVG niet met de VSSE gedeeld.

cruciale rol is weggelegd; zeker voor het OCAD, wiens taak het is om dreigingsevaluaties en strategische analyses op te stellen.

II.4.8. CONCLUSIES

Net zoals bij de aanslagen in Parijs, leidden de werkzaamheden van de inlichtingendiensten niet tot de tijdige detectie van de aanslagen in Zaventem en Brussel. Uit de studie van de verzamelde informatie kon evenmin worden vastgesteld dat de diensten over gegevens beschikten om deze aanslagen te voorkomen.

Het Vast Comité I heeft geen dysfuncties bespeurd in de manier waarop de VSSE voorafgaand aan deze aanslagen zijn opdrachten heeft vervuld als zijnde de in de wet expliciet aangewezen inlichtingendienst in de strijd tegen het terrorisme. Een aantal van de betrokken (mede)daders waren sinds de aanslagen in Parijs bekend en behoorden tot de prioritaire targets van de dienst. Ze wisten evenwel meer dan vier maanden lang aan het oog van de VSSE – net als aan dat van andere Belgische en buitenlandse inlichtingen- en politiediensten – te ontsnappen. De VSSE zette in de maanden voorafgaand aan de aanslagen de beschikbare middelen in (HUMINT, SOCMINT, BIM…) en paste haar werking aan, maar dit leverde weinig bruikbare informatie op. Ook de internationale kanalen en de talrijke vergaderingen met partnerdiensten voorafgaand aan 22 maart 2016, brachten weinig bij. Samengevat kan dus worden gesteld dat ondanks de vele inspanningen de informatiepositie van de VSSE *in casu* onvoldoende sterk was om deze dreiging te keren. Dit doet niets af aan de verdiensten en de concrete bijdrage die werd geleverd bij het verder identificeren en oprollen van het terroristisch netwerk.

Het Comité was van oordeel dat de informatiepositie van de inlichtingendiensten kon worden versterkt inzonderheid op vlak van informantenwerking en door een betere toegang tot de communicatiekanalen van de (potentiële) terroristen.

Wat de ADIV betreft, kon worden vastgesteld dat de dienst na de aanslagen in Parijs zijn HUMINT en SIGINT-bronnen probeerde te activeren ten einde meer te weten te komen over de daders van deze aanslagen. Dit leverde zekere resultaten op op vlak van inzicht in de IS-werking en de interconnectiviteit tussen targets. Het leverde echter geen pertinente gegevens over een concrete dreiging in België. De dienst zette wel geen BIM-methoden in en paste geen SOCMINT toe ten aanzien van de vier door de dienst gekende (mede)daders noch van de andere (mede)daders. Gelet op de zeer beperkte inzet van eigen collectemiddelen, beschikte de ADIV slechts over schaarse informatie en bijgevolg over een slechte informatiepositie met betrekking tot de dreiging in België. Het Vast Comité I stelde in zijn onderzoek vast dat de doorstroming van informatie vanuit de *Operation Vigilant Guardian* zeker beter had kunnen verlopen. In het kader hiervan brachten de in het binnenland ontplooide militaire detachementen informatie-elementen aan die dan ter kennis werden gebracht van de politiediensten in wiens steun de detachementen stonden. Het Vast Comité I ging niet na welk gevolg de

politiediensten hieraan gaven, maar stelde wel vast dat dezelfde informatie tegelijkertijd via de militaire gezagsketen ook tot bij de ADIV kwam, die ze niet behandelde. Het Comité was van mening dat dit wel had moeten gebeuren, zeker in het kader van zijn opdracht om de ontplooide militairen van alle nuttige inlichtingen te voorzien (*force protection*). Wel merkte het Comité op dat de ADIV een deel van zijn operationele CI-capaciteit ten dienste had gesteld van de VSSE wat alleszins de goede onderlinge samenwerking illustreerde.

Het Comité stelde vast dat de nationale en internationale gegevensuitwisseling tussen bevoegde diensten in zijn totaliteit sinds de aanslagen in Parijs sterk toenam, maar dat deze hoe dan ook nog in nominale cijfers vrij beperkt bleef en, zoals ook bleek uit vorige onderzoeken, de informatie-uitwisseling nog verbeterd moest worden. Het Comité kon vaststellen dat de samenwerking tussen voornamelijk Europese inlichtingendiensten in de loop van 2016 een nieuwe dimensie kreeg. De uitwisseling diende op Belgisch en internationaal niveau nog verder te worden uitgediept om de informatiepositie te versterken.

Uit het verslag van het Vast Comité I naar aanleiding van het onderzoek naar de aanslagen in Parijs, bleek dat de ADIV net voor die aanslagen nog een zeer belangrijke waarschuwing over de plannen van IS tegen Europese doelen naar zijn binnen- en buitenlandse contacten had gezonden. De informatie was weliswaar niet concreet genoeg om tot een gerichte tegenactie te kunnen overgaan. Voorafgaand aan de aanslagen in Brussel kwamen geen nieuwe onrustwekkende zaken aan het licht en kon de ADIV in zijn wekelijkse bulletins slechts wijzen op de algemeen aanwezige dreiging tegen doelwitten in Europa.

Beide diensten waren actief betrokken bij het overleg in de Nationale Veiligheidsraad en in dit kader werden door de diensten briefings gegeven en informatie verstrekt. Wat de VSSE betrof, bleek dat de inlichtingen die de dienst naar de Belgische overheden stuurde, vooral van punctuele aard waren en ze zich niet bij machte achtte om meer algemene analyses te maken. Niettemin herhaalde het Comité dat het tot de essentie van een inlichtingendienst behoort om voorspellende en strategische inlichtingen aan te maken ten behoeve van de overheden.

Het Vast Comité I heeft reeds herhaaldelijk vastgesteld dat wanneer de inlichtingendiensten als gerechtelijk expert voor de Parketten worden aangesteld, de gerechtelijke logica de inlichtingenlogica dreigt op te slorpen terwijl juist een goed evenwicht tussen de gerechtelijke actie en administratieve actie vereist is. Er moet daarom effectief aandacht zijn voor een optimale aansturing van de inlichtingendiensten door de administratieve overheden zodat de inlichtingendiensten hun schaarse capaciteiten niet inzetten voor louter gerechtelijke opdrachten zoals de bewijscollecte. Het Comité is daarom van mening dat het risico voor 'vergerechtelijking' van de inlichtingendiensten een belangrijk aandachtpunt is.

Voor het overige verwees het Vast Comité I naar de verschillende aandachts- en verbeterpunten opgenomen in het eindrapport in het kader van het toezichtonderzoek naar de aanslagen in Parijs (zie II.2.4).

II.5. DE BESCHERMING VAN HET WETENSCHAPPELIJK EN ECONOMISCH POTENTIEEL EN DE SNOWDEN-ONTHULLINGEN

II.5.1. INLEIDING

Op 6 juni 2013 publiceerden *The Guardian*[74] en *The Washington Post*[75] voor het eerst informatie uit de tienduizenden (geclassificeerde) documenten die door Edward Snowden, die verschillende functies heeft vervuld in of voor Amerikaanse inlichtingendiensten, waren gelekt. Sindsdien volgden nieuwe onthullingen elkaar op.

De berichten gaven een inkijk in geheime programma's van voornamelijk de Amerikaanse *National Security Agency* (NSA) en de Britse *General Communications Headquarters* (GCHQ). Ze onthulden onder meer het bestaan van het PRISM-programma waarbij de NSA (meta)data van telecommunicatie verkrijgt en brachten aan het licht dat Amerikaanse maar ook Britse diensten inlichtingenoperaties hebben opgezet ten aanzien van bepaalde internationale instellingen en samenwerkingsverbanden (VN, EU en G20) en waarbij ook zogenaamde 'bevriende landen' werden geviseerd.

Deze onthullingen waren het startschot voor vele parlementaire, gerechtelijke en inlichtingenonderzoeken over heel de wereld. Zo ook in België. Op 1 juli 2013 vroeg de toenmalige Begeleidingscommissie van de Senaat aan het Vast Comité I '*[…] een update van de bestaande informatie over de praktijken op het vlak van datamining. […] In de tweede plaats wil de begeleidingscommissie dat het Comité I onderzoekt welke de gevolgen zijn voor de bescherming van het economisch en wetenschappelijk potentieel van ons land, en van de wettelijke opdrachten van onze inlichtingendiensten. Ten slotte wenst de begeleidingscommissie dat het Comité I onderzoekt hoe dergelijke praktijken worden getoetst aan de nationale en internationale rechtsregels die de privacy van burgers beschermen*.'

Het Vast Comité I heeft daarop verschillende toezichtonderzoeken geopend die nauw met elkaar verweven waren.[76] Drie ervan werden in 2014 afgerond.[77]

---

74 G. GREENWALD en E. MACASKILL, *The Guardian*, 6 juni 2013 ('NSA Taps in to Internet Giant's Systems to Mine User Data, Secret *files* Reveals').

75 B. GELLMAN en L. POITRAS, *The Washington Post*, 6 juni 2013 ('US Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program').

76 Een ander onderzoek werd geïnitieerd op klacht van de voorzitter van de Nederlandse Orde van Advocaten bij de Balie van Brussel ('Toezichtonderzoek ingevolge een klacht van een stafhouder naar het gebruik van informatie afkomstig van massale buitenlandse data-captatie in Belgische strafzaken'). Zie hierover VAST COMITE I, *Activiteitenverslag 2014*, 38-43 (Hoofdstuk II.3 'Het gebruik in strafzaken van informatie afkomstig van massale datacaptatie door buitenlandse diensten').

77 Zie VAST COMITÉ I, *Activiteitenverslag 2014*, 7-43 (het betreft respectievelijk 'II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten', 'II.2.

Voorliggend, laatste toezichtonderzoek[78] behandelt de mogelijke implicaties van boven vernoemde buitenlandse programma's op de bescherming van het wetenschappelijk en economisch potentieel van het land.[79] Het wou nagaan of de Belgische inlichtingendiensten:

– aandacht hebben besteed aan dit fenomeen;
– een reële of mogelijke bedreiging hebben gedetecteerd voor het Belgische wetenschappelijk en economisch potentieel;
– er de bevoegde overheden van in kennis hebben gesteld en beschermingsmaatregelen hebben voorgesteld; en
– over voldoende en adequate middelen beschikken om deze problematiek op te volgen.

Ook werd, op verzoek van de dezelfde Begeleidingscommissie, bestudeerd welke de gevolgen waren van het PRISM-programma en/of andere analoge systemen voor het wetenschappelijk en economisch potentieel van het land. Het rapport werd begin 2016 afgerond.[80]

II.5.2. DE VASTSTELLINGEN

II.5.2.1. Massale communicatie-interceptie-systemen en het WEP

Het Vast Comité I kon vaststellen dat de Snowden-onthullingen – ten overvloede en op gedocumenteerde wijze – de feitelijkheid van intercepties van communicaties en data door inlichtingendiensten van bevriende landen (Verenigde Staten, Verenigd Koninkrijk…) hebben aangetoond. Dit gebeurde zowel op massale als op doelgerichte wijze. De overheden van deze landen, voor zover ze al tekst en uitleg gaven, stelden in hun reacties evenwel dat de intercepties enkel gericht waren op – naar hun nationaal recht – legitieme doelwitten zoals de strijd tegen terrorisme, de georganiseerde misdaad en corruptie. Zij ontkenden dat ze worden

---

Privacybescherming en massale datacaptatie' en 'II.3. Het gebruik in strafzaken van informatie afkomstig van massale data-captatie door buitenlandse diensten').

78 Toezichtonderzoek over de aandacht die de Belgische inlichtingendiensten (al dan niet) besteden aan de mogelijke dreigingen voor het Belgisch wetenschappelijk en economisch potentieel uitgaande van op grote schaal door buitenlandse grootmachten en/of inlichtingendiensten gehanteerde elektronische bewakingsprogramma's op communicatie- en informatiesystemen.

79 Zo verklaarde Edward Snowden dat de Europese Unie een prioritair doelwit is voor de NSA en het Britse GCHQ, vooral inzake buitenlands beleid, internationale handel en economische stabiliteit. *'That a major goal of the US Intelligence Community is to produce economic intelligence is the worst kept secret in Washington.'* In: www.europarl.europa.eu:document/activites/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

80 De onderzoekdaden werden diverse malen onderbroken gelet op andere toezichtonderzoeken die aan het Vast Comité I waren toevertrouwd en die een hogere graag van urgentie hadden. De als 'VERTROUWELIJK (Wet 11.12.1998)' geclassificeerde versie van het eindverslag werd aan de bevoegde ministers overgezonden op 11 februari 2016.

ingezet voor economische spionagedoeleinden dan wel om hun eigen bedrijven te bevoordelen.

Het Vast Comité I heeft na afloop van zijn toezichtonderzoek geen kennis van bewezen spionage ten opzichte van Belgische bedrijven of wetenschappelijke instellingen door middel van de massale communicatie-interceptie-systemen zoals het PRISM-programma van de NSA.

Wel kan met een aan zekerheid grenzende waarschijnlijkheid worden aangenomen dat buitenlandse bedrijven, zowel binnen als buiten Europa, het voorwerp waren van interceptie-activiteiten door diensten van voornoemde landen. Hetzelfde kan geconcludeerd worden aangaande de spionage gericht op toppolitici (cf. *Merkelgate*[81]) en op overheden en internationale instellingen zoals de Europese instellingen met betrekking tot de economische en financiële politiek. Deze ontwikkelingen waren voldoende coherent en gedocumenteerd om de reëel vastgestelde Belgacom/BICS-hacking[82] toe te schrijven aan dezelfde diensten.

Het Comité stelde ervan uit te kunnen gaan dat Belgische bedrijven, wetenschappelijke instellingen en politieke overheden verantwoordelijk voor het financiële en economisch beleid, het voorwerp kunnen zijn van economische spionage. Dit geldt ongeacht de gebruikte spionagetechnieken incluis gerichte en ongerichte intercepties, en zeker ook door andere dan de voornoemde landen, *a fortiori* door minder bevriende landen.[83]

Ondanks alle commotie na de onthullingen van Edward Snowden moet worden vastgesteld dat de buitenlandse interceptieprogramma's niet werden stopgezet, maar hoogstens wat beter werden onderbouwd naar het nationaal recht van de betrokken diensten. Er is dan ook geen enkele indicatie dat in de toekomst communicatie-intercepties of cyberspionage zal afnemen, wel integendeel. Redelijkerwijs is het zelfs te betwijfelen of politieke of internationaalrechtelijke afspraken oplossingen of garanties kunnen bieden, gezien het intrinsiek geheim karakter van de spionageactiviteiten. Daarom moet vooral aandacht worden besteed aan de verbeterde bescherming van ICT- en communicatiesystemen.

Nog steeds omwille van het geheim karakter van de interceptieoperaties, waardoor zeer weinig informatie beschikbaar is over de omvang van de spionage die economisch gerelateerd is en nog minder over het uiteindelijk gebruik of effect van die ingewonnen inlichtingen, is het illusoir om ook maar een ruwe inschatting te kunnen maken van de schadelijke gevolgen van het gebruik van deze

81 Edward Snowden bracht aan het licht dat de NSA telefoongesprekken van de Duitse kanselier Angela Merkel afluisterde.

82 Halverwege september2013 meldde telefonieoperator BELGACOM in een persbericht dat het tijdens een veiligheidscontrole sporen van een digitale inbraak in het interne informaticasysteem had gevonden. Er werd toen klacht ingediend bij het Federaal Parket (www.belgacom.com/be-nl/newsdetail/ND). Het zou gaan om een zaak van cyberspionage, gericht op het internationale telefoonverkeer dat wordt beheerd door Belgacom International Carrier Services (BICS).

83 Volledigheidshalve mocht ook de industriële en concurrentiële bedrijfsspionage door private actoren niet vergeten worden, al vielen die buiten het eigenlijk bestek van het onderzoek.

spionagesystemen voor het Belgische economisch weefsel. Bovendien manifesteert de schade zich slechts uitzonderlijk of is ze onrechtstreeks, zoals bij de *hacking* van Belgacom/BICS. Dit concreet geval (van doelgerichte *hacking* en dus *a priori* van niet massale interceptie) toont wel aan dat de schade zeer belangrijk kan zijn.

II.5.2.2. De rol van de Belgische inlichtingendiensten en het OCAD

Zoals in eerdere onderzoeken van het Vast Comité I werd aangetoond[84], hebben de Belgische inlichtingendiensten ook nauwelijks enige rol van betekenis gespeeld in deze problematiek, niet preventief maar ook niet door hun samenwerking aan de operaties van deze buitenlandse diensten.

Specifiek wat het wetenschappelijk en economisch potentieel aangaat, hebben de diensten weinig activiteit vertoond ter bescherming van dit potentieel tegen de bedreiging van intercepties (al dan niet massaal), terwijl ze toch op de hoogte waren of moesten zijn van de risico's, zeker na eerdere onthullingen zoals de ECHELON- en SWIFT-affaires.

Er diende te worden vastgesteld dat er op geen enkel ogenblik, ook niet na de onthullingen, een fenomeen-analyse werd geproduceerd over de massale intercepties en de gevolgen ervan voor België of zijn wetenschappelijk en economisch potentieel.

Anderzijds werden de diensten na de onthullingen hierover evenmin bevraagd door de betrokken sectoren en overheden, in dit laatste geval behalve dan de vraag over de gebeurlijke medeplichtigheid van de inlichtingendiensten aan de *hacking* bij Belgacom/BICS.

Het toen geldende wettelijk kader bleek niet toereikend om complexe dreigingen ten overstaan van de nationale kritieke infrastructuur te weerstaan.[85] In het kader van de implementering van de Wet op de beveiliging van kritieke infrastructuren[86], waarin een rol is weggelegd voor het OCAD (en voor zijn ondersteunende diensten evenals voor het Crisiscentrum), voor de sector van de elektronische communicaties, werd nog geen inventaris opgesteld van de kritieke infrastructuur.

De risicoanalyse die het OCAD ter zake dient te maken, is bovendien een 'all risk'-analyse, terwijl het OCAD in zijn andere opdrachten (en dus expertise)

---

84 Zie bijvoorbeeld 'De zaak-SWIFT', in VAST COMITÉ I, *Activiteitenverslag 2006*, 42-51 of 'ECHELON', in VAST COMITÉ I, *Aanvullend Activiteitenverslag 1999*, 2-51.

85 Deze wetgeving zou een oplossing kunnen bieden of versterken als bepaalde communicatie- of informatica-infrastructuren, bijvoorbeeld de *servers* van de belangrijkste Belgische telecomoperatoren, als behorend tot die infrastructuur zouden worden gerekend. Hierdoor zou ook de exploitant van de infrastructuur er wettelijk toe gehouden zijn de beveiliging op een adequaat niveau te brengen.

86 Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, *BS* 15 juli 2011.

beperkt is tot extremisme en terrorisme. Bovendien omschrijft de Wet van 1 juli 2011 de infrastructuur *'als een installatie, systeem of een deel daarvan, van federaal belang, dat van essentieel belang is voor het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, en waarvan de verstoring van de werking of de vernietiging een aanzienlijke weerslag zou hebben doordat die functies ontregeld zouden raken*'; niet iedereen was van mening dat (cyber-) spionage hieronder valt. Het Comité was evenwel van mening dat de mogelijkheid van intercepties of *hacking* de integriteit van de kritieke communicatiesystemen bedreigen, ongeacht of dit gebeurt omwille van spionagemotieven dan wel andere of meer destructieve motieven.

Andermaal moet ook worden vastgesteld dat de uitoefening van de opdrachten van de inlichtingendiensten, en in het bijzonder van de VSSE, inzake de bescherming van het WEP in de praktijk moeizaam verloopt. Dit was al duidelijk toen de wettelijke bevoegdheid moest geoperationaliseerd worden en het geruime tijd duurde alvorens een definitie van het WEP kon worden ontwikkeld.[87]

Een verklaring hiervoor ligt volgens het Comité vermoedelijk bij het ontbreken van afstemming tussen deze inlichtingendienst en de *stakeholders* zijnde de diverse overheden (federale zeker ook regionale) bevoegd voor het economisch en financieel beleid en de private sector. Dit lijkt te leiden tot een vicieuze cirkel van ontbrekende analyses, onbekendheid van de fenomenen bij de te beschermen sectoren en wat deze te verwachten hebben van onze inlichtingendiensten. De concrete invulling van deze bescherming lijkt daarenboven tot nu toe te lijden onder een negatieve invulling door de inlichtingendiensten (bijvoorbeeld onder de vorm van negatieve adviezen voor export of voor buitenlandse investeringen). Nochtans is een verbeterde bescherming van het WEP niet enkel een verhaal van kosten en beperkingen maar ook van economische groeikansen. Vooralsnog ontbreekt het evenwel aan een instrument dat de brug kan vormen tussen de inlichtingendiensten en de publieke en private actoren van het wetenschappelijk en economisch potentieel.

Het Comité verwijst eveneens naar het actieplan van de VSSE dat – op het ogenblik van de rapportage – prioriteit verleende aan de bescherming van het WEP, maar waarvan de resultaten nog niet konden worden geverifieerd. Ook de ADIV stelde meer werk te willen maken van deze problematiek. Verder bleken, onder de leiding van de Nationale Veiligheidsraad, werkgroepen aan de slag om de bescherming van het WEP enerzijds en de cyberveiligheid anderzijds te verbeteren. De operationalisering van het Cyber Security-centrum was voor het Vast Comité I op dit vlak alleszins een keerpunt en een uiterst beloftevol gegeven.

87 VAST COMITÉ I, *Activiteitenverslag 2006*, 134.

II.6. DE VSSE EN HET SAMENWERKINGS-PROTOCOL MET DE STRAFINRICHTINGEN

Op 1 oktober 2014 werd een toezichtonderzoek opgestart naar de wijze waarop de VSSE het '*protocolakkoord tot regeling van de samenwerking tussen de Veiligheid van de Staat (VSSE) en het Directoraat-generaal Uitvoering van Straffen en Maatregelen (DGUSM)*' uitvoert.[88] Dit akkoord werd afgesloten op 20 november 2006 in het kader van het Plan Radicalisme, dat op 28 april 2006 werd goedgekeurd door het toenmalige Ministerieel Comité voor Inlichting en Veiligheid. Het samenwerkingsakkoord kwam er (vooral) op vraag van de VSSE, die in het begin van de jaren 2000 meermaals aandrong op een betere informatie-uitwisseling met de gevangenissen. Zo maakte de VSSE zich bijvoorbeeld in 2001 zorgen over '*de bekeringsijver van sommige islamistische organisaties in de gevangenissen*'. De dienst betreurde dat '*het Bestuur der Strafinrichtingen nog niet de gewoonte (heeft) aangenomen informatie hierover uit eigen beweging aan de Veiligheid van de Staat te bezorgen.*'[89]

Het doel van het onderzoek lag er in te bestuderen of het akkoord efficiënt werd toegepast, of de VSSE er voor de uitvoering van zijn opdrachten nuttige informatie uit kon putten en, zij het in de marge, na te kijken of de uitwisseling van gegevens van gedetineerden conform de bescherming van de rechten die de Grondwet en de wet aan de personen waarborgen verliep.[90] Rechtstreekse aanleiding van het onderzoek vormden twee eerder afgesloten toezichtonderzoeken.[91]

II.6.1. UITWISSELING VAN INFORMATIE MET DE PENITENTIAIRE ADMINISTRATIE

Artikel 13 W.I&V bepaalt dat de inlichtingen- en veiligheidsdiensten, in het raam van hun opdrachten, inlichtingen en persoonsgegevens kunnen opsporen, verzamelen, ontvangen en verwerken die nuttig kunnen zijn om deze opdrachten te vervullen. De penitentiaire administratie vormt in deze uiteraard een belangrijke informatiebron. De bevoegdheid voor leden van deze administratie om informatie door te zenden naar de Veiligheid van de Staat ligt vervat in artikel 14 W.I&V: ambtenaren en agenten van openbare diensten kunnen, op vraag of uit eigen

88 De DGUSM wijzigde van naam en werd Directoraat-generaal Penitentiaire Instellingen (DG EPI). Het Vast Comité I riep eerder op tot een strikte toepassing van dit Protocolakkoord tussen de VSSE en het DG EPI, in VAST COMITÉ I, *Activiteitenverslag 2012*, 97.

89 VAST COMITÉ I, *Activiteitenverslag 2001*, 104.

90 Het onderzoek werd afgerond half maart 2016.

91 VAST COMITÉ I, *Activiteitenverslag 2011*, 22-25 ('II.3. De informatiepositie en acties van de inlichtingendiensten met betrekking tot Lors Doukaev') en *Activiteitenverslag 2012*, 28-33 ('II.3. De eventuele opvolging van een particulier tijdens en na zijn opsluiting in België').

beweging, inlichtingen meedelen aan de inlichtingendiensten '*op basis van de eventueel afgesloten akkoorden en de door hun verantwoordelijke overheid bepaalde regels*'.

Een in 2010 toegevoegd laatste lid van artikel 14 W.I&V bepaalt dat de VSSE '*toegang [kan] krijgen tot de gegevensbanken van de openbare sector die nuttig zijn voor de uitoefening van hun opdrachten*.' In dit kader kan erop gewezen worden dat de VSSE een rechtstreekse toegang heeft tot SIDIS Suite, het griffiedatabestand van het DG EPI.

Naast het inwinnen van informatie is de VSSE conform artikel 20 § 1 W.I&V ook gehouden om te zorgen voor een zo doeltreffend mogelijke samenwerking met – onder meer – administratieve overheden. Daarnaast kan de VSSE middels protocolakkoorden zijn medewerking en technische bijstand verlenen aan diezelfde overheden (artikel 20 § 2 W.I&V).

II.6.2. DE TOEPASSING VAN HET PROTOCOL DOORHEEN DE JAREN

De finaliteit van het afgesloten akkoord lag erin '*de informatie-uitwisseling te vergemakkelijken en aan te moedigen, de praktische regels te bepalen voor de verwezenlijking van de samenwerking, de uitwisseling van ideeën en analyses te intensifiëren of, met andere woorden, de samenwerking voor wat de opdrachten en de activiteiten van bovenvermelde diensten betreft meer op de praktijk te richten*'.

Het Vast Comité I kon vaststellen dat de implementatie van het Protocolakkoord een lange aanlooptijd nodig had. In de toepassing ervan tekenden zich twee perioden af. Enerzijds de periode tussen 2006 en midden 2014 (waarin de mechanismen die bepaald werden om samen te werken en informatie uit te wisselen slechts matig werden toegepast). Anderzijds de periode vanaf midden 2014 (waarbij de informatie-uitwisseling tussen de VSSE en het gevangeniswezen in een stroomversnelling kwam, zonder dat dit noodzakelijkerwijze geënt was op de mechanismen uit het protocolakkoord).

Het Vast Comité I moest vaststellen dat de wijze waarop het akkoord tot midden 2014 op het terrein uitvoering kreeg, in schril contrast stond met het belang dat de dienst er vóór de totstandkoming, maar ook nadien aan had toegedicht. Zo bleek dat het aantal uitgewisselde documenten over terrorisme-gelieerde of geradicaliseerde gedetineerden in de periode 2006-2014 beperkt was.[92] Wel zou het aantal uitgewisselde inlichtingen met de jaren in stijgende lijn zijn gegaan. Het betrof evenwel voor het merendeel informatie-uitwisseling op basis van persoonlijke/informele contacten. Het Protocolakkoord zou in deze een faciliterende factor zijn geweest in die zin dat personeelsleden van de penitentiaire administratie

92 Naar luid van de VSSE konden er geen cijfers worden gegeven.

(bijvoorbeeld gevangenisdirecteurs) zich minder terughoudend gingen opstellen in hun contacten met leden van de VSSE omdat zij zich juridisch en administratief ingedekt wisten.[93] In die periode werden evenwel nooit de in het Protocol voorziene lijsten van radicale gedetineerden en van terrorisme-gelieerde personen opgesteld. Hiervoor was het wachten tot medio 2014.

Dat het Protocol in de eerste jaren niet echt werd gebruikt als instrument voor inlichtingengaring, had mogelijk te maken met de wijze waarop de VSSE de dreiging percipieerde.[94] In de daaropvolgende jaren leek de problematiek hoger te worden geagendeerd. In de Actieplannen 2011, 2012 en 2013 werd 'extremisme – terrorisme – islamisme (in) gevangenissen' onder 'actieve prioritaire opvolging ' geplaatst.

Het Vast Comité I zag de échte oorzaken voor de verbeterde informatie-uitwisseling en samenwerking tussen de VSSE en het DG EPI evenwel in de volgende elementen: enerzijds belandden vanaf 2012-2013 veel (kandidaat-)Syriëstrijders en ronselaars in de gevangenis en anderzijds legde de nieuwe directie van de VSSE sterk de nadruk op informatie-uitwisseling in het algemeen, en met de strafinrichtingen in het bijzonder.

II.6.3. EEN PUNCTUELE EVALUATIE VAN HET PROTOCOL: VASTSTELLINGEN

Het Comité kon in het kader van zijn onderzoek onderstaande vaststellingen doen:

- hoewel het protocol in hoofdzaak de nadruk legde op moslim-gelieerde radicalisering en terrorisme, bleek dat eveneens informatie werd uitgewisseld over andere fenomenen zoals schadelijke sektarische organisaties, inmenging, anarchisme, extreem rechts en links[95];
- het Protocol bepaalde dat er zou gewerkt worden met lijsten: de VSSE met een lijst van radicale elementen en een van aan terrorisme-gelieerde personen; de DG EPI met een lijst van voor terrorisme veroordeelde gedetineerden. Het DG EPI stelde het 'EPI Register Terrorisme' ter beschikking van de VSSE.[96] De VSSE van haar kant stelde geen lijst op. Volgens de dienst zou het praktisch noch wenselijk zijn dergelijke lijst op te maken. Om tegemoet te komen aan haar deel

---

93 Ook het feit dat de VSSE in 2006 iemand met een grote praktische kennis ter zake had aangesteld om de materie op te volgen, maakte dat de kloof tussen beide administraties kleiner werd. Deze persoon gaf een eerder pragmatisch invulling aan de verplichtingen uit het akkoord, hetgeen mede zorgde voor een stijgende informatie-uitwisseling, weze het op informele wijze.

94 In zijn 'Fenomeenanalyse islamitisch extremisme' uit 2009 wijdt de dienst een hoofdstuk aan het extremisme in de gevangenissen. De dienst besluit daarin dat '*Les activités prosélytes islamiques-extrémistes dans les prisons belges semblent pour l'instant plutôt limitées.*'

95 Gezien de meeste contacten op een informele wijze verliepen, kon hieromtrent geen cijfermateriaal voorgelegd worden.

96 De lijst werd voor het eerst besproken in februari 2014 in de Werkgroep Gevangenissen (Plan R). Nadien werd de lijst gedeeld en regelmatig geactualiseerd.

van de afspraken opteerde de VSSE sinds augustus 2014 om te werken met fiches voor elke gedetineerde die vermeld stond in het 'EPI Register Terrorisme'. Deze fiche vermeldde relevante informatie voor het gevangeniswezen: de mate van vluchtgevaarlijkheid, de kans op radicalisering van derden, de antecedenten op het gebied van wapengebruik… De fiches werden aan de betrokken gevangenisdirecteurs bezorgd die op hun beurt de nodige maatregelen konden treffen;
- het DG EPI, dat bijkomende info kon opvragen bij de VSSE, maakte van deze mogelijkheid in stijgende mate gebruik. Dit was zeker zo sinds de Syrië-crisis waardoor er een toename was van het aantal terrorisme-gelieerde gedetineerden;
- een belangrijke vaststelling was dat de VSSE de toegang tot de SIDIS-gegevensbank activeerde.[97] Voorheen maakte de VSSE gebruik van specifiek daartoe voorziene computers en aparte toegangscodes, maar in 2016 werd een algehele toegang gemaakt. De SIDIS-gegevensbank werd in september 2014 gevoelig aangepast; het nieuwe systeem (SIDIS Suite) werd uitgebreid met tal van gegevens (zoals bezoekers, telefoonnummers…);
- de VSSE en de DG EPI waren, in het kader van het Plan Radicalisme en de daaruit voortvloeiende JIB-lijst, ook samen aanwezig op bepaalde werkvergaderingen. Ook bij die gelegenheden werd informatie uitgewisseld. Beide vormen van informatie-uitwisseling bestonden naast elkaar. De 'EPI Register Terrorisme'-lijst (voor terrorisme veroordeelde gedetineerden) en de Plan R/JIB-lijst (opsomming van radicaliserende elementen) waren duidelijk onderscheiden lijsten met een ander oogmerk;
- daarnaast merkte het Vast Comité I op dat er buiten het Protocol om een praktijk was ontstaan waarbij informatie rechtstreeks met de betrokken gevangenis werd uitgewisseld en niet met de eigenlijke *point of contact* (POC) op nationaal niveau. Het Vast Comité I wees in deze op een gevaar: in de mate waarin bijvoorbeeld van deze uitwisseling geen formeel verslag of PV werd opgemaakt dat in centrale databank van de VSSE (VESTA) werd opgenomen, bestond het risico dat de POC het overzicht zou verliezen;
- volgens de VSSE maakte het DG EPI in toenemende mate melding van personen die tekenen van radicalisering vertonen. Dit was mogelijks een gevolg van de – door de VSSE gegeven – vorming over radicalisering binnen het gevangeniswezen. Evenwel merkte de VSSE zelf op dat ook de actualiteit en de veelvuldige aandacht in de media tot een grotere alertheid bij het penitentiair personeel hadden geleid;

---

97 Artikel 36*bis* van de Privacywet van 8 december 1992 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*'. Het Comité stelde vast dat dergelijke machtiging *in casu* niet werd aangevraagd. Deze aanvraag was naar oordeel van het Comité niet zonder belang aangezien de Privacycommissie in haar advies 08/2016 van 24 februari 2016 stelde dat SIDIS/SIDIS Suite '*de toets van de WVP niet doorstaat*'. Reeds in 2013 maande de Privacycommissie de betrokken administratie aan om '*een wettelijke basis voor deze gegevensbank op punt te stellen*'.

- in het Protocol werd gepoogd een onderscheid te maken tussen terrorisme en radicalisme. Dit onderscheid bleek kunstmatig; er zouden twee afgescheiden regimes moeten zijn, terwijl er in werkelijkheid qua benadering weinig verschil was in de praktijk;
- het Vast Comité I wees op twee ontwikkelingen die ten tijde van het onderzoek van belang waren. Enerzijds waren de VSSE en de DG EPI in groeiende mate verplicht om aandacht te besteden aan het fenomeen anarchisme. Eén bijzondere stroming bleek immers zeer actief in het benaderen van gevangenen en het bestrijden van het bestaan van gevangenissen. Informatie over de 'aanhangers' van de bewuste anarchistische stroming werd sedert enkele jaren regelmatig uitgewisseld. Zowel voor de DG EPI als voor de VSSE leverde de uitwisseling van gegevens pertinente informatie op. Anderzijds werd vastgesteld dat extremistische islamitische groeperingen niet via bezoeken maar veeleer via briefwisseling trachtten invloed te krijgen op moslimgevangenen;
- de VSSE gaf aan dat het DG EPI in een groeiend aantal gevallen melding maakte van opvallend gedrag inzake radicalisering van gedetineerden. Cijfers hierover waren evenwel niet beschikbaar.
- wat betreft het naleven van de regelgeving inzake geclassificeerde informatie, bleek de VSSE zeer tevreden. Het DG EPI van zijn kant stelde evenmin inbreuken vast inzake geclassificeerde stukken;
- het Protocolakkoord benadrukte, zoals hoger aangehaald, ook het belang van opleiding van penitentiaire beambten.[98] Het Comité stelde echter vast dat hiervan pas in 2011 ernstig werk werd gemaakt. Toen werd een vorming georganiseerd voor directeurs, de leden van de psychosociale dienst en enkele penitentiaire beambten. De nadruk van de vorming lag op het herkennen van radicalisme. De opgeleide personen zouden nadien zelf opleidingen kunnen geven binnen de strafinrichtingen. Onder meer door personeelsverloop bleek dit niet optimaal te functioneren. In alle gevangenissen werd er in 2012 en 2013 een algemene sensibiliseringscursus gegeven aan de directie en het hoger bewakingskader. Gevolg hiervan was dat slechts een minderheid van de gevangenisbeambten werd bereikt;
- de in het Protocol afgesproken zesmaandelijkse vergadering tussen de hoofden van de VSSE en het DG EPI ten slotte, greep omzeggens nooit plaats. Dit betekent niet dat er niet gecommuniceerd werd. Medewerkers van beide diensten wisselden ervaringen uit en waren vlot contacteerbaar. Overleg op een hoger niveau bleef evenwel afwezig.

---

98 Zo wordt gedacht aan het inschakelen van de vorming in de COPPRA-vorming (*Community Policing and Prevention of Radicalisation*), het verlenen van medewerking aan het OCAD-deradicaliseringsproject 'ISF' (*Internal Security Fund*), en het aanbieden van een online *tool* voor penitentiaire beambten die zich op die manier via een zelfstudiepakket bepaalde vaardigheden kunnen eigen maken. Deze pistes bevinden zich evenwel nog in een pril stadium en zijn nog weinig concreet.

II.6.4. INITIATIEVEN VAN DE VSSE BUITEN HET PROTOCOL[99]

De VSSE hing voor zijn informatiepositie over (geradicaliseerde) gedetineerden vanzelfsprekend niet integraal af van het met het DG EPI afgesloten Protocol. De dienst nam diverse andere initiatieven. Zo was er bijvoorbeeld de samenwerking in 2013 met een aantal Europese inlichtingendiensten waarbij ervaringen werden uitgewisseld en wat leidde tot het rapport '*After the Prison*'.[100]

Verder werd er bij de VSSE een *point of contact* (POC) aangesteld, werd een cel 'Radicalisering in de gevangenissen' opgericht, ontving elke provinciepost van de VSSE een lijst van contactpersonen van de penitentiaire instelling binnen zijn ambtsgebied en werd er bestudeerd wat nodig was om de problematiek van radicalisering binnen gevangenissen optimaal op te volgen.[101, 102]

II.6.5. CONCLUSIE

Het Vast Comité I concludeerde dat het Protocol één en ander in beweging heeft gezet. Een grote evolutie was merkbaar. Vele aspecten bleven evenwel vrij lang onaangeroerd. Sommige aspecten van het Protocol werden zelfs nooit uitgevoerd. Toch bestond er bij beide diensten een grote mate van tevredenheid. Zowel het DG EPI als de VSSE gaven aan geen zware tekortkomingen te hebben vastgesteld in de werking van het Protocol; het werd als positief ervaren. Het Vast Comité I merkte wel op dat er nooit een evaluatie van het Protocolakkoord werd uitgevoerd.

II.7. DE OPVOLGING VAN EEN POTENTIËLE DREIGING TEGEN EEN BUITENLANDSE BEZOEKER

In maart 2015 richt een agent van de Buitendiensten van de VSSE zich tot het Vast Comité I. Hij beklaagde zich over de wijze waarop de Analysediensten zouden gewerkt hebben in een het dossier over het nakende bezoek van de Congolese dr.

---

99 Deze maakten niet het voorwerp van onderzoek uit door het Vast Comité I.

100 Een omstandige interne nota van de VSSE ('*Intensifiëren van de VSSE-inspanningen in gevangenissen),* wees dan weer op de noodzaak om zicht te krijgen op radicalisering binnen de penitentiaire instellingen.

101 Deze inschatting gebeurde in december 2014 en werd opgenomen in de vermelde interne nota van de VSSE, *genaamd 'Intensifiëren van de VSSE-inspanningen in gevangenissen'* van 1 december 2014. Zij bevat o.a. een studie over de personeelsnoden, de nood inzake HUMINT, de mogelijkheid om een gedetineerde als menselijke bron te hanteren, het bepalen van de frequentie om overheden te informeren en het aanduiden van de medewerkers die exclusief toegang hebben tot het SIDIS-systeem.

102 Halverwege maart 2016 ontving het Comité een uitgebreide studie genaamd 'Fenomeenanalyse Radicalisering en Terrorisme in Belgische gevangenissen – Maart 2016'.

Mukwege aan België. Volgens de klager – tevens een kennis van dr. Mukwege en mede-organisator van het bezoek – werd het OCAD niet correct op de hoogte gebracht van alle relevante informatie om een evaluatie op te stellen over de potentiële dreiging die op de betrokkene rustte.[103]

II.7.1. CONTEXTUALISERING

De Congolese gynaecoloog Mukwege is gekend als een voorvechter van de mensenrechten. Hij trok voor het eerst de aandacht van de VSSE in het kader van de verkiezingen in de Democratische Republiek Congo in 2011. De dienst startte met de opvolging van diens activiteiten in het kader van zijn bezoeken aan België. Deze bezoeken konden immers gevolgen hebben binnen de Afrikaanse diaspora of voor de relaties tussen België en Congo, wat mogelijks een gevaar inhield voor de binnenlandse en buitenlandse veiligheid van België of de buitenlandse relaties.

Dr. Mukwege bezocht meerdere malen België; deze bezoeken gaven nooit aanleiding tot veiligheidsmaatregelen vanwege de Belgische autoriteiten.

In december 2014 werd de VSSE op de hoogte gebracht van de intentie van betrokkene om in maart 2015 opnieuw een bezoek te brengen aan ons land. Aangezien de evaluatie van de situatie in Congo – net zoals de bedreigingen gericht aan de dokter – een permanente opdracht zijn, schreef de Analysedienst hieromtrent geen specifiek kantschrift uit. Het initiatief om informatie te verzamelen, werd op autonome wijze overgelaten aan de Buitendiensten.

Eind februari 2015 stelde de Analysedienst op basis van elementen bekomen via menselijke bronnen en informatie uit sociale media, een nota op voor het OCAD en het Crisiscentrum. In de loop van maart 2015 bereikten nog een aantal rapporten van andere bronnen de dienst, maar deze leverden geen bijkomende elementen op over een eventuele bedreiging tegen de dokter. Ze gaven geen aanleiding tot het opstellen van een nieuwe nota.

Na aandringen van de agent van de Buitendiensten (met name de agent die later de klacht zou indienen bij het Vast Comité I) en van de hiërarchische chef, stelde de Analysedienst op de vooravond van het bezoek alsnog een aanvullende nota op. Deze nieuwe nota vormde voor het OCAD geen aanleiding om zijn dreigingsevaluatie te wijzigen; het handhaafde 'niveau 2'.[104]

II.7.2. VASTSTELLINGEN

Het Vast Comité I stelde vast dat de verzamelde elementen werden geëvalueerd, geanalyseerd en binnen een redelijke termijn meegedeeld aan het OCAD en aan het Crisiscentrum, zodanig dat de passende maatregelen konden genomen worden.

---

103 Het toezichtonderzoek werd in mei 2016 afgerond.

104 De betrokken agent werd door het OCAD verwittigd dat het niveau behouden bleef.

Het Comité stelde zich vragen bij de dubbele rol en de hoedanigheid van de klager: enerzijds trad hij op als agent van de VSSE en anderzijds als privé-persoon.[105] Het Vast Comité I wees er op dat deze 'rolverwarring' nadelig kon zijn voor het uiteindelijke analysewerk.

Het Comité kon geen disfuncties vaststellen in de manier waarop de Analysedienst het bezoek van dokter Mukwege aan België had behartigd. Het gegeven dat een meerderheid van de verzamelde informatie afkomstig was van één enkele collecte-agent (te weten de klager zelf) zou wel de objectiviteit van de daaruit volgende analyse hebben kunnen ondergraven, wat echter *in casu* niet het geval was.

De 'vrijheid van handelen' waarover de collecte-agent beschikte in deze zaak is voor een deel te verklaren door de afwezigheid van richtlijnen, zowel vanwege de Analysedienst ten overstaan van de Buitendiensten als vanwege de betrokken secties van de Buitendiensten. Er was geen collecteplan in de strikte zin van het woord aanwezig. De hiërarchische chef van de agent had wel een signaal gegeven door twee rapporten die deze laatste had opgesteld te weigeren, maar voor het overige werd zijn houding niet op fundamentele wijze gecorrigeerd. In dergelijke gevallen zou de directie van de VSSE een rol kunnen spelen door proactief tussen te komen.

II.8. EEN KLACHT TEGEN EEN INDISCRETE COLLEGA

In juli 2015 dient een hoofdofficier van ADIV een klacht in bij het Vast Comité I. Een medewerker van de ADIV zou immers in een publieke ruimte in de gemeente waar zowel hij als de medewerker wonen, gegevens over diens persoonlijke en professionele leven verspreid hebben. Hij vreesde zelfs dat dit gevolgen zou kunnen hebben voor zijn veiligheid en die van zijn gezin.

De klager richtte zich eerder tweemaal tot de directie van de ADIV, maar vond dat er niet kordaat gereageerd werd. Uiteindelijk diende hij klacht in bij het Vast Comité I. De klacht had zowel betrekking op de beweerde indiscreties als op de wijze waarop de ADIV hierop reageerde. Het eindrapport werd in mei 2016 goedgekeurd.

II.8.1. VASTSTELLINGEN

De medewerker erkende dat hij tijdens gesprekken in de drankgelegenheid over de klager had gesproken. Hij ontkende echter dat hij geclassificeerde gegevens over de klager had meegedeeld; hij zou overigens nooit toegang hebben gehad tot dergelijke gegevens. De Chef van de ADIV stelde met beide betrokkenen een gesprek te hebben gevoerd; hij vond de indiscreties van zijn medewerker profes-

[105] Hij ontkende overigens zijn nauwe betrokkenheid met de dokter niet.

sioneel ongepast. Zijn diensten werden gevraagd om de administratieve medewerker tot de orde te roepen – wat ook gebeurde – maar hij kreeg hierover, door een communicatiefout, geen *feedback*.

De klacht werd oorspronkelijk door de ADIV ingeschat als een problematiek van een lagere orde. De wijze waarop deze werd afgehandeld gaf de klager geen voldoening. De Chef van de ADIV vond het gedrag van de administratieve medewerker ontoelaatbaar, maar stelde vast dat hij geen misbruik had gemaakt van vertrouwelijke informatie. Hij was dan ook van mening dat geen tuchtrechtelijk sanctie aangewezen was. De medewerker werd wel overgeplaatst naar een andere dienst binnen de ADIV. Uiteindelijk werd de klacht binnen de ADIV alsnog behandeld door de sectie veiligheidsmachtigingen. De administratieve medewerker kreeg uiteindelijk een terechtwijzing.

II.8.2. CONCLUSIES

Het Vast Comité I vond geen indicaties dat de administratieve medewerker zijn geheimhoudingsplicht zou hebben geschonden. Evenmin werd er een ongeoorloofde toegang tot het veiligheidsonderzoek van de klager of tot geclassificeerde informatie genoteerd.

Op het vlak van de discretieplicht kon evenwel worden vastgesteld dat de administratieve medewerker niet de nodige professionele terughoudendheid en voorzichtigheid aan de dag had gelegd door in een drankgelegenheid professionele dan wel privé-aangelegenheden van de klager aan te kaarten. In die zin was de klacht gegrond.

Het Vast Comité I vond in zijn onderzoek geen elementen die wezen op een veiligheidsprobleem in hoofde van de klager of zijn gezin. Algemeen was het Vast Comité I van oordeel dat de klacht intern op een meer adequate manier had kunnen worden afgehandeld.

II.9. EEN KLACHT OVER EEN (ON)VERSCHULDIGDE BETALING

Een gewezen inspecteur van de VSSE richtte in april 2015 een klacht aan het Vast Comité I. Hij werd namelijk verplicht een (klein) bedrag terug te betalen dat hij ten onrechte zou ontvangen hebben uit de kas van de speciale fondsen. Nadat hij zijn standpunt tevergeefs had trachten te verdedigen bij de VSSE, richtte hij zich tot het Vast Comité I. Bovendien meldde hij dat de problemen die hij had ondervonden met zijn directe hiërarchie, hem er mee toe hadden gebracht om de VSSE te verlaten.[106]

[106] De klager werkte meer dan drie jaar als lid van de Buitendiensten van de Veiligheid van de Staat.

Het Comité opende hierop een '*toezichtonderzoek naar aanleiding van de klacht van een gewezen agent van de VSSE betreffende het beheer van de afdelingskas van een provinciepost*'.[107]

In de periode waarin de klager werd gevraagd een som terug te betalen (2012-2013), werd een boekhoudkundig systeem gehanteerd dat niet in overeenstemming was met de instructies van het hoofdbestuur en dat niet adequaat was.[108] Het Vast Comité I kon overigens geen bewijzen pro noch contra de stelling van de klager vinden. Het toenmalig boekhoudkundig systeem liet geen controle *post factum* toe, zodat boekhoudkundig niet kon worden vastgelegd of het betwiste bedrag al dan niet verschuldigd was. Bij de afhandeling van de klacht op het niveau van de VSSE werd(en) er geen verantwoordelijke(n) aangeduid, met een mandaat om het gerezen geschil op te lossen. Dit had tot gevolg dat een groot aantal personen zich met de zaak inliet zonder daarbij tot een voor alle betrokkenen aanvaardbare oplossing te komen. Dergelijke handelswijze heeft onnodige spanningen en ontevredenheid in de hand gewerkt.

II.10. EEN KLACHT OVER EEN INTERVENTIE VAN TWEE PROTECTIE-ASSISTENTEN

Tijdens een opdracht op de openbare weg in juni 2015 deed zich een incident voor met twee leden van de (toenmalige[109]) Dienst Persoonsbescherming van de VSSE. De protectieassistenten stonden in voor de veiligheid van een buitenlandse diplomaat, wanneer de wagen van een particulier hen kort bleef volgen en hun bevelen om afstand te houden meermaals negeerde. Wanneer het voertuig van de betrokkene door een verkeerslicht tot stilstand komt, gaan de protectieassistenten over tot een interventie. Zij zouden daarbij brutaal tewerk zijn gegaan. Een van hen trok zelfs zijn wapen. De bestuurster van de wagen gaf deze feiten aan bij het Comité.[110]

Het Vast Comité I hoorde alle protagonisten. Alle interne verslagen die in dit verband werden opgesteld bij de VSSE, werden onderzocht. Het Comité nam eveneens kennis van de wettelijke en reglementaire bepalingen en van de interne

---

107 Het onderzoek werd afgesloten in mei 2016.

108 Uit een vorig toezichtonderzoek naar het gebruik van de zogenaamde 'geheime fondsen' van de VSSE, bleek dat er tijdens de geciteerde periode weinig controle werd uitgeoefend op de manier waarop met de gelden op lokaal niveau werd omgegaan, of op de manier van boekhoudkundige verwerking ter plaatse. Hierover: VAST COMITÉ I, *Activiteitenverslag 2013*, 57 en *Activiteitenverslag 2014*, 63.

109 Deze bevoegdheid werd overgeheveld van de VSSE naar de Federale Politie (art. 7, 3° W.I&V werd opgeheven bij art. 20 Wet van 21 april 2016, *BS* 29 april 2016).

110 Het Vast Comité I besliste op 24 juni 2015 om een toezichtonderzoek te openen. Het diende evenwel meermaals te worden opgeschort als gevolg van andere onderzoeken waarmee het Comité werd belast en die geacht werden dringender te zijn. Het eindverslag werd goedgekeurd op 11 mei 2016.

richtlijnen en voorschriften die van toepassing waren op de uitvoering van persoonsbeschermingsopdrachten.

De persoon die op de dag van de feiten werd begeleid, genoot permanente bescherming en was het voorwerp van een bedreiging die werd geëvalueerd op het niveau drie.[111] Het Comité meende dat het feit dat de klaagster het escorte-voertuig telkens opnieuw naderde, voor de agenten van de VSSE een redelijke grond was om te geloven dat het leven of de fysieke integriteit van de persoon die ze dienden te beschermen ernstig in gevaar was. Deze bezorgdheid rechtvaardigde bijgevolg de controle van het voertuig en zijn bestuurster. Het incident was zonder enige twijfel het resultaat van een gebrek aan voorzichtigheid en inzicht vanwege de klaagster, die onvoldoende afstand nam ten opzichte van het voertuig van de VSSE.

Het Comité was er echter van overtuigd dat het incident had kunnen worden vermeden indien het beschermingsteam geen communicatieproblemen had ondervonden. Het team kon niet adequaat communiceren met betrokkene (geen communicatiepaneel) en beschikte niet over passende communicatiemiddelen[112] waardoor zij hun inschatting in de situatie niet konden aftoetsen. Het Comité stelde eveneens vast dat er bij de VSSE geen trainingsmogelijkheden bestonden in realistische stresssituaties.

Het Vast Comité I oordeelde dat het geweld in de gegeven omstandigheden 'redelijk' was, ook al was dat volgens de klaagster niet zo en ook al bleek de situatie achteraf geen reële bedreiging in te houden.

II.11. EEN KLACHT OVER EEN TUSSENKOMST VAN HET OCAD

In mei 2015 opende het Vast Comité I, samen met het Vast Comité P, een onderzoek naar de wijze waarop het OCAD een rol had gespeeld bij de intrekking van de licentie van een lijnpiloot.[113] Deze stelde zich vragen over de tussenkomst en de bevoegdheid van het OCAD. De comités waren van mening dat ze niet wettelijk bevoegd waren om de gegrondheid te beoordelen van de reden van de schorsing van de vergunning. Het onderzoek beperkte zich tot de evaluatie van de rol van het OCAD. Het onderzoek werd gefinaliseerd in december 2016.

---

111 Niveau 3 wordt toegekend wanneer de bedreiging als mogelijk en waarschijnlijk wordt beschouwd; dat vereist bijgevolg bijzondere aandacht vanwege de beschermingsagenten.

112 Tijdens de opdrachten verliep de communicatie tussen de beschermingsteams en de politiediensten via het ASTRID-netwerk. Het toezichtonderzoek in 2014 had al uitgewezen dat het communicatienetwerk in sommige delen van het land problemen kende. Zie VAST COMITÉ I, *Activiteitenverslag 2014*, 44-51 ('II. 4. De VSSE en haar wettelijke opdracht van persoonsbescherming').

113 Op basis van art. 63 W.Toezicht onthield een raadslid van deelname aan het toezichtonderzoek.

II.11.1. DE EVALUATIENOTA'S VAN HET OCAD

Begin 2010 stelt het Directoraat-generaal luchtvaart (DGLV) van de FOD Mobiliteit en Vervoer het OCAD in kennis van het feit dat een Belgisch staatsburger er mee zou gedreigd hebben een aanslag te plegen in het land waarin hij het beroep van piloot had uitgeoefend tot 1999. Zijn dreigingen zouden tot doel hebben de bevoegde overheden te dwingen hem zijn vliegvergunning terug te geven, dewelke was ingetrokken omwille van psychische redenen.

Het DGLV vroeg een dreigingsevaluatie aan het OCAD, dat snel reageerde: '*Het OCAD kan niet evalueren of (betrokkene) de vermelde bedreigingen daadwerkelijk geuit heeft. Wel zijn de aard van de bedreigingen van die aard dat de grootste omzichtigheid aan de dag moet worden gelegd, ook al wordt het uiten van de dreiging door de betrokkene tegengesproken. Er zijn – op dit ogenblik – ten andere geen elementen aanwezig om te twijfelen aan de versie van de politie*.' En verder: '*een onderzoek van de psychische toestand van betrokkene lijkt meer dan aangewezen. Als dit onderzoek aantoont dat er wel degelijk sprake is van psychische labiliteit, dan kan het OCAD niet anders concluderen dat de ernst van de dreiging als ernstig moet worden ingeschat en de waarschijnlijkheid tot het plegen van een aanslag als mogelijk. Rekening houdend met de bovenstaande elementen stelt het OCAD het niveau van de terroristische of extremistische dreiging uitgaande van betrokkene in deze hypothese vast op ERNSTIG (niveau 3)*'.

Daarop schorste de DGLV de pilotenvergunning in België van de klager. Aangezien er getwijfeld werd aan de geschiktheid van de klager om zijn vergunning te behouden, werd hem gelast zich te onderwerpen aan een medisch onderzoek. Dit vond plaats in april 2010 en besloot dat de klager over zijn vliegvergunning kon beschikken, op voorwaarde dat hij zich jaarlijks zou onderwerpen aan een psychiatrisch onderzoek.

In mei 2010 maakte het OCAD een nieuwe evaluatie. Rekening houdend met het medisch verslag werd de dreigingsevaluatie nu teruggebracht tot niveau 2. De evaluatienota vermeldt: '*de ernst van de dreiging, uitgaande van de heer X blijft, gelet op de concrete geuite bedreigingen in het verleden, door het OCAD ingeschat op ernstig. Evenwel wordt op heden de waarschijnlijkheid van de uitvoering van de dreiging, gelet op het vermeld psychiatrisch verslag, ingeschat als weinig waarschijnlijk*'. En de nota gaat verder: '*het komt in deze context evenwel wettelijk gezien niet aan het OCAD toe om advies te geven over de wenselijkheid om aan de Heer X opnieuw een vliegbrevet uit te reiken*'.

II.11.2. EEN BEVOEGDHEID VAN HET OCAD?

De bevoegdheden *rationae materiae* van het OCAD staan omschreven in artikel 3 van de Wet van 10 juli 2006 betreffende de analyse van de dreiging

(W.OCAD) en worden verduidelijkt in het Koninklijk besluit van 28 november 2006 tot uitvoering van de W.OCAD (KB OCAD). Worden beoogd, de dreigingen opgesomd in artikel 8, 1°, b) en c) W.I&V, zijnde terrorisme[114] en extremisme.[115] Bovendien moeten deze dreigingen gericht zijn tegen de integriteit van personen in België en van Belgische onderdanen in het buitenland, de kritieke nationale infrastructuur onder bepaalde voorwaarden, de gedefinieerde gebeurtenissen of groeperingen en de instellingen en Belgische belangen in het buitenland.

In zijn eerste evaluatienota meende het OCAD dat de dreiging van terroristische en extremistische aard was. Volgens de aanvankelijke informatie had de dreiging tot doel om de bevoegde overheden te dwingen om hem zijn vliegvergunning terug te geven.

Aangezien het zich genoodzaakt voelde om dringend een uitspraak te doen, verrichtte het OCAD zijn evaluatie op basis van de enige informatie-elementen die het ter kennis waren gebracht. Er werd rekening gehouden met volgende criteria:

- de ernst van de dreiging;
- de betrouwbaarheid van de informatiebron, die dadelijk als vaststaand werd beoordeeld aangezien het om een buitenlandse politiedienst ging;
- het vermogen van de klager om die dreiging ten uitvoer te brengen, dat als vaststaand werd beoordeeld gelet op zijn beroep van piloot;
- de waarschijnlijkheid dat hij de dreiging ten uitvoer zou brengen, die als positief werd beoordeeld gezien de psychische toestand van de betrokkene.

Deze elementen werden echter niet afgetoetst aan het standpunt dat de klager bleek te hebben uiteengezet aan het DGLV.

De Comités waren de mening toegedaan dat volgens de beschikbare informatie de dreigingen ingegeven waren vanuit een persoonlijke overweging, en niet vanuit enig ideologisch of politiek motief. Er was in dit geval geen sprake van een terroristische of extremistische dreiging. De wettelijke bevoegdheid van het OCAD om in deze een analyse uit te voeren, was dus niet vastgesteld. Beide Comités waren zich evenwel bewust van de moeilijke situatie waarin het OCAD zich bevond ten aanzien van de vraag van het Directoraat-generaal luchtvaart.

---

114 Artikel 8, 1°, b) W.I&V definieert terrorisme als *'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'.*

115 Artikel 8, 1°, c) W.I&V definieert extremisme als *'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'.*

II.12. INDIVIDUELE DREIGINGSEVALUATIES DOOR HET OCAD

II.12.1. ONDERZOEKSOPZET

Het OCAD heeft als taak het dreigingsniveau inzake terrorisme en extremisme te bepalen. Dit dreigingsniveau kan onder andere worden vastgesteld voor gebeurtenissen, voor plaatsen of voor individuen. In maart 2015 opende de Vaste Comités I en P een gemeenschappelijk onderzoek naar '*de wijze waarop het OCAD het dreigingsniveau bepaalt dat uitgaat van een individu of waaraan een individu blootstaat, naar de gevolgen die de bepaling van dat dreigingsniveau heeft voor de taakverdeling, de te nemen maatregelen en de informatieuitwisseling tussen de betrokken diensten, alsook naar de praktische gevolgen voor de betrokken persoon en diens opvolging*'. Dit gebeurde op verzoek van de Begeleidingscommissie van de Kamer. Deze wenste geïnformeerd te worden over volgende items:

- Welke criteria hanteert het OCAD om het dreigingsniveau te bepalen ten aanzien van een individu?
- Welke instantie legt de taken vast van de betrokken diensten eens het dreigingsniveau is bepaald?
- Welke operationele maatregelen resulteren uit een bepaald dreigingsniveau en welke dienst is belast met de coördinatie?
- Hoe zijn de informatiestromen tussen de diverse diensten geregeld?
- Wat zijn de concrete gevolgen voor een individu die het voorwerp is van een bepaald dreigingsniveau?
- Hoe wordt de 'classificatie' van dit individu opgevolgd door de lokale politionele en administratieve overheden?

In februari 2016 werd een tussentijds rapport gezonden aan de Begeleidingscommissie. In het verlengde van de werkzaamheden voor de parlementaire onderzoekscommissie 'terroristische aanslagen' werd door beide comités beslist dat het onderzoek geen actualiteitswaarde meer had en werd het onderzoek stopgezet. Hieronder worden dan ook alleen de tussentijdse onderzoeksresultaten hernomen.

II.12.2. WETTELIJK KADER

Krachtens de Wet van 10 juli 2006 betreffende de analyse van de dreiging (W. OCAD) heeft het coördinatieorgaan drie opdrachten, waaronder '*op punctuele basis een gemeenschappelijke evaluatie uit te voeren die moet toelaten te oordelen of die dreigingen gelinkt aan terrorisme en extremisme zich voordoen en welke maatregelen in voorkomend geval noodzakelijk zijn*' (art. 8, 2 W.OCAD). Het

OCAD is dus niet bevoegd om over te gaan tot evaluaties betreffende andere soorten van dreigingen dan terrorisme en extremisme.[116]

Het Koninklijk besluit tot uitvoering van de Wet van 10 juli 2006 betreffende de analyse van de dreiging (KB OCAD) bepaalt dat de evaluaties van het coördinatieorgaan betrekking moeten hebben, enerzijds, op personen, groeperingen, voorwerpen of gebeurtenissen die een terroristische of extremistische dreiging kunnen inhouden en, anderzijds, op personen, groeperingen of voorwerpen die het doelwit of het slachtoffer van een dergelijke dreiging kunnen zijn. Volledigheidshalve moet worden opgemerkt dat de dienst ook bevoegd is om dreigingsevaluaties uit te voeren voor kritieke infrastructuren.

De modaliteiten voor de evaluaties werden door de Koning bepaald. Artikel 11 § 6 KB OCAD beschrijft twee evaluatiecriteria voor het dreigingsniveau: enerzijds de ernst van het gevaar of van de dreiging en anderzijds de waarschijnlijkheid van dat gevaar of van die dreiging. Om de ernst van iedere dreiging vast te stellen (en dus ook wat personen betreft), bepaalt het OCAD een 'niveau', gaande van 1 (laag) tot 4 (zeer ernstig) (art. 11 § 6 KB OCAD).

II.12.3. DE DREIGINGSEVALUATIES VAN HET OCAD (2011-2015)

Een interne OCAD-nota uit 2011 stelde dat 'de punctuele e*valuatie […] altijd [de volgende punten omvat]: de uiteenzetting van de gebeurtenis, de beschrijving van de context (politieke situatie, historische precedenten…), de bepaling van het dreigingsniveau en, in voorkomend geval, het voorstellen van bepaalde maatregelen*'. De nota schreef ook voor dat de evaluatie het voorwerp moest uitmaken van een kwaliteitscontrole op basis van een informele peer counseling.

Uit een eerder toezichtonderzoek bleek dat er geen geformaliseerde werkwijze noch analysecriteria voorhanden waren voor de opmaak van die evaluaties.[117] Gelet op de specificiteit van elk geval en op de toepassing van 'algemene principes inzake analyse', achtte het OCAD het zelfs niet nuttig om te beschikken over een geformaliseerde evaluatieprocedure en bestond de enige kwaliteitsgarantie in de controle, door de leiding, van de conformiteit van de evaluatie met de algemene lijn van het OCAD.

Tussen 2013 en 2015 evolueerde de toestand amper. De Comités stelden vast dat het OCAD het niet noodzakelijk achtte om zijn werkwijze aan te passen.

---

116 Zo bijvoorbeeld behoren de dreigingen gelinkt aan spionage tot de bevoegdheid van de inlichtingendiensten en deze die een aanslag op de openbare orde inhouden of die gelinkt zijn aan de georganiseerde misdaad, tot de bevoegdheid van de Federale Politie.

117 VAST COMITÉ I, *Activiteitenverslag 2012*, 35-38 ('II.5. Gemeenschappelijk onderzoek naar de dreigingsevaluaties van het OCAD inzake buitenlandse VIP's op bezoek in België').

In het kader van voorliggend toezichtonderzoek analyseerden de Vaste Comités I en P een dertigtal evaluaties behorende tot zeven individuele dossiers[118] en kwamen daarbij tot volgende vaststellingen:

- tot eind 2015 werden geen formele methodologie noch duidelijke criteria gebruikt om de ernst, de waarschijnlijkheid en dus het niveau van dreiging ten aanzien van of uitgaande van personen, te bepalen. De methodologie zoals bepaald in artikel 11 § 6 KB OCAD dat twee evaluatiecriteria voor het dreigingsniveau vastlegt (*supra*), werd haast nooit expliciet toegepast;
- het OCAD leefde zelden zijn eigen regels inzake evaluatie na. De evaluaties uitgevoerd tussen 2012 en 2015 waren vaak beknopt en besteedden maar weinig aandacht aan de contextualisering. Men kon niet spreken van echte analyses;
- er werden problemen in de informatiestromen tussen de politiediensten, de gerechtelijke overheden en het OCAD vastgesteld. Bovendien verhinderde de classificatie van bepaalde informatie door de inlichtingendiensten dat ze werd verspreid en gebruikt door de overheden die belast waren met de uitvoering van de veiligheidsmaatregelen;
- zodra het Crisiscentrum dreigingsevaluaties ontvangen had, werden deze besproken met de vertegenwoordigers van de verschillende diensten en overheden. De meeste maatregelen werden gezamenlijk besproken alvorens de beslissing werd genomen door het Crisiscentrum van de regering. Daar waar het OCAD voorstellen voor maatregelen formuleerde, bleken deze vaag te zijn.

II.12.4. EEN NIEUWE METHODOLOGIE

In 2015 gelastten de Nationale Veiligheidsraad en het Strategisch comité voor inlichting en veiligheid, het OCAD en het Crisiscentrum een methodologie voor punctuele evaluaties uit te werken '*die het dreigingsniveau zo nauwkeurig mogelijk kan bepalen*'. De door beide diensten voorgestelde werkwijze onderscheidde drie types van analyses:

- de dreiging jegens personen, gebeurtenissen of belangen;
- de dreiging uitgaande van individuen en/of groepen;
- de algemene dreiging in België.

Er werd voorgesteld dat de methodologie voor de evaluatie van de dreiging voor de eerste categorie (personen, gebeurtenissen of belangen) zou berusten op de analyse van drie factoren:

[118] Deze werden geselecteerd gedurende de drie jaar volgend op het gemeenschappelijk onderzoek van beide Comités uit 2012. In de loop van die periode heeft het OCAD zowat 1000 evaluaties per jaar uitgevoerd en in 2015 zelfs meer dan 1500.

– de basisinformatie die aanleiding geeft tot de evaluatie (uit welke bron is die informatie afkomstig? Is ze betrouwbaar en geloofwaardig?);
– de waarschijnlijkheid van de informatie (informatie moet worden beoordeeld als 'zeer onwaarschijnlijk', 'onwaarschijnlijk', 'mogelijk', 'waarschijnlijk' of 'zeker);
– de graad van ernst ('zeer laag', 'laag', 'gemiddeld', 'hoog', 'zeer hoog', 'kritiek') van de impact op de veiligheid, de openbare orde, de infrastructuur, het leven van de burgers.

Aan elk van die factoren dient een score te worden toegekend en aan de hand van de combinatie van die scores op een evaluatiematrix, zal een dreigingsniveau (tussen 1 en 4) worden verkregen. Ook werden in een intern en een extern controleniveau voorzien.

Deze nieuwe methodologie, voorgesteld in oktober 2015, werd ter beoordeling voorgelegd aan de twee voogdijministers. Aangezien de methodologie niet ten uitvoer werd gelegd in de loop van voorliggend onderzoek, waren de Comités niet in staat om de toepassing ervan te beoordelen.

II.13. SPECIFIEKE DISFUNCTIES BINNEN HET OCAD

In de tweede helft van 2015 ontvingen de Vaste Comités I en P twee anonieme brieven. Ze maakten melding van 'onregelmatigheden' en 'ernstige structurele problemen' binnen het coördinatieorgaan. Wat later ontvingen de Comités nog een klacht over de interne werking van het OCAD. In oktober 2015 bundelden de Vaste Comités I en P alle kwesties in een '*gemeenschappelijk onderzoek betreffende de aangifte van interne disfuncties binnen het OCAD*'.[119]

De eerste aangifte betrof het opstellen van individuele fiches betreffende de *foreign terrorist fighters*.[120] De klager was van oordeel dat de uitvoering van deze opdracht in strijd was met zijn functie als expert. Artikel 3 KB OCAD bepaalt dat het OCAD kan beschikken over (statutaire) analisten en (gedetacheerde) experten, elk met een eigen profiel.[121] De Comités waren van mening dat het

119 Het eindrapport werd in september 2016 goedgekeurd.

120 De Omzendbrief van 21 augustus 2015 betreffende de uitwisseling van informatie en het opvolgen van FTF's geeft aan het OCAD de opdracht om een individuele inlichtingenfiche op te maken van zodra een individu opduikt als potentiële FTF. De dienst dient daarbij de nodige maatregelen te treffen om hieraan zo vlug mogelijk opvolging te geven.

121 Bijlage 3 van het KB OCAD definieert de profielen.
'De analist is, onder het gezag van de directeur OCAD of het door hem gedelegeerd departementshoofd, verantwoordelijk voor de inzameling en opzoeking van informaties en inlichtingen betreffende het fenomeen terrorisme en dit volgens een indeling in o.a. geografische, etnische en religieuze belangensferen. Daarnaast dient hij de, aan deze belangensferen gekoppelde,

opstellen van individuele fiches een punctuele evaluatie inhield van de dreiging die van elke FTF uitgaat. De toebedeling van deze taak aan de experten was dan ook niet strijdig met hun profiel. Daarnaast was het vanzelfsprekend dat ook de analisten in deze een verantwoordelijkheid toebedeeld kregen. Ook dit was niet strijdig met hun profiel. In de loop van het onderzoek kon worden vastgesteld dat de taakverdeling inzake het opstellen van de FTF-fiches tussen experten en analisten aangepast werd naar een beter evenwicht.

Een tweede luik van de aangifte betrof een onregelmatige detachering van een contractueel personeelslid van een steundienst naar het OCAD. De detachering van een contractuele agent was inderdaad niet conform artikel 83 van het Koninklijk besluit van 23 januari 2007 betreffende het personeel bij coördinatieorgaan van de dreigingsanalyse.[122, 123] Enkel een wijziging van de regelgeving zou toelaten om de detachering van contractuele personeelsleden te regulariseren.[124]

De anonieme klager haalde verder aan dat een expert een voorkeursbehandeling zou hebben genoten vanwege de directie en zou worden bevoordeeld op het vlak van vorming. De Vaste Comités I en P vonden hiervan geen indicatie.

Een andere klager haalde de – volgens hem onterechte – beslissing aan om een einde te stellen aan zijn detachering. De Vaste Comités I en P onthielden zich van een oordeel over de gegrondheid van deze beslissing. Ze moesten evenwel vaststellen dat meerdere voorafgaande incidenten de professionele en persoonlijke relatie tussen de directie en de klager hadden bemoeilijkt. Ze waren wel van

---

geopolitieke situatie grondig te analyseren volgens zijn vakspecialiteit. Hij is ook verantwoordelijk voor de inbreng van zijn verwerkte gegevens in de bestanden van de gespecialiseerde OCAD–documentatie. Hij is belast met de analyse van de ingezamelde gegevens en de verwerking ervan in periodieke, strategische evaluaties en dit in samenwerking met de experten, afgedeeld vanuit de verscheidene steundiensten'. Betrokkene neemt eveneens deel aan vergaderingen in binnen– en buitenland over terrorisme en extremisme. Hij neemt deel aan een permanentie beurtrol.

'*De expert […] is verantwoordelijk voor de inzameling en de opzoeking van informaties en inlichtingen betreffende de geopolitieke toestand en het fenomeen terrorisme […]. Hij is belast met de permanente analyse van de verkregen gegevens en verantwoordelijk voor de verwerking ervan in bruikbare, punctuele evaluaties betreffende de potentiële terroristische dreiging en dit in nauwe samenwerking met de andere experten en analisten bij OCAD*'. Tevens fungeert hij als verbindingsofficier naar zijn oorspronkelijke dienst. Hij is verantwoordelijk voor de inbreng en het actualiseren van de verwerkte gegevens in de bestanden van de gespecialiseerde OCAD–documentatie.

122 '*De betrekkingen van deskundige en de betrekkingen van administratief personeel bij het OCAD worden via detachering ingevuld door vastbenoemde ambtenaren in de ondersteunende diensten volgens een verdeling die, op voorstel van de directeur en van de adjunct-directeur, door de Nationale Veiligheidsraad vastgelegd wordt*'.

123 De directie van het OCAD wees er met aandrang op dat de detachering nooit het voorwerp heeft uitgemaakt van enig beroep en dat zij bijzonder tevreden was over het door betrokkene geleverde werk. Dit maakte de onregelmatigheid niet ongedaan.

124 De OCAD-directie nam hieromtrent een initiatief, maar kreeg hierop geen reactie van de voogdijministers.

oordeel dat de wijze waarop de formele beslissing was genomen, een miskenning inhield van een algemeen beginsel van behoorlijk bestuur. De Comités hadden evenwel niet de bevoegdheid om de beslissing ongedaan te maken of te herzien.[125]

De aangifte maakte ook melding van onnodige reizen en ongepaste internationale contacten van het OCAD. De Comités deden eerder reeds onderzoek naar deze aantijgingen.[126] De klacht droeg op dat vlak geen nieuwe elementen aan.

Wat betreft de opmerking over 'sluimerende alcoholproblemen' bij sommige personeelsleden werd de directie gevraagd om de objectieve draagwijdte van het probleem te evalueren en mee te delen welke (preventieve of disciplinaire) maatregelen er werden genomen. De Comités namen akte van de genomen maatregelen.

Ten slotte stelde de klager dat er druk op hem zou zijn uitgeoefend om hem te weerhouden voormelde disfuncties aan te kaarten. Bij gebrek aan tastbare elementen waren de Comités niet in staat zich te buigen over deze beschuldiging.

II.14. EEN KLACHT IN HET KADER VAN EEN VEILIGHEIDSONDERZOEK BIJ DE ADIV

II.14.1. CONTEXTUALISERING

In april 2015 ontving het Vast Comité I een klacht over een door de ADIV uitgevoerd veiligheidsonderzoek. Meer in het bijzonder haalde de klaagster aan dat de ADIV in het kader van zijn veiligheidsonderzoek naar haar echtgenoot foutieve informatie over haar had verwerkt. Zij meende dat haar verweten werd op een ongeoorloofde manier informatie uit de database van de Dienst Vreemdelingenzaken (DVZ) te hebben ingewonnen over een lid van Defensie waarmee haar echtgenoot in contact kwam. De klaagster ontkende dit ten stelligste. Ze specificeerde dat de ADIV persoonsgebonden informatie niet juist zou hebben gerepertorieerd in zijn gegevensbestanden en dat hierdoor haar beroepsintegriteit in twijfel werd getrokken.[127]

---

125 De Comités namen akte van het feit dat de klager geen beroep indiende bij de Raad van State of voor bevoegde rechtbanken.

126 VAST COMITÉ I, *Activiteitenverslag 2015*, 33-37 ('II.7. De internationale contacten van het OCAD').

127 Haar echtgenoot ging niet akkoord met een verminderd niveau van zijn nieuwe veiligheidsmachtiging en tekende daartegen (met succes) beroep aan bij het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen. Door deze beroepsprocedure diende het toezichtonderzoek te worden geschorst. Het onderzoek werd afgesloten in maart 2016.

II.14.2. VASTSTELLINGEN

De ADIV baseerde zich voor zijn veiligheidsonderzoek in deze enkel op gegevens dewelke conform de wettelijke bepalingen[128] verzameld werden. Het betrof enerzijds de persoonsgegevens die in de basisvragenlijst werden ingevuld door de aanvrager zelf en bij uitbreiding zijn partner en anderzijds aanvullende inlichtingen (administratieve, politionele en gerechtelijke gegevens) ingewonnen door de inlichtingendienst.[129] Er kon na inzage van het veiligheidsdossier door het Comité worden vastgesteld dat de naam van de klaagster niet voorkwam in de beslissing aangaande het veiligheidsonderzoek en dat de ADIV de integriteit van de betrokkene nooit heeft besmeurd.

II.15. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2016 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2016 WERDEN OPGESTART

II.15.1. 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 (hierover II.3). Ook het Vast Comité P startte een toezichtonderzoek op, zij het 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 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.

---

128 De Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen en de Richtlijn van 16 februari 2000 van het (toenmalige) Ministerieel Comité voor inlichtingen en veiligheid betreffende de omvang van veiligheidsonderzoeken.

129 Deze gegevens zijn uitsluitend toegankelijk voor daartoe speciaal aangeduide agenten van de ADIV en voor zover de kennisname en de toegang noodzakelijk zijn voor de uitoefening van hun functies en opdrachten om deze gegevens te behandelen in het kader van de aanvraag voor een veiligheidsmachtiging.

Omdat beide twee 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 onderzoekscommissie dat *de facto* de onderzoeksvragen overnam, achtte de Comités het hervatten van de onderzoekverrichtingen niet langer relevant.[130]

II.15.2. INTERNATIONALE GEGEVENSUITWISSELING OVER *FOREIGN TERRORIST FIGHTERS*

Tijdens een internationale vergadering met verschillende Europese toezichthouders[131] werd beslist een gelijkaardig toezichtonderzoek op te starten in alle deelnemende landen over de internationale samenwerking tussen de diverse inlichtingendiensten met betrekking tot de strijd tegen de *foreign terrorist fighters* (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[132] 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 de tweede helft van 2016 werden zowel op nationaal als op internationaal niveau diverse onderzoeksopdrachten uitgevoerd. De resultaten van het Belgisch toezichtonderzoek zullen – waar mogelijk gezien de restricties inzake classificatie – worden aangewend om het internationale onderzoek te stofferen.

---

130 De twee Comités stelden 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.

131 Het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, de Nederlandse Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD), de Zwitserse *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.

132 Het onderzoek werd opgestart eind augustus 2016, nadat het initiatief eerder werd voorgelegd aan en goedgekeurd door de Begeleidingscommissie van de Kamer van Volksvertegenwoordigers.

HOOFDSTUK III
CONTROLE OP DE BIJZONDERE INLICHTINGENMETHODEN

Dit hoofdstuk biedt een overzicht van de inzet van de bijzondere inlichtingenmethoden door de VSSE en de ADIV in 2016 en van de wijze waarop het Vast Comité I zijn jurisdictionele controletaak hierop heeft waargenomen.[133] 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.[134]

In een eerste deel wordt echter nader ingegaan op de vier wetten die in de loop van 2016 in werking zijn getreden en die een wijziging betekenden inzake de BIM-methoden. Door deze wijzigingen is het niet steeds mogelijk gebleken de cijfers van het werkingsjaar 2016 te vergelijken met die van eerdere jaren.

In dit hoofdstuk wordt om evidente redenen nog geen rekening met twee andere wetswijzigingen. Vooreerst is er de zogenaamde PNR-Wet van 25 december 2016.[135] Deze was in het refertejaar weliswaar gestemd maar nog niet in werking getreden. Ten tweede is er de ingrijpende wijziging van de BIM-regeling die in 2016 door het Parlement werd besproken maar die pas op 8 mei 2017 in werking trad.

III.1. DE VIER WETSWIJZIGINGEN UIT 2016

III.1.1. EEN NIEUWE OPDRACHT VOOR DE INLICHTINGENDIENSTEN

Bij Wet van 29 januari 2016[136] kregen beide inlichtingendiensten uitdrukkelijk de opdracht '*het inwinnen, analyseren en verwerken van inlichtingen die betrekking*

133 De BIM-Commissie staat in voor de *a priori*-controle van de inzet van bijzondere inlichtingenmethoden. Hierover: VAST COMITÉ I, *Activiteitenverslag 2010*, 55-56 ('III.1.2. De controle door de BIM-Commissie') en P. DE SMET, 'Check and balances. A priori en a posteriori controle', in VAN LAETHEM, W., VAN DAELE, D. en VANGEEBERGEN, B. (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Intersentia, Antwerpen, 2010, 93-118.

134 Ingevolge de Wet van 5 februari 2016 tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie (*BS* 19 februari 2016), waarbij artikel 35 § 2, eerste lid, W.Toezicht werd gewijzigd, zal het Comité vanaf 2016 niet meer '*om de zes maanden*' rapporteren over de toepassing van de BIM-methoden, maar wel '*jaarlijks*'.

135 Voluit de Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, *BS* 25 januari 2017. PNR staat voor *Passenger Name Record*.

136 *BS* 24 februari 2016.

hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied' (artt. 7, 3°/1; en 11 § 1, 5° W.I&V). Ingevolge artikel 18/1, eerste lid, 1° en 2° W.I&V mogen de VSSE en de ADIV in dit kader specifieke of uitzonderlijke methoden inzetten. Deze nieuwe bevoegdheid hangt in vele gevallen nauw samen met de mogelijkheid om buitenlandse inlichtingendiensten op te volgen die zich in België bezondigen aan spionage of inmenging. Het Comité merkte dan ook op dat de inlichtingendiensten in dergelijke gevallen verwezen naar deze laatste dreigingen en niet naar de nieuwe bevoegdheid. Het Vast Comité I heeft de VSSE en de ADIV hierop gewezen zodat in de toekomst een accuraat beeld kan geschetst worden van de inzet van deze nieuwe bevoegdheid.

III.1.2. DE IDENTIFICATIE VAN DE GEBRUIKER VAN TELECOMMUNICATIE OF VAN EEN GEBRUIKT COMMUNICATIEMIDDEL ALS GEWONE METHODE

Bij Wet van 5 februari 2016 tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie[137] werd – in navolging van de aanbevelingen van het Vast Comité I[138] – de identificatie van de gebruiker van telecommunicatie 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 Inlichtingenwet van 30 november 1998.

Wanneer de identificatie (en de lokalisatie) met behulp van een technisch middel verloopt – en dus niet via de vordering aan een operator – blijft de collecte een specifieke methode. Hiertoe werden de artikelen 18/2 § 1 en 18/7 § 1 W.I&V aangepast. In deze bepalingen werd ook een nieuwe specifieke methode ingeschreven: 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 via de vordering van een operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst of door een rechtstreekse toegang tot de desbetreffende bestanden.

De nieuwe 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.

137 *BS* 19 februari 2016.
138 VAST COMITE I, *Activiteitenverslag 2012*, 69.

Deze wetswijziging trad in werking op 29 februari 2016. Dit maakte het voor het Comité niet evident cijfers te produceren die een volledige vergelijking toelaten met de voorgaande jaren (zie verder onder III.2).

III.1.3. EEN NIEUWE DATARETENTIEWET MET IMPLICATIES VOOR DE INLICHTINGENDIENSTEN

Sinds de Wet van 29 mei 2016[139] wordt de verplichting voor operatoren om bepaalde metadata gedurende twaalf maanden bij te houden, gewijzigd. Deze wetswijziging was het gevolg van een uitspraak van het Europees Hof te Luxemburg en van een arrest van het Grondwettelijk Hof.

De wetswijziging had ook gevolgen voor de inzet van sommige specifieke methoden door de inlichtingendiensten. Zo werd het vorderen van bepaalde gegevens via operatoren beperkt in de tijd. Artikel 18/8 W.I&V maakt het voor beide inlichtingendiensten mogelijk '*zo nodig door daartoe de medewerking van de operator van een elektronisch communicatienetwerk of van de verstrekker van een elektronische communicatiedienst te vorderen, overgaan of doen overgaan tot: 1° het opsporen van de verkeersgegevens van elektronische communicatiemiddelen van waaruit of waarnaar elektronische communicaties worden of werden gedaan; 2° het lokaliseren van de oorsprong of de bestemming van elektronische communicaties*'. Indien de VSSE of de ADIV deze gegevens wenst te bekomen via een operator, stelt de wet volgende limieten: voor een potentiële dreiging die betrekking heeft op een activiteit die verband kan houden met criminele organisaties of schadelijke sektarische organisaties, kan het diensthoofd in zijn beslissing de gegevens slechts vorderen voor een periode van zes maanden voorafgaand aan de beslissing. Wanneer de dreiging betrekking heeft spionage, inmenging of proliferatie mag deze periode negen maanden bedragen. Voor activiteiten die verband houden met terrorisme of extremisme, bedraagt de termijn twaalf maanden voorafgaand aan de beslissing.

Deze nieuwe regeling houdt in dat ook de ADIV wettelijk verplicht is om aan te duiden binnen welk van deze concrete dreigingen zijn collecte te situeren is. Dit is nieuw in die zin dat de ADIV in zijn werking normaliter niet gebonden is door deze zeven dreigingen. In de praktijk zal er echter niet veel veranderen omdat de ADIV in zijn BIM-beslissingen steeds verwezen heeft naar een van de zeven dreigingen.

Ten slotte moet opgemerkt worden dat bij de uitwerking van deze regeling geen rekening is gehouden met de nieuwe bevoegdheid van de VSSE en de ADIV om de activiteiten van buitenlandse diensten op ons grondgebied op te volgen. Ook hier zou een maximale termijn voor kennisname van metadata moeten worden gespecifieerd.

139 *BS* 18 juli 2016.

III.1.4. DE IDENTIFICATIE VAN EEN *PREPAID*-KAARTHOUDER

Bij Wet van 1 september 2016[140] werd een nieuwe gewone methode ingevoerd in 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 eindegebruiker 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 (zie III.1.2) – een register bijhouden van alle gevorderde identificaties.

Deze regeling is pas midden december 2016 in werking getreden. Ze gaf geen aanleiding tot concrete toepassingsgevallen.

III.2. CIJFERS MET BETREKKING TOT SPECIFIEKE EN UITZONDERLIJKE METHODEN

Tussen 1 januari en 31 december 2016 werden door de twee inlichtingendiensten samen 1868 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 1747 door de VSSE (waarvan 1558 specifieke en 189 uitzonderlijke) en 121 door de ADIV (waarvan 88 specifieke en 33 uitzonderlijke).

Onderstaande tabel maakt een vergelijking met de cijfers van de afgelopen jaren.

	ADIV		VSSE		TOTAAL
	Specifieke methode	**Uitzonderlijke methode**	**Specifieke methode**	**Uitzonderlijke methode**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868

Deze cijfers duiden enerzijds op een *status quo* voor de ADIV maar anderzijds op een zeer aanzienlijke stijging (met niet minder dan 34%) voor de VSSE. Maar om een reële vergelijking met de cijfers van vorig jaar te maken, moet tevens rekening worden gehouden met de 'gewone identificaties via de operator' die sinds 29 februari 2016 niet langer als een specifieke methode wordt beschouwd (zie III.1.2).

140 *BS* 7 december 2016.

Vanaf maart 2016 werden door de VSSE niet minder dan 2203 vorderingen aan operatoren gericht en door de ADIV 216. Een vergelijking met de cijfers van 2015 toont aan dat dit zou overeenkomen met meer dan 1700 methoden van 'identificaties via operatoren' voor de VSSE en om en bij de 60 voor de ADIV.[141] In 2015 zette de VSSE slechts een fractie in van deze methoden. Er werden amper 663 'identificaties' toegelaten.[142] Uit deze enorme stijging in 2016 mag zeker niet worden afgeleid dat de versoepelde procedure aanleiding heeft gegeven tot een ondoordacht gebruik van deze methode. De maandcijfers van de vorderingen aan de operatoren over de periode 2015 en 2016 tonen immers aan dat de grote stijging in het aantal identificaties verband houden met de aanslagen in Parijs en deze in Zaventem en Maalbeek.

In wat volgt, worden, per dienst, drie rubrieken onderscheiden: cijfers over de specifieke methoden, cijfers over de uitzonderlijke methoden en cijfers inzake de dreigingen en de te verdedigen belangen die door de methoden geviseerd worden.

III.2.1. METHODEN MET BETREKKING TOT DE ADIV

III.2.1.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	14	7	4	2
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0	0	0	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	0	0	0	0
Kennisnemen van identificatiegegevens van elektronisch communicatieverkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	66 methoden	67 methoden	55 methoden	–[143]

141 De inzet van één identificatiemethode impliceert doorgaans immers meerdere vorderingen aan verschillende Belgische operatoren.

142 De ADIV zette deze methode in 2015 55 maal in.

143 Vanaf 29 februari 2016 is deze methode enerzijds verengd tot '*de identificatie of de lokalisatie, 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 anderzijds verruimd tot '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'* (zie hierover III.1.2).

AARD SPECIFIEKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Kennisnemen van identificatiegegevens van elektronisch communicatieverkeer via technisch middel; of vordering van een operator i.v.m. betaalmiddel- of wijze van gebruiker	–	–	–	12 methoden
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	15	12	12	42
Kennisnemen van lokalisatiegegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	36	28	16	32
TOTAAL	**131**[144]	**114**	**87**	**88**

Dat het aantal 'kennisnames van identificatiegegevens' vorige jaren hoger lag, heeft uitsluitend te maken met het feit dat de identificaties via operatoren vanaf februari 2016 als een gewone methode wordt beschouwd (III.1.2). Een benaderende vergelijking met vorig jaar laat een lichte stijging zien. Het aantal 'kennisnames van oproepgegevens' en het aantal 'lokalisaties' steeg echter veel meer: er viel respectievelijk een verdrievoudiging en een verdubbeling te noteren. Ook de gemiddelde duur waarop de lokalisatie betrekking had, nam gevoelig toe (van 164 naar 201 dagen).

Deze cijfers tonen aan dat de in 2014 en 2015 geobserveerde tendens waarbij minder gebruik werd gemaakt van identificaties en lokalisaties, zich niet doorzet.

III.2.1.2. Uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	1	1	3	1
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	0	1	0	0
Oprichten en gebruiken van een fictieve rechtspersoon	0	0	0	0

144 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

AARD UITZONDERLIJKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	0	0	0	1
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	5	5	3	11
Binnendringen in een informaticasysteem	0	03	3	4
Afluisteren, kennisnemen en opnemen van communicaties	17	26	25	16
TOTAAL	**23**[145]	**36**	**34**	**33**

Wat betreft de uitzonderlijke methoden moet vastgesteld worden dat het aantal tapmaatregelen significant daalde, terwijl er veel meer bankgegevens werden opgevraagd.

III.2.1.3. De belangen en dreigingen die de inzet van de bijzondere methoden rechtvaardigen[146]

Sinds de inwerkingtreding van de Wet van 29 januari 2016 aangaande het toezicht op de activiteiten van de buitenlandse inlichtingendiensten in België (zie III.1.1) mag de ADIV specifieke en de uitzonderlijke methoden aanwenden in het kader van vier in plaats van drie opdrachten:

- de inlichtingenopdracht die gericht is op dreigingen tegen onder meer de onschendbaarheid van het nationaal grondgebied, de militaire defensieplannen en het wetenschappelijk en economisch potentieel op vlak van defensie (art. 11, 1° W.I&V);
- de opdracht inzake de militaire veiligheid die bijvoorbeeld gericht is op het behoud van de militaire veiligheid van het defensiepersoneel, van de militaire installaties en de militaire informatica- en verbindingssystemen (art. 11, 2° W.I&V);
- de bescherming van militaire geheimen (art. 11, 3° W.I&V);
- 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). Dit betreft de nieuwe opdracht waarbij bijzondere inlichtingenmethoden kunnen worden ingezet.

145 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

146 Per toelating kunnen meerdere belangen en dreigingen aan de orde zijn.

AARD VAN DE OPDRACHT	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Inlichtingenopdracht	111	109	112	64
Militaire veiligheid	15	5	6	1
Bescherming geheimen	28	36	4	1
Activiteiten buitenlandse diensten in België opvolgen	–	–	–	Niet gekend

AARD DREIGING	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Spionage	94	123	101	55
Terrorisme (en radicaliseringsproces)	6	7	4	5
Extremisme	24	15	13	6
Inmenging	1	0	4	0
Criminele organisatie	16	2	0	0
Andere	13	0	0	0

Ondanks het feit dat het aantal methodes gelijk is gebleven, laten de cijfers inzake de 'aard van de opdracht' en 'aard van de dreiging' over de hele lijn een gevoelige daling zien. Dit is louter te wijten aan een andere registratiewijze. De nominale cijfers liggen beduidend lager maar de onderlinge verhoudingen bleven nagenoeg dezelfde. Qua inzet van bijzondere methoden blijft voor de ADIV spionage de voornaamste dreiging.

III.2.2. METHODEN MET BETREKKING TOT DE VSSE

III.2.2.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	109	86	86	125
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0	0	0	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	0	0	0	0

AARD SPECIFIEKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Kennisnemen van identificatiegegevens van elektronisch communicatie-verkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	613 methoden	554 methoden	663 methoden	–[147]
Kennisnemen van identificatiegegevens van elektronisch communicatieverkeer via technisch middel; of vordering van een operator i.v.m. betaalmiddel- of wijze van gebruiker	–	–	–	215 methoden
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	136	88	33	622
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator	244	248	361	596
TOTAAL	**1102**	**976**	**1143**	**1558**

Eerder werd reeds aangegeven dat het globale aantal toelatingen met betrekking tot de inzet van specifieke methoden door de VSSE uitermate sterk is toegenomen. Bovenstaande tabel maakt duidelijk dat dit *quasi* volledig toe te schrijven is aan de 'kennisname van oproepgegevens' die steeg van amper 33 gevallen in 2015 naar 622 in 2016. Maar ook het aantal observaties en lokalisaties nam toe. Ten slotte kende ook de 'identificaties' – die vanaf februari 2016 als een gewone methode worden beschouwd indien zij gebeuren via een operator – een sterke groei. Op basis van de beschikbare gegevens schat het Comité het aantal ingezette identificaties op meer dan 1700.

De sterke stijging van het aantal ingezette specifieke methoden loopt uiteraard samen met de golf van terroristische aanslagen.

147 Vanaf 29 februari 2016 is deze methode enerzijds verengd tot '*de identificatie of de lokalisatie, 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 anderzijds verruimd tot '*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*' (zie hierover III.1.2).

III.2.2.2. De uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	6	9	6	7
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	6	21	8	18
Oprichten en gebruiken van een fictieve rechtspersoon	0	0	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	6	18	5	8
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	11	8	6	6
Binnendringen in een informaticasysteem	12	18	16	27
Afluisteren, kennisnemen en opnemen van communicaties	81	86	87	123
TOTAAL	**122**	**156**[148]	**128**	**189**

De talrijke aanslagen in binnen- en buitenland hebben de daling in het aantal toegepaste uitzonderlijke methoden die in 2015 te noteren viel, omgezet in een sterke stijging. Vooral het aantal doorzoekingen (van 9 naar 22), intrusies in IT-systemen (van 16 naar 27) en tapmaatregelen (van 91 naar 123) was hiervoor verantwoordelijk. Er waren niet alleen meer maatregelen, hun gemiddelde duur was ook beduidend langer.

III.2.2.3. De dreigingen en belangen die de inzet van de bijzondere methoden rechtvaardigen

De volgende tabel toont in het kader van welke (potentiële) dreigingen de VSSE specifieke en uitzonderlijke toelatingen verleende. Uiteraard kan één methode gericht zijn tegen meerdere dreigingen. De VSSE kan de specifieke methoden aanwenden in het kader van alle dreigingen die tot haar bevoegdheid behoren (art. 8 W.I&V). De uitzonderlijke methoden mochten in 2016 nog niet ingezet worden in het kader van het extremisme en de inmenging (dit is vanaf 2017 wel mogelijk). Zij zijn wel toegelaten in het kader van het aan het terrorisme vooraf-

[148] In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

gaande radicaliseringsproces (art. 3, 15° W.I&V). 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;
3. 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
4. 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;
5. 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;
6. 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;
7. inmenging: de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden;
8. 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 commerciele 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 29 januari 2016 aangaande het toezicht op de activiteiten van de buitenlandse inlichtingendiensten in België (zie III.1.1) mag de VSSE de specifieke en uitzonderlijke methoden ook inzetten bij '*het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied*' (art. 7, 3/1° W.I&V).

In acht genomen dat per toelating verschillende dreigingen aan de orde kunnen zijn, komen we tot volgende cijfers:

AARD DREIGING	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
Spionage	359	319	253	209
Terrorisme (en radicaliseringsproces)	580	499	812	684
Extremisme	246	267	171	67
Proliferatie	15	33	30	6
Schadelijke sektarische organisaties	9	0	0	0
Inmenging	8	10	10	15
Criminele organisaties	9	8	0	0
Activiteiten buitenlandse diensten in België opvolgen[149]	–	–	–	Niet gekend

Bovenstaande cijfers tonen aan dat 'terrorisme', wat betreft de inzet van BIM-methoden, de absolute prioriteit wegdraagt van de VSSE.[149]

De bevoegdheid van de VSSE wordt niet alleen bepaald door de aard van de dreiging. De dienst mag slechts optreden ter vrijwaring van welbepaalde belangen:

– de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde zijnde,
  a) de veiligheid van de instellingen van de Staat en het vrijwaren van de continuïteit van de regelmatige werking van de rechtsstaat, de democratische instellingen, de elementaire beginselen die eigen zijn aan iedere rechtsstaat, alsook de mensenrechten en de fundamentele vrijheden;
  b) de veiligheid en de fysieke en morele vrijwaring van personen en de veiligheid en de vrijwaring van goederen;
– de uitwendige veiligheid van de Staat en de internationale betrekkingen: het vrijwaren van de onschendbaarheid van het nationaal grondgebied, van de soevereiniteit en de onafhankelijkheid van de Staat, van de belangen van de landen waarmee België gemeenschappelijke doeleinden nastreeft, alsook van

149 Deze bevoegdheid werd pas ingevoegd bij Wet van 29 januari 2016 (zie III.1.1).

de internationale en andere betrekkingen die België met vreemde Staten en internationale of supranationale instellingen onderhoudt;
– de vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

In acht genomen dat per toelating verschillende belangen aan de orde kunnen zijn, komen we tot volgende cijfers voor 2016:

AARD BELANG	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde	1177	1100	1258	968
De uitwendige veiligheid van de Staat en de internationale betrekkingen	1160	1075	1150	927
De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel	11	10	4	13

III.3. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS JURDISCTIONEEL ORGAAN EN ALS PREJUDICIEEL ADVIESVERLENER

III.3.1. DE CIJFERS

In dit onderdeel wordt ingegaan op de activiteiten van het Vast Comité I met betrekking tot de specifieke en uitzonderlijke inlichtingenmethoden. Daarbij zal uitsluitend aandacht besteed worden aan de ter zake genomen jurisdictionele beslissingen. Vooraf dient evenwel te worden onderlijnd dat het Comité *alle* toelatingen tot de inzet van bijzondere methoden aan een *prima facie*-onderzoek onderwerpt, en dit met het oog op de al dan niet vatting.

Artikel 43/4 W.I&V stelt dat het Vast Comité I op vijf manieren kan worden gevat:
– op eigen initiatief;
– op verzoek van de Commissie voor de bescherming van de persoonlijke levenssfeer;
– op klacht van een burger;
– van rechtswege als de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden;
– van rechtswege als de bevoegde minister een toelating heeft verleend op basis van artikel 18/10 § 3 W.I&V.

Daarnaast kan het Comité ook gevat worden in zijn hoedanigheid van 'prejudicieel adviesverlener' (art. 131*bis*, 189*quater* en 279*bis* Sv.). In dat geval geeft het Comité een advies over de al dan niet rechtmatigheid van aan de hand van specifieke of uitzonderlijke methoden ingewonnen inlichtingen die in een strafzaak worden gebruikt. De beslissing om een advies te vragen berust bij de onderzoeksgerechten of de strafrechters. Strikt genomen treedt het Comité alsdan niet op als jurisdictioneel orgaan.

WIJZE VAN VATTING	AANTAL 2013	AANTAL 2014	AANTAL 2015	AANTAL 2016
1. Op eigen initiatief	16	13[150]	16	3
2. Privacycommissie	0	0	0	0
3. Klacht	0	0	0	1
4. Schorsing door BIM-Commissie	5	5	11[151]	[19]
5. Toelating minister	2	1	0	0
6. Prejudicieel adviesverlener	0	0	0	0
TOTAAL	**23**	**19**	**27**	**23**

Deze tabel laat één opmerkelijke evolutie zien: het Vast Comité I heeft zich in aanzienlijk minder gevallen gevat, zeker rekening houdend met het toegenomen aantal bijzondere inlichtingenmethoden. Zo vatte het Comité zich in 2015 nog in 1,1% van de dossiers terwijl dit in 2016 beperkt bleef tot 0,15%. Hiervoor zijn twee redenen aan te halen. Vooreerst blijkt uit de *prima facie*-controle die binnen het Comité op elk BIM-dossier wordt uitgevoerd, dat de twee inlichtingendiensten terdege rekening houden met de beperkingen van de wet, met de beslissingen van de BIM-Commissie en met de rechtspraak van het Comité. De andere reden is het feit dat de BIM-Commissie vaker overgaat tot een schorsing van mogelijk problematische methoden (19 gevallen). Zoals uit de volgende tabel blijkt, heeft het Comité wel in 11 van die 19 gevallen de schorsing door de Commissie (gedeeltelijk) herroepen.

Ook interessant te vermelden is de klacht door een burger, die voor het eerst sinds de invoering van deze mogelijkheid in 2010, geleid heeft tot een uitspraak van het Comité. Omwille van het belang van deze zaak wordt er verder uitgebreid aandacht aan besteed (zie verder).

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.

150 In twee gevallen viel de beslissing van het Comité pas in januari 2015.

151 In één dossier vond de vatting plaats in 2015 maar viel de beslissing van het Comité in 2016.

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). Behoudens in het klachtdossier – waarin de zaak diende te worden uitgesteld – werd die termijn in alle dossiers gerespecteerd.

AARD VAN DE BESLISSING	2013	2014	2015	2016
Beslissingen voorafgaand aan de vatting				
1. Nietige klacht	0	0	0	0
2. Kennelijk ongegronde klacht	0	0	0	0
Tussenbeslissingen				
3. Schorsing methode	0	3	2	1
4. Bijkomende informatie van BIM-Commissie	0	0	0	0
5. Bijkomende informatie van inlichtingendienst	0	1	1	4
6. Onderzoeksopdracht Dienst Enquêtes	50	54	48	60
7. Horen BIM-Commissieleden	0	0	2	0
8. Horen leden inlichtingendiensten	0	0	2	0
9. Beslissing m.b.t. geheim van onderzoek	0	0	0	0
10. Gevoelige informatie tijdens verhoor	0	0	0	0
Eindbeslissingen				
11. Stopzetting methode	9	3	3	6
12. Gedeeltelijke stopzetting methode	5	10	13	4
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	2	0	4	11
14. Onbevoegd	0	0	0	0
15. Wettige toelating / Geen stopzetting methode / Ongegrond	7	4	6	2
Prejudicieel advies				
16. Prejudicieel advies	0	0	0	0

III.3.2. DE RECHTSPRAAK

Hieronder wordt de essentie weergegeven van de eindbeslissingen die het Vast Comité I in 2016 nam. De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk wor-

den opgenomen. Het Comité diende hierbij de nodige omzichtigheid aan de dag te leggen omdat vele beslissingen werden geclassificeerd (zestien als VERTROUWELIJK en vier als GEHEIM).

De beslissingen werden gegroepeerd onder vijf rubrieken:
- motivering van de toelating;
- de proportionaliteits- en de subsidiariteitseis;
- wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging;
- de gevolgen van een onwettig(e) (uitgevoerde) methode;
- de jurisdictionele beslissing met betrekking tot de klacht.

Indien relevant werden sommige beslissingen onder meerdere rubrieken opgenomen.

III.3.2.1. Motivering van de toelating

In vier onderscheiden gevallen moest het Comité oordelen of een toelating tot het uitvoeren van een methode voldoende was gemotiveerd, en dit zowel in feite als in rechte.

In een eerste dossier wou een inlichtingendienst overgaan tot de kennisname van '*les données de connexion du passé (dont notamment des adresses IP) sur des comptes [d'un réseau social] utilisés par un target et que la période était limitée à 90 jours précédents la notification à la Commission BIM*'[152] (dossier 2016/4542). De inlichtingendienst had dit gekwalificeerd als een kennisname van oproepgegevens. Het Comité merkte op dat '*les méthodes s'apparentent plus à une localisation de l'origine ou de la destination de communications électroniques qu'à une identification et un repérage (…); que cependant la localisation est également une méthode spécifique dont les conditions sont identiques à celles applicables à l'identification et au repérage et qu'en conséquence le changement (éventuel) de "qualification" n'a pas d'incidence en terme de légalité*'.[153] De methode was dan ook niet onwettig.

In het tweede dossier werd de 'motivering in feite' beoordeeld. Een buitenlandse inlichtingendienst vraagt zijn Belgische partnerdienst om een kennisname en een lokalisatie te verrichten op Belgische telefoonnummers van waaruit tweemaal doodsbedreigingen zouden zijn geuit tegen buitenlandse hoogwaardigheids-beklederS. De BIM-Commissie schorste de methode omdat de tekst en de

---

152 '*data over connecties uit het verleden (waaronder met name IP-adressen) met betrekking tot [sociaal netwerk]-accounts gebruikt door een target waarbij de periode beperkt was tot 90 dagen voorafgaand aan de kennisgeving aan de BIM-Commissie' (vrije vertaling).*

153 '*de methoden meer lijken op een lokalisatie van de oorsprong of van de vernietiging van elektronische communicatie dan op een identificatie en een kennisname (…); dat nochtans de lokalisatie ook een specifieke methode is waarvan de voorwaarden identiek zijn aan deze die van toepassing zijn op de identificatie en de kennisname en dat bijgevolg de (eventuele) wijziging van 'kwalificatie' geen invloed heeft op de wettigheid*' (vrije vertaling).

geest van de BIM-Wet vereisen dat in de beslissing meer precieze aanwijzingen worden gegeven over de link met 'terrorisme' als een van de op te volgen dreigingen (dossier 2016/4707). Het Comité vroeg hieromtrent bijkomende informatie aan de Belgische dienst. Daaruit bleek niet rechtstreeks de link met terrorisme. Maar het Comité stelde dat '*dans les circonstances actuelles, des menaces de mort adressées par deux fois à des personnes proches du gouvernement […] d'un pays européen, même si à ce stade, celles-ci ne sont pas très caractérisées, peuvent être considérées comme relevant du "terrorisme" au sens de l'article 8-1° al 2 – b*'.[154]

In een ander dossier was er onduidelijkheid over de exacte bedoeling van de inlichtingendienst. Verwijzend naar artikel 18/16 W.I&V wilde een inlichtingendienst in een bepaald communicatietoestel software plaatsen om de aard van de communicaties in kaart te brengen én om gesprekken af te luisteren (dossier 2016/5365). Omdat het afluisteren van gesprekken valt onder artikel 18/17 W.I&V werd er meer uitleg gevraagd aan de betrokken inlichtingendienst. Hieruit bleek dat het *niet* de bedoeling was om ook effectief af te luisteren. Het Comité besloot daarom dat de methode '*wettig is, voor zover de beoogde methode niet het afluisteren, kennisnemen of registreren van communicaties op het oog heeft*'.

Het laatste geval had betrekking op de vraag of de inlichtingendienst een groep buitenlanders mocht opvolgen die in België verbleven (dossiers 2016/4875 en 2016/4877). Deze personen, die in hun land van herkomst een belangrijke functie bekleedden of bekleed hadden, werden verondersteld lid te zijn van een bepaalde beweging. De inlichtingendienst baseerde zich in zijn beslissing op 'inmenging' als dreiging en zette de motieven uiteen die aantoonden dat hij belang had bij de opvolging. De BIM-Commissie en het Comité vonden dit echter onvoldoende: '*Attendu qu'il échet de constater que, aussi bien la menace identifiée que les motifs sont loin d'être exposés d'une manière optimale puisque, par exemple [l'organisation dont dépende le groupe] est décrite comme une organisation sectaire en faisant simplement référence à une étude réalisée à l'étranger et que l'ingérence (réelle ou potentielle) n'est pas caractérisée à suffisance à défaut d'identifier les moyens illicites trompeurs ou clandestins*'.[155] Het Comité vroeg daarom bijkomende informatie. '*Attendu qu'à l'issue d'une enquête complémentaire, le Comité permanent R n'a, en principe, pas à substituer une motivation plus adéquate de la méthode sollicitée à la motivation insuffisamment étayée du service; que cependant dans le cas d'espèce, et vu notamment que [l'organisation] constitue un mouvement*

---

154 '*in de huidige omstandigheden, doodsbedreigingen tot tweemaal toe geformuleerd tegen personen uit de omgeving van de regering […] van een Europees land, kunnen beschouwd worden als 'terrorisme' in de zin van artikel 8, 1°, tweede lid, b, ook al zijn ze momenteel niet zeer uitgesproken.*'

155 '*Overwegende dat moet vastgesteld worden dat zowel de geïdentificeerde bedreiging als de motieven verre van optimaal werden weergegeven aangezien bijvoorbeeld [de organisatie waarvan de groep afhangt] wordt omschreven als een sektarische organisatie door eenvoudigweg te verwijzen naar een buitenlandse studie en dat de (reële of potentiële) inmenging onvoldoende werd aangetoond omdat de ongeoorloofde, bedrieglijke of clandestiene middelen niet werden geïdentificeerd*'. (vrije vertaling).

[…] qui tente de s'installer en Europe occidentale et entre autres en Belgique et qui est relativement récent et donc moins connu que d'autres mouvements [similaires], le Comité permanent R a décidé de demander des informations complémentaires. Celles-ci l'amènent à considérer que la méthode spécifique peut-être autorisée'.[156] Er waren immers voldoende elementen voorhanden die niet alleen wezen op 'inmenging' maar ook op 'extremisme'. '*Attendu en conséquence que la méthode est légale pour les motifs tels que requalifiés*'.[157]

III.3.2.2. De proportionaliteits- en de subsidiariteitseis

Een methode dient niet alleen te voldoen aan een aantal wettelijke vereisten, ze moet ook in verhouding staan tot de onderliggende dreiging en ze mag niet intrusiever zijn dan noodzakelijk.

De toets van deze proportionaliteits- en subsidiariteitseis was aan de orde in het hogervermelde dossier 2016/4707. Een buitenlandse inlichtingendienst had zijn Belgische zusterdienst gevraagd om een kennisname en een lokalisatie te verrichten op Belgische telefoonnummers van waaruit tweemaal doodsbedreigingen zouden zijn geuit tegen buitenlandse regeringsleden. Het Comité stelde dat '*la méthode projetée devrait permettre d'objectiver les menaces puisque les méthodes ordinaires ne sont pas suffisantes et que la méthode en question a un caractère limité d'intrusion dans la vie privée de personnes; Attendu que l'éventuelle décision de recours à d'autres méthodes concernant ces numéros de GSM ou leurs utilisateurs devra préciser plus amplement en quoi les menaces ont un caractère terroriste; Attendu en conséquence que la méthode spécifique visée est légale en ce compris le principe de proportionnalité et de subsidiarité*'.[158]

De vraag naar de proportionaliteit kwam ook aan bod in dossier 2016/4785. Een inlichtingendienst wou de oproepgegevens opsporen van het communicatiemiddel van zijn target, maar ook van enkele van zijn familieleden. Gelet op de gegeven motivatie en de verstrekte informatie bleek de methode gerechtvaardigd ten aanzien van de target. '*Dat evenwel het opsporen van de oproepgegevens van*

---

156 '*Overwegende dat na een bijkomend onderzoek, het Comité in principe geen meer adequate motivering van de gevraagde methode in de plaats kan stellen van de gebrekkige motivering zoals aangebracht door de dienst; dat echter in voorliggend geval, en vooral gezien de ([organisatie] een beweging vormt […] die zich tracht te vestigen in West-Europa en onder meer in België en die relatief nieuw is en dus minder gekend als andere (gelijkaardige) bewegingen, het Vast Comité I besliste om bijkomende informatie te vragen. Deze leiden het Comité ertoe om te overwegen dat de specifieke methode mag worden toegelaten*'. (vrije vertaling).

157 '*Overwegende dat bijgevolg de methode legaal is voor de motieven zoals die werden geherkwalificeerd*'. (vrije vertaling).

158 '*de voorgestelde methode moest toelaten om de dreigingen te objectiveren omdat gewone methoden ontoereikend zijn en dat de betrokken methode beperkt is qua intrusie in de privacy van personen; Overwegende dat de eventuele beslissing om een beroep te doen op andere methoden betreffende die gsm-nummers of hun gebruikers meer in detail moet preciseren waarom de dreigingen een terroristisch karakter hebben; Overwegende bijgevolg dat de betrokken specifieke methode wettig, proportioneel en subsidiair is.' (vrije vertaling).*

de […] familieleden gemotiveerd wordt door de mogelijkheid dat de target een telefoontoestel van één van zijn familieleden kan gebruiken.' Desgevraagd beschikte de betrokken dienst niet over concrete aanwijzingen dat de target de telefoontoestellen van zijn familieleden zou gebruiken. Het Comité achtte het gebruik van de beoogde methode ten aanzien van deze familieleden dan ook niet proportioneel.

III.3.2.3. Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging

De inlichtingendiensten kunnen uiteraard niet zomaar elke techniek aanwenden om bij wie dan ook informatie in te winnen. De wet stelt duidelijke grenzen en dit op diverse niveaus: voor welke dreiging en ter verdediging van welk belang mag een methode worden aangewend? Welke handelingen mogen daarbij gesteld worden en welke niet? Door wie, ten aanzien van wie én ten aanzien van welke gegevens? Hoelang mag een techniek worden aangewend? Mogen de maatregelen buiten België worden toegepast?… In enkele beslissingen verduidelijkte het Vast Comité I bepaalde van deze grenzen.

III.3.2.3.1. Een inlichtingenfinaliteit en geen gerechtelijke finaliteit

De BIM-Commissie had een methode geschorst omdat de inlichtingendienst in zijn beslissing had opgetekend dat de resultaten van de methoden '*dienen om het inlichtingendossier (…) af te ronden zodat deze kunnen toegevoegd worden aan een ander lopende gerechtelijk onderzoek (…) waarbij de VSSE technisch assistent is*' (dossier 2016/4414). De BIM-Commissie stelde terecht dat het niet tot de taak van een inlichtingendienst behoort om inlichtingen te verzamelen die moeten dienen om een gerechtelijk dossier te stofferen. Het Comité vroeg echter nadere uitleg aan de betrokken dienst. Deze stelde dat de motivering te summier was. Uit de verstrekte informatie bleek dat het de bedoeling was om inzicht te krijgen in een bepaald netwerk. De dienst had dus wel degelijk een inlichtingenfinaliteit voor ogen zodat de methode als wettig werd aanzien.

III.3.2.3.2. De grenzen van de opdrachten van de inlichtingendiensten

De inlichtingendienst wenste te achterhalen welk communicatiemiddel een groep personen gebruikte om hen nadien te kunnen lokaliseren (dossier 2016/4633) en observeren (dossier 2016/4634). Het betrof personen die in hun land van oorsprong deel uitmaakten van een politieke oppositiebeweging en die in België het statuut van vluchteling hadden aangevraagd. De dienst was van oordeel dat die politieke beweging '*de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, alsook de uitwendige veiligheid van de*

staat en de internationale betrekkingen bedreigt of zou kunnen bedreigen'. Het Comité merkte op dat de dienst hiermee wel verwees naar een te beschermen belang, maar dat in de beslissing nergens afdoende een bedreigende activiteit (spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties, criminele organisaties) was aangetoond, behoudens een enkele vermelding dat de betrokken groepering er 'sektarische praktijken' op nahield. De beslissing vermeldde wel dat de organisatie ervan verdacht werd '*van te pogen het […] staatsapparaat [van hun land van herkomst] binnen te dringen*', en dat de organisatie anderzijds een invloed trachtte uit te oefenen zowel op de diaspora als op de Belgische politieke verantwoordelijken. Het Comité oordeelde '*dat deze motivering geenszins voldoet aan de definitie van inmenging, nu volgens de wet inmenging het volgende inhoudt: 'de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden*.' De dienst was dan ook niet bevoegd om ter zake inlichtingen in te winnen.

III.3.2.3.3. De grenzen van de methode om bankgegevens op te vragen

De betrokken inlichtingendienst wenste de titularis van een bankrekeningnummer te achterhalen (dossier 2016/4688). Wanneer de dienst te weten komt dat die persoon een storting heeft gedaan op de rekening van een firma, wil hij gedurende een bepaalde periode alle stortingen op het bankrekeningnummer van de firma nagaan. Hij baseert zich hiervoor op artikel 18/15 § 1 W.I&V: '*In het belang van de uitoefening van hun opdrachten kunnen de inlichtingen- en veiligheidsdiensten gemachtigd worden de volgende inlichtingen te vorderen: 1° de lijst van bankrekeningen (…), waarvan de geviseerde persoon titularis, gevolmachtigde of de uiteindelijke gerechtigde is, en, in voorkomend geval, alle gegevens hieromtrent; 2° de bankverrichtingen die in een bepaald tijdvak zijn uitgevoerd op een of meer van deze bankrekeningen of financiële instrumenten, met inbegrip van de bijzonderheden betreffende iedere rekening van herkomst of bestemming*'. Het Comité merkte op dat deze bepaling niet toelaat bankgegevens van een derde op te vragen; dit is enkel toegelaten ten aanzien van '*de geviseerde persoon*'. Het Comité besloot dan ook dat *'aldus de wet niet toelaat dat een bankrekening van een derde (in casu de firma) wordt onderzocht, om uiteindelijk de geviseerde persoon te identificeren*'.

III.3.2.3.4. Onduidelijkheid over de duur van een methode

In de beslissing tot aanwending van een specifieke methode werd enerzijds vermeld dat ze kon ingezet worden 'v*oor de periode vanaf [welbepaalde datum] tot en met [welbepaalde datum]'* en anderzijds dat ze *'kan worden uitgevoerd gedurende drie maanden vanaf de beslissing van het diensthoofd en na kennisgeving van deze beslissing aan de commissie.'* Er was in deze geen duidelijkheid over de aanvangs- en de einddatum. Het Comité oordeelde dat de aanvangsdatum samenviel met de dag waarop de kennisgeving aan de Commissie gebeurde. Verder stelde het

Comité dat in geval van '*tegenstrijdigheid van data […] voor de kortste periode dient te worden gekozen*' (dossier 2016/4515).

III.3.2.3.5. De berekening van de nieuwe termijn *ex* artikel 18/8 W.I&V

In het kader van een mogelijke spionage besliste een inlichtingendienst op een bepaald ogenblik via een operator over te gaan tot de kennisname van oproepgegevens voor een periode van negen maanden die zich volledig situeerde vóór de aanvraag (dossier 2016/5266). Op dat ogenblik was het desbetreffende artikel 18/8 W.I&V gewijzigd in die zin dat voor deze dreiging '*het diensthoofd in zijn beslissing de gegevens [kan] vorderen voor een periode van negen maanden voorafgaand aan de beslissing*' [onze onderlijning]. Het Comité stelde daarop dat '*sous peine de vider le texte de sa portée, le terme "préalable" ['voorafgaand' in de Nederlandse versie, nvda] doit être compris comme instituant la date de décision […] comme un point de départ non inclus dans le calcul du délai légal visé.*'[159] *In casu* betekende dit dat de methode betrekking had op een periode die één dag te lang was.

III.3.2.3.6. Een onvolledige vordering

Het Comité diende in twee dossiers tussen te komen omdat de vordering aan de operatoren niet volledig bleek.

Zo wenste een inlichtingendienst oproepgegevens te bekomen voor een periode van 90 dagen (dossier 2016/4542). In de vordering die naar de *provider* was verzonden, was echter geen melding gemaakt van die limiet. De inlichtingendienst was immers van oordeel dat de betrokken *provider* die gegevens maar 90 dagen bijhield. Dit bleek niet zo te zijn en de dienst kreeg gegevens voor een heel jaar. Ook al gaf de dienst te kennen deze gegevens niet te zullen gebruiken, toch schorste de BIM-Commissie de methode en besloot het Comité dat de methode gedeeltelijk onwettig was.

In een andere zaak beschikte een inlichtingendienst over buitenlandse telefoonnummers die toebehoorden aan personen die gelinkt waren met een terroristische groepering (dossier 2016/4838). Via een kennisname en een lokalisatie van de oproepgegevens wenste hij te achterhalen of deze personen gedurende een bepaalde maand contacten hebben gehad in België. De vordering aan de operator vermeldde echter niet dat de methode beperkt was tot 'Belgische contacten'. Daarop schorste de Commissie de methode. Het Comité onderzocht de zaak en stelde vast dat de operator alle informatie die in zijn bezit was, had doorgezonden. Geen van deze gegevens had betrekking op een Belgisch nummer of een contact dat in België kon gesitueerd worden. Het Comité besliste daarop het volgende: '*Attendu que les méthodes sont légales dans la mesure où elles visent les contacts en*

[159] '*om de tekst van de wet te respecteren, de term "préalable" ['voorafgaand' in de Nederlandse versie, nvda] moet begrepen worden in die zijn dat de datum waarop de beslissing is genomen […] geldt als vertrekpunt dat niet begrepen is in de bedoelde wettelijke termijn.*' (vrije vertaling).

Belgique de numéros étrangers utilisés à l'étranger; Attendu que cependant l'exécution des méthodes est illégale dans la mesure où le réquisitoire transmis à l'opérateur n'est pas conforme à la décision […] puisqu'il n'est pas limité aux contacts belges'.[160]

III.3.2.3.7. De BIM-Wet en het Verdrag van Wenen inzake diplomatiek verkeer van 18 april 1961

Een dienst wilde een aantal methoden inzetten die betrekking hadden op belangen die onder het toepassingsgebied van het Verdrag van Wenen van 1961 vielen (dossier 2016/4458). De BIM-Commissie schorste de methoden. Het Comité bevestigde deze beslissing.

Het Vast Comité I vatte zichzelf in twee andere zaken (2016/5147 en 2016/5259) om na te gaan of de gehanteerde methode strookte met het wettelijkheidsprincipe en meer bepaald met de Conventie van Wenen. Na onderzoek bleek dat (een deel van) de methoden betrekking had(den) op gegevens die binnen de door het Comité in zijn rechtspraak geëxpliciteerde 'onschendbare perimeter' vielen (dossier 2014/3148). Het Comité bracht tevens in herinnering dat het toen had gewezen op een afwezigheid van richtlijnen ter zake van het Ministerieel Comité voor inlichting en veiligheid (nu: Nationale Veiligheidsraad). In dossier 2016/5259 stelde het Comité daarenboven vast dat dergelijke richtlijnen nog steeds niet voorhanden waren. Het voegde hier volgende considerans aan toe: '*Overwegende dat het Vast Comité I, en deze keer met aandrang, herhaalt dat in dergelijke omstandigheden geen methode ten aanzien van [bepaalde aspecten] die vallen onder de Conventie van Wenen van 1961 kunnen worden toegelaten*.'[161]

III.3.2.4. De gevolgen van een onwettig(e) (uitgevoerde) methode

Omwille van de hoogdringendheid machtigde een diensthoofd in zeven gelijkaardige dossiers mondeling een specifieke methode (dossiers 2016/4490 tot en met 2016/4496). Pas meer dan anderhalve maand later volgde de schriftelijke bevestiging. Omdat artikel 18/7 § 2 eist dat '*de mondelinge beslissing […] zo spoedig mogelijk [wordt] bevestigd door een met redenen omklede schriftelijke beslissing van het diensthoofd*' schorst de BIM-Commissie de methode. Het Comité volgt deze beslissing van de BIM-Commissie niet om volgende redenen: '*Attendu qu'il échet de constater que la loi n'a pas prévu explicitement de sanctions en cas du non-respect de cette exigence; Attendu que le Comité permanent R a déjà antérieure-*

---

160 '*Overwegende dat de methoden wettelijk zijn in de mate waarin ze de contacten viseren in België van buitenlandse nummers gebruikt in het buitenland; Overwegende echter dat de uitvoering van methoden niet wettig is in de mate waarin de vordering aan de operator niet conform de beslissing is […] omdat ze niet beperkt is tot Belgische contacten.*' (vrije vertaling).

161 Om de problematiek ten gronde te bespreken, organiseerde het Comité een werkvergadering met de Kabinetten van de Eerste Minister, Justitie en Defensie, waarop de verschillende standpunten en bekommernissen werden uiteengezet.

ment émis un avis selon lequel la procédure d'extrême urgence devait être améliorée; Attendu qu'il ne fait pas de doute que la loi n'a pas été respectée en ce qui concerne la confirmation écrite de la réquisition qui doit être faite dans les plus brefs délais, selon les termes de la loi, mais que, par ailleurs, le Comité permanent R doit prendre attitude sur les conséquences du non-respect de cette condition formelle; Attendu que le retard mis par [le service de renseignement] à confirmer, par écrit, la réquisition verbale trouve son explication dans les circonstances de faits, dans lesquels la méthode a été mise en œuvre; Attendu que l'irrégularité formelle constatée n'affecte pas la fiabilité des informations recueillies et qu'elle n'a pas de plus entraîné de violation des droits fondamentaux des personnes faisant l'objet de la méthode; Que le comité se réfère dans sa décision à la jurisprudence "Antigone" qui a amené le législateur à insérer un art. 32 dans le titre préliminaire du Code de Procédure pénale ainsi que la jurisprudence en droit administratif dans certains cas de non-respect des formes et des procédures.'[162]

III.3.2.5. De jurisdictionele beslissing met betrekking tot de klacht

De klager werd vervolgd voor feiten van terrorisme. In zijn strafdossier trof hij elementen aan waaruit bleek dat hij destijds was opgevolgd door de VSSE. Zo bevatte het dossier onder meer foto's van de verzoeker. Hij wenste te weten te komen of de VSSE op een wettige wijze was tewerk gegaan bij de inzet van – naar zijn oordeel – specifieke inlichtingenmethoden.

In deze zaak kwamen diverse principiële kwesties aan bod. Omwille van hun precendentwaarde worden ze hieronder uitgebreid hernomen.

III.3.2.5.1. Verzoek tot stellen van prejudiciële vragen

De verzoeker wenste vooreerst dat het Vast Comité I, als jurisdictioneel orgaan, een aantal prejudiciële vragen zou stellen aan het Grondwettelijk Hof op basis van

---

162 'Overwegende dat moet vastgesteld worden dat de wet niet expliciet voorzien heeft in *sancties in geval van het niet respecteren van deze verplichting; Overwegende dat het Vast Comité I voorheen reeds het advies heeft geformuleerd om de procedure van hoogdringendheid te verbeteren; Overwegende dat het geen twijfel lijdt dat de wet in dit geval niet werd gerespecteerd met betrekking tot de schriftelijke bevestiging van de vordering die volgens de wet zo snel mogelijk dient te gebeuren, maar dat het Comité zich ook moet uitspreken over de gevolgen van het niet respecteren van deze formele verplichting; Overwegende dat de vertraging door [de inlichtingendienst] om de mondelinge vordering schriftelijk te bevestigen te verklaren is door de feitelijke omstandigheden waarin de methode werd uitgevoerd; Overwegende dat de vastgestelde formele onregelmatigheid de betrouwbaarheid van de informatie niet aantast en ook geen schending van fundamentele rechten van de personen die het voorwerp waren van de methode, met zich heeft gebracht; Dat het Comité in zijn beslissing verwijst naar de Antigoon-rechtspraak die de wetgever ingeschreven heeft in art. 32 van de Voorafgaande titel bij het Wetboek van strafvordering en naar de administratiefrechtelijke rechtspraak in bepaalde gevallen van niet-respect van vormvereisten en procedures.*' (vrije vertaling).

artikel 26 § 2, tweede lid, Bijzondere wet op het Grondwettelijk Hof[163] of – indien het Comité hier niet zou op ingaan – aan het Europees Hof van Justitie te Luxemburg.[164] Het Comité, dat in deze optreedt als een rechtscollege en in beginsel dus bij machte is prejudiciële vragen voor te leggen aan het Grondwettelijk Hof, oordeelde dat niet op dit verzoek diende te worden ingegaan.

Wat betreft de eerste vraag verwees het Comité naar volgende elementen:

- anders dan de klager voorhield, gebeurt de controle op *elke* bijzondere inlichtingenmethode automatisch en zonder uitzondering, eerst door de BIM-Commissie en naderhand door het Vast Comité I;
- in 2010 werd reeds een verzoek tot gehele of gedeeltelijke vernietiging van de bepalingen die ook de klager aanhaalde, afgewezen door het Grondwettelijk Hof dat in zijn arrest nr. 145/2011 van 22 september 2011 stelde dat er ter zake geen onverenigbaarheden waren tussen de Inlichtingenwet van 30 november 1998 en de Grondwet;
- de bijzondere opsporingsmethoden van de politie volgen een andere methodiek en parcours dan de bijzondere inlichtingenmethoden. De wetgever heeft voor elk van de methoden in een passende procedure voorzien ter bescherming van iedere rechtsonderhorige. De dubbele controle voor de BIM's (met name een *a priori* controle door de Commissie gevolgd door een *a posteriori* controle door het Comité) biedt op meer dan afdoende wijze garanties tegen een mogelijke onwettige aanwending van bijzondere inlichtingenmethoden.

---

163 *'Schenden de bepalingen van hoofdstuk IV/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen-en veiligheidsdienst de artikelen 10 en 11 van de grondwet in die zin dat de a posteriori controle van de inlichtingendiensten, zoals in casu de observatie met een technisch hulpmiddel, enkel gebeurt op verzoek van de rechtsonderhorige en niet op automatische wijze en dat hiervoor een aparte klacht ingediend moet worden, terwijl de controle door de kamer van inbeschuldigingstelling van de bijzondere opsporingsmethoden, zoals een observatie met een technisch hulpmiddel, overeenkomstig artikel 235ter van het Wetboek van strafvordering steeds gebeurt wanneer de onderzoeksrechter zijn dossier aan de Procureur des Konings overzendt krachtens artikel 127 § 1, lid 1 van het Wetboek van strafvordering?' en 'Schendt artikel 43/8 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst de artikelen 10 en 11 van de grondwet in die zin dat het niet mogelijk is voor de klager die overeenkomstig artikel 43/4 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst een klacht indiende, beroep in te stellen tegen de beslissing van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten omtrent de controle op de inlichtingenmethoden, terwijl het voor een beklaagde of inverdenking gestelde wel mogelijk is om cassatieberoep in te stellen tegen de beslissing van de kamer van inbeschuldigingstelling omtrent de controle op de bijzondere opsporingsmethoden?'*

164 *'Schendt artikel 26 van de bijzondere wet op het Grondwettelijk Hof de Verdragen en meer bepaald de artikelen 47 en 48 van het Handvest van de grondrechten van de Europese Unie in samenhang met artikel 20 van het Handvest van de grondrechten van de Europese Unie in die zin dat het een rechtsonderhorige niet mogelijk is om een prejudiciële vraag te stellen aan het Grondwettelijk Hof aangaande de schending van zijn grondrechten doordat het Vast Comité van Toezicht op de Inlichtingen- en veiligheidsdiensten geen rechtscollege zou betreffen in de zin van artikel 26 van de Bijzondere Wet op het Grondwettelijk Hof, terwijl het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten wel uitspraak in enige en laatste aanleg doet over de regelmatigheid van de aangewende inlichtingenmethoden?'*

Omtrent de tweede prejudiciële vraag wees het Comité onder meer op volgende aspecten:
- artikel 43/8 W.I&V bepaalt dat tegen de BIM-beslissingen van het Comité geen beroep mogelijk is. Zoals hierboven vermeld, werd er in 2010 reeds een verzoek tot gehele of gedeeltelijke vernietiging van de BIM-Wet behandeld bij het Grondwettelijk Hof. In zijn arrest sprak het Grondwettelijk Hof zich derhalve reeds uit in de zin dat het ter zake geen onverenigbaarheden tussen de Wet van 30 november 1998 en de Grondwet zag;
- verder herinnerde het Comité eraan dat het een *sui generis*-rechtscollege is dat niet tot de rechterlijke macht behoort en dat in het leven werd geroepen om een inbreuk op de grondrechten van rechtsonderhorigen onmogelijk te maken door een wettigheidcontrole op te leggen ten einde het onwettig handelen van inlichtingendiensten te verhinderen. Het Comité is een onafhankelijk orgaan en biedt vergaande garanties op onpartijdigheid, wat overigens duidelijk werd erkend door het Grondwettelijk Hof.

Met betrekking tot de kwestie of het Comité verplicht was de door de klager geformuleerde prejudiciële vraag te stellen aan het Europees Hof van Justitie, werden volgende argumenten ontwikkeld:
- daar waar de klager in zijn voorgestelde initiële vraag aanhaalde dat het Vast Comité I geen rechtscollege is, diende dit zoals hogervermeld, te worden tegengesproken. Het verzoek om een prejudiciële vraag te laten stellen aan het Europees Hof van Justitie berustte dus op een verkeerde premisse;
- bovendien lag het hoe dan ook buiten de bevoegdheid van Comité om zich uit te spreken over de toepassing van de bijzondere wet van 6 januari 1989 op het Grondwettelijk Hof in het algemeen en in het bijzonder om deze te toetsen aan de Europese verdragsbepalingen;
- het stellen van een prejudiciële vraag ter zake vertoonde geen enkel verband met de rechtsmacht van het Vast Comité I en kon evenmin bijdragen tot oplossing van het geschil dat voorlag zodat elk voorwerp van de vraag ontbrak;
- de vermelde artikelen 46 en 47 van het Handvest behoren trouwens tot de penale sfeer en zijn van toepassing bij strafrechtbanken. Ook deze materie valt buiten de bevoegdheden van het Vast Comité I en vertoont geen enkel verband met de rechtsmacht van het Comité.

III.3.2.5.2. Schorsende werking procedure

De verzoeker vroeg het Comité een schorsende werking toe te kennen aan zijn controle en dit ten aanzien van het gebruik van de in de strafzaak betwiste inlichtingen. Het Comité wees deze vraag af als 'zonder voorwerp'. In de Inlichtingenwet van 30 november 1998 is alleen sprake van 'schorsing' van een methode. Daarmee wordt bedoeld de schorsing van de uitvoering ervan. Aangezien de

methode waarvan sprake reeds in 2013 werd uitgevoerd én beëindigd, kon ze niet meer worden geschorst.

III.3.2.5.3. Inzage in dossierstukken

De klager vroeg inzage van alle informatie over de observaties, de machtigingen van het diensthoofd en de beslissing van de BIM-Commissie ter zake. Dit moest hem toelaten om de wettigheid van de inlichtingenmethode na te gaan.

Het Comité wees erop dat dergelijke stukken conform de Classificatiewet van 11 december 1998 nooit ter kennis kunnen worden gebracht van personen die geen houder zijn van een veiligheidsmachtiging, nu het telkens om geclassificeerde documenten gaat. Overigens komt het niet aan de klager toe om de voorlegging van bepaalde documenten te vragen nu de wet heel specifiek een procedure heeft voorzien tot kennisname van alle relevante elementen. Deze procedure is vervat in artikel 43/5 § 3 W.I&V waarin wordt bepaald dat het dossier '*alle informatie en inlichtingen [bevat] die ter zake relevant zijn, met uitzondering van die welke afbreuk doen aan de bescherming van bronnen, de bescherming van de persoonlijke levenssfeer van derden, de classificatieregels bepaald bij de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, of de vervulling van de in de artikelen 7, 8 en 11 omschreven opdrachten van de inlichtingen-en veiligheidsdiensten.*'

De klager was evenwel van oordeel dat hij niet op afdoende wijze beschikte over de nodige elementen om de proportionaliteit en subsidiariteit te beoordelen. Hij beweerde inzage te moeten krijgen van de informatie waarover de VSSE beschikte voorafgaand aan de observaties om na te gaan of geen gewone inlichtingenmethoden konden worden aangewend. Het Comité wees er op dat de afweging inzake proportionaliteit en subsidiariteit toekomt aan de BIM-Commissie en aan het Vast Comité I. Het zijn deze twee instanties die de bevoegdheid hebben gekregen om de naleving van deze beginselen te controleren.

III.3.2.5.4. Beoordeling ten gronde

Het Comité oordeelde dat de methoden waarvan sprake beantwoordden aan de principes van proportionaliteit en subsidiariteit. *In casu* bestond het doel erin met zekerheid en objectief vast te stellen dat de betrokkene contacten had met personen gekend voor hun islamistische extremistische opvattingen en/of er een link was met de Syriëproblematiek. Gewone methoden waren hier '*ontoereikend […] en het opstellen van een camera die beelden opneemt de gepaste mogelijkheid […] om de inlichtingen te verzamelen en de contacten tussen de klager en anderen vast te stellen, en dit zonder afbreuk te doen aan het tweede principe dat moet worden in acht genomen, met name de proportionaliteit*'. In deze waren de potentiële bedreigingen (met name terrorisme en extremisme) ernstig genoeg om een bij-

zondere inlichtingenmethode te rechtvaardigen. Tevens bleek aan alle vorm- en procedurevoorwaarden voldaan.

III.3.2.5.5. Het *ultra petita*-beginsel

Daar waar de klager initieel in zijn klacht verwees naar twee observaties, breidde hij deze naderhand uit met de motivering dat hij tot de vaststelling was gekomen dat meerdere observaties ten aanzien van hem waren gebeurd.

Het Vast Comité I wees op het *ultra petita*-beginsel dat inhoudt dat een rechtscollege niet meer kan toekennen dan hetgeen geëist werd. Het Comité zag dan ook niet de noodzaak om, '*buiten de controle op de inlichtingenmethoden van 3 juni 2013 en van 13 december 2013, andere mogelijke bijzondere inlichtingenmethoden aan een controle te onderwerpen. Bij de beoordeling van onderhavige klacht werd aldus een wettigheidscontrole uitgevoerd op alle inlichtingenmethoden die van toepassing waren op de klager.*'

III.3.2.5.6. Vernietiging gegevens en verbod van exploitatie

Tot slot verzocht de klager dat de exploitatie van de onrechtmatig verzamelde gegevens zou worden gestaakt en dat ze onverwijld zouden worden vernietigd.

Het staken van de exploitatie van de informatie en de vernietiging ervan zijn mogelijkheden die door de wetgever zijn geboden aan het Vast Comité I voor elke bijzondere inlichtingenmethode die aan hem wordt voorgelegd in het kader van zijn *a posteriori* controle.

Het Vast Comité I heeft telkenmale, bij elke bijzondere methode, beslist dat een staking van de exploitatie van gegevens of de vernietiging ervan zich niet opdrong. Daarover nam het Vast Comité I, tijdens zijn stelselmatige controle, al een definitieve beslissing.

III.4. CONCLUSIES EN AANBEVELINGEN

Het Vast Comité I formuleerde volgende algemene conclusies en aanbevelingen aangaande het toezicht op de bijzondere inlichtingenmethoden:

- het aantal door de VSSE ingezette bijzondere methoden groeide exponentieel. Dit was zo omwille van de toegenomen inlichtingenactiviteiten na de aanslagen in Parijs en Zaventem/Maalbeek. De stijging was *quasi* volledig toe te schrijven aan de 'kennisname van oproepgegevens' die steeg van amper 33 gevallen naar 622. Maar ook de uitzonderlijke methoden stegen aanzienlijk. Er waren niet alleen meer uitzonderlijke maatregelen, hun gemiddelde duur was ook beduidend langer;
- ondanks de aanslagen bleef het aantal door de ADIV ingezette specifieke en uitzonderlijke methoden vrij stabiel;

- het aantal vorderingen bij operatoren ter identificatie van de gebruiker van een telecommunicatiemiddel (nieuw artikel 16/2 W.I&V) lag zeer hoog. Maar ook dit was het rechtstreekse gevolg van de terroristische aanslagen;
- daar waar de ADIV zich bij de inzet van BIM-methoden traditioneel meer toespitste op de dreiging van 'spionage' bleef dit voor de VSSE 'terrorisme';
- waar het Comité zich in 2015 nog in 1,1% van de BIM-dossiers vatte, bleef dit in 2016 beperkt tot 0,15% van de gevallen. Een van de redenen hiervoor was dat uit de *prima facie*-controle die binnen het Comité op elk BIM-dossier wordt uitgevoerd, bleek dat de twee inlichtingendiensten terdege rekening hielden met de beperkingen van de wet, met de beslissingen van de BIM-Commissie en met de rechtspraak van het Comité;
- het Comité wees erop dat de VSSE en de ADIV in hun BIM-beslissingen desgevallend expliciet kunnen verwijzen naar de nieuwe bevoegdheid om de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied op te volgen (zie III.1.1);
- bij de uitwerking van de regeling inzake vordering van operatoren (zie III.1.3), werd geen rekening gehouden met de nieuwe bevoegdheid van de VSSE en de ADIV om de activiteiten van buitenlandse diensten op ons grondgebied op te volgen. Het Vast Comité I beval aan dat de wetgever ook hier een maximale termijn voor kennisname van metadata zou bepalen.

HOOFDSTUK IV

HET TOEZICHT OP DE INTERCEPTIE VAN COMMUNICATIE UITGEZONDEN IN HET BUITENLAND

Sinds begin 2011 kunnen zowel de VSSE als de ADIV onder zeer strikte voorwaarden communicaties afluisteren, er kennis van nemen en ze registreren (art. 18/17 § 1 W.I&V).

Deze zogenaamde 'BIM-intercepties'[165] moeten evenwel duidelijk worden onderscheiden van '*het zoeken, het onderscheppen, het afluisteren, het kennisnemen of het opnemen door de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht van elke vorm van communicatie uitgezonden in het buitenland*.' Deze tweede vorm van intercepties was al langer mogelijk en kan worden ingezet om redenen van militaire aard in het kader van de opdrachten gedefinieerd in artikel 11 § 2, 1° en 2° W.I&V als om redenen van veiligheid en bescherming van Belgische en van geallieerde troepen tijdens opdrachten in het buitenland alsook van onderdanen die in het buitenland gevestigd zijn (art. 11 § 2, 3° en 4° W.I&V). Deze 'intercepties' kennen een volkomen ander controlekader.[166]

Het externe toezicht erop is namelijk uitsluitend opgedragen aan het Vast Comité I en dit zowel voor, tijdens als na de intercepties (art. 44*bis* W.I&V). Het Comité heeft hierbij de bevoegdheid om lopende intercepties te doen stopzetten wanneer blijkt dat de voorwaarden waarin ze uitgevoerd worden, de wettelijke bepalingen en/of de ministeriële toelating niet respecteren (art. 44*ter* W.I&V). Elk jaar, begin december, dient de ADIV immers aan de minister van Defensie zijn gemotiveerde lijst voor te leggen met organisaties of instellingen, van wie de communicatie het komende jaar mag onderschept worden. Dit gebeurt met het oog op de ministeriële toelating van deze intercepties. De minister dient zijn beslissing te nemen binnen tien werkdagen en moet ze vervolgens meedelen aan de ADIV. Nadien moeten zowel de lijst als de ministeriële toelating door de ADIV worden toegezonden aan het Vast Comité I. De overzending van deze lijst loopt echter

165 Hierover 'Hoofdstuk III. Controle op de bijzondere inlichtingenmethoden'.

166 Bij Wet van 30 maart 2017 (*BS* 28 april 2017) werd deze interceptiemogelijkheid gevoelig uitgebreid. De wet voorziet ook in een verscherpte controle door het Vast Comité I, onder meer aan de hand van een maandelijkse interceptielijst. In voorliggend activiteitenverslag wordt uiteraard alleen de regeling besproken die in 2016 van toepassing was.

vaak vertraging op.[167] Zo ook in 2016. Het Comité ontving het interceptieplan pas in juni.

Mede op basis van zijn bevindingen naar aanleiding van de Snowden-onthullingen[168] en gelet op de verklaringen van de ADIV dat het in de toekomst de mogelijkheid wil benutten om telecommunicatiekabels af te tappen, actualiseerde en verdiepte het Vast Comité I in 2015-2016 zijn kennis over de SIGINT[169]-activiteiten van de ADIV. Het Comité deed dit aan de hand van werkbezoeken aan de binnenlandse sites waar deze activiteiten worden verricht. Zo bijvoorbeeld werd het werk van de SIGINT-operatoren *in real time* bekeken en nadien vergeleken met de vermeldingen in het logboek (art. 44*bis* 2° en 3° W.I&V). Tevens werd een steekproef getrokken van de in het logboek vermelde intercepties en werd gecontroleerd of deze traceerbaar en onder te brengen waren in het Interceptieplan 2016. Ten slotte werden gesprekken gevoerd met leden van de technische sectie van de SIGINT-afdeling. Dit liet toe om een zicht te krijgen op het gebruikte materiaal; ook de samenwerkingsverbanden met andere SIGINT-partners werd besproken.

Deze onderzoeken, inspecties en gesprekken resulteerden in een studie die in juli 2016 werd overgezonden aan de minister van Defensie en de ADIV. Het Comité formuleerde daarin onder meer volgende vaststellingen en opmerkingen:

- de prioriteiten die aan de operatoren werden toevertrouwd, waren in overeenstemming met het 'Interceptieplan 2016';
- de SIGINT-afdeling van de ADIV was in 2016 actief in een nieuwe regio. De afdeling was hier voornamelijk belast met het zoeken en identificeren van relevante selectoren;
- het logboek beantwoordde aan de eisen zoals geformuleerd door het Comité in eerdere aanbevelingen;
- de aan de hand van de steekproef nader gecontroleerde intercepties bleken traceerbaar en verenigbaar met het 'Interceptieplan 2016';
- de ADIV toonde zich bereid om de personen en organisaties die in de interceptieplannen voorkomen, nader te identificeren dan te verwijzen naar typologieën. Het Comité benadrukte evenwel dat deze intentie ook effectief moet gerealiseerd worden;
- bepaalde materiële behoeften werden reeds ingevuld of staan in de planning. Echter, wat betreft het personeelskader werd niet in een uitbreiding voorzien. Het Comité uitte zijn bezorgdheid over deze situatie, meer in het bijzonder inzake gekwalificeerde vertalers, naast de noodzakelijke analisten, operatoren en stafmedewerkers;

---

167 VAST COMITÉ I, *Activiteitenverslag 2010*, 105 ('IX3.2. Tijdig overzenden van geviseerde veiligheidsintercepties') en *Activiteitenverslag 2015*, 71. Het Vast Comité I ontving het Afluisterplan 2017 pas in juli 2017.

168 VAST COMITÉ I, *Activiteitenverslag 2014*, 8-35 ('II.1. De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten').

169 SIGINT is een samentrekking van *Signals Intelligence* en zijn inlichtingen die verzameld worden door het onderscheppen van elektronische signalen.

– het Comité werd in kennis gesteld van nieuwe initiatieven inzake SIGINT-samenwerking met derde landen en van het voornemen om nieuw materiaal aan te schaffen. Het Comité verwelkomde deze openheid van de ADIV. Wel wees het er op dat dergelijke initiatieven met de nodige aandacht zullen worden opgevolgd, net zoals dat het geval was met eerdere projecten van de ADIV[170];
– het Vast Comité I heeft geen vaststellingen gedaan die geleid hebben tot de stopzetting van intercepties.

In zijn geheel stelde het Comité vast dat er door de ADIV transparantie werd geboden over de interceptieactiviteiten, werkprocessen en toekomstige projecten. Het Comité nam zich voor zijn specifieke toezicht op dit vlak verder uit te bouwen.

170 VAST COMITÉ I, *Activiteitenverslag 2015*, 73-75 ('V.1. Advies inzake internationale samenwerking met betrekking tot SIGINT').

HOOFDSTUK V
OPDRACHTEN VOOR PARLEMENTAIRE ONDERZOEKSCOMMISSIES

Bij Wet van 18 juli 1991 werd het Vast Comité I ingesteld als het specifieke toezichtorgaan op de inlichtingen- en veiligheidsdiensten. In 1996[171] wordt het Comité voor het eerst met een nieuwe opdracht belast: voortaan kan een parlementaire onderzoekscommissie het toezichtorgaan inschakelen in haar onderzoeken. Dit gebeurde in het kader van een globale hervorming (lees: uitbreiding[172]) van de mogelijkheden van parlementaire onderzoeken. Van de mogelijkheid om het Comité in te schakelen werd pas in 2016 voor het eerst gebruik gemaakt: het Vast Comité I kreeg diverse opdrachten van twee verschillende onderzoekscommissies.

V.1. DE PARLEMENTAIRE ONDERZOEKSCOMMISSIE NAAR DE AANSLAGEN

Op 22 maart 2016 werd België het doelwit van 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'.[173] Deze commissie werd

171 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.

172 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.

173 *Parl. St.* Kamer 2016-17, 54K1752/001.

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*'.[174]

In juli 2016 startte het Vast Comité I ambtshalve een toezichtonderzoek op 'over de informatiepositie van de twee inlichtingendiensten, voorafgaand aan 22 maart 2016, over de individuen of groepen die de aanslagen te Zaventem en Brussel hebben uitgevoerd of hierbij betrokken waren evenals naar de individuen of groepen die Salah Abdeslam hebben toegelaten zich in de clandestiniteit op te houden tot aan zijn arrestatie op 18 maart 2016'.[175] Maar de commissie schakelde het Vast Comité I – en het Vast Comité P – ook diverse malen in.

De werkzaamheden van het Vast Comité I voor deze onderzoekscommissie kunnen worden verdeeld onder diverse noemers: het toezenden van onderzoeksverslagen, het opstellen van een rapport met daarin de eerder geformuleerde aanbevelingen in de strijd tegen terrorisme en extremisme, het fungeren als doorgeefluik voor geclassificeerde informatie, het horen als getuige en het uitvoeren van bijkomende onderzoeksopdrachten.

V.1.1. TOEZENDEN VAN ONDERZOEKSVERSLAGEN

Het Vast Comité I heeft in het verleden vele toezichtonderzoeken[176] gevoerd die rechtstreeks of onrechtstreeks van belang konden zijn voor de parlementaire onderzoekscommissie.[177] Het betrof volgende onderzoeken:

- toezichtonderzoek over de manier waarop de Veiligheid van de Staat extremistische en terroristische 'islamistische' activiteiten opvolgde (2001);
- toezichtonderzoek over de opvolging van het radicaal islamisme door de inlichtingendiensten (2007);
- toezichtonderzoek over de wijze waarop de Belgische inlichtingendiensten de gebeurlijke activiteiten opvolgen die inlichtingendiensten uit belangrijke immigratielanden van buiten de Europese Unie ontplooien op het Belgische grondgebied (2011);
- toezichtonderzoek naar de opsporing en opvolging door de ADIV van extremistische elementen bij het personeel van Defensie en de Krijgsmacht (2012);

---

174 *Parl. St.* Kamer 2016-17, 54K1752/008, 25.

175 Hierover uitvoerig: 'Hoofdstuk II.4. De aanslagen in Zaventem en Maalbeek'.

176 Begin juni 2016 werd een lijst met alle toezichtonderzoeken uitgevoerd door het Vast Comité I in de periode 2000-2016 overgezonden aan de voorzitter van de parlementaire onderzoekscommissie.

177 In de marge van de werkzaamheden van de Commissie, werd het Comité op de hoogte gebracht van het feit dat *'la commission d'accompagnement a décidé que dorénavant, elle n'examinerait plus les dossiers des Comités P et R concernant le terrorisme tant que la commission d'enquête parlementaire sur les attentats terroristes n'aurait pas terminé ses travaux'*.

- gezamenlijk toezichtonderzoek over de wijze waarop het OCAD internationale relaties onderhoudt met gelijkaardige buitenlandse of internationale diensten in toepassing van art. 8, 3° van de W.OCAD van 10 juli 2006 (2013);
- toezichtonderzoek betreffende een klacht van een stafhouder naar het gebruik van informatie afkomstig van massale buitenlandse datacaptatie in Belgische strafzaken (2013);
- toezichtonderzoek betreffende de klacht van een in België verblijvende Tunesische onderdaan die meent door de inlichtingendiensten gevolgd te worden (2014);
- toezichtonderzoek betreffende de informatiepositie van de twee inlichtingendiensten over de rekrutering, de zending, het verblijf en de terugkeer in België van jongeren (van Belgische en andere nationaliteiten die in België verblijven) die vertrekken of vertrokken zijn naar Syrië of Irak en aangaande de uitwisseling van inlichtingen met diverse overheden (alsook het addendum over de mislukte aanslag in de Thalys) (2016);
- toezichtonderzoek naar de wijze waarop de VSSE het 'protocolakkoord tot regeling van de samenwerking tussen de Veiligheid van de Staat (VSSE) en het Directoraat-generaal Uitvoering van Straffen en Maatregelen (DGUSM)' uitvoerde (2016);
- toezichtonderzoek over de informatiepositie van de twee inlichtingendiensten, voorafgaand aan 13 november 2015 's avonds, over de individuen of groepen die de aanslagen te Parijs hebben uitgevoerd of hierbij betrokken waren (2016).

Het Vast Comité I stelde de parlementaire onderzoekscommissie in het bezit van deze toezichtonderzoeken.

V.1.2. EEN OVERZICHT VAN DE AANBEVELINGEN IN DE STRIJD TEGEN TERRORISME EN EXTREMISME

Op verzoek van de parlementaire onderzoekscommissie stelde het Comité een rapport op met daarin alle sinds 2000 geformuleerde aanbevelingen die rechtstreeks of onrechtstreek van belang zijn in de strijd tegen terrorisme en extremisme. Zij werden aangevuld met aanbevelingen die betrekking hebben op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen. Telkenmale werd – voor zover het Comité in het bezit was van de vereiste informatie – kort weergegeven of en in welke mate de betrokken aanbeveling reeds werd geïmplementeerd. Hieronder wordt dit document samengevat weergegeven.

Voldoende personele en technische middelen en wettelijke mogelijkheden

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.

Wat betreft de wettelijke bevoegdheden, werd uiteraard melding gemaakt van de Wet van 4 februari 2010 waarbij de VSSE en de ADIV uitgebreide specifieke en uitzonderlijke methoden werden toegekend. Deze middelen worden uiteraard frequent ingezet tegen terroristische en extremistische dreigingen.

Ten slotte besteedde het Comité ook aandacht aan het feit dat de ADIV niet expliciet bevoegd is voor de opvolging van extremisme en terrorisme *an sich*. Dit is alleen het geval in de mate waarin er een band is met de militaire veiligheid. Een voorbeeld hiervan vormt de opvolging van het extremisme binnen het leger. Ook de situatie waarbij er een reële militaire bedreiging uitging van *foreign terrorist fighters* (FTF) onder meer voor de bevolking, maakte dat de ADIV duidelijk bevoegd was om op te treden. Het Comité beval aan om na te denken over een meer duidelijke bevoegdheidsomschrijving van de ADIV ter zake.[178]

Wijzigingen aan de BIM-Wet

Het Comité heeft de afgelopen jaren een aantal aanbevelingen geformuleerd om de BIM-Wet aan te passen, enerzijds om een performanter optreden mogelijk te maken, anderzijds om een noodzakelijk evenwicht te bewaren met fundamentele rechten en vrijheden.

Zo werd erop gewezen dat de BIM-Wet het niet mogelijk maakte om uitzonderlijke methoden in te zetten in geval van extremisme. Het Comité stelde voor af te stappen van dit verbod. De Inlichtingenwet werd in die zin gewijzigd bij Wet

[178] Bij Wet van 30 maart 2017, waarbij de Inlichtingenwet gevoelig werd gewijzigd, werd de bevoegdheid van de ADIV ruimer omschreven. Er werd evenwel niet expliciet verwezen naar terrorisme of extremisme.

van 30 maart 2017. Die wet voerde nog een aantal andere wijzigingen door die aansloten bij eerdere aanbevelingen van het Comité: de inzet van BIM-methoden in het buitenland, het afschaffen van het verbod om via taps verzamelde gegevens na een jaar en twee maanden te vernietigen, het gebruik van de hoogdringendheidsprocedure *ex* art. 13/1 § 2, derde lid W.I&V voor het plegen van strafbare feiten… Wat betreft het respect voor fundamentele rechten en vrijheden wees het Comité meermaals op het feit dat de door het arrest van het Grondwettelijk Hof van 22 september 2011 vernietigde notificatieverplichting diende vervangen te worden. Ook hierop bood de wetswijziging uit 2017 een antwoord.

Ten slotte wees het Comité 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 breder een 'internationaal mandaat'. Bepaalde van deze aspecten werden nader geregeld in de Wet van 30 maart 2017.

Coördinatie op het gebied van de inlichtingen en de oprichting van het OCAD

In het kader van een onderzoek naar het informatiebeheer in een zaak die verband hield met terrorisme, herhaalde het Comité zijn voorstel om een coördinator op het gebied van de inlichtingen te benoemen. Deze persoon zou een overzicht hebben van de productie van de operationele diensten. Zijn taak zou erin bestaan de rapporten te ontvangen van de inlichtingendiensten op de gebieden die het toenmalige Ministerieel Comité (nu Nationale Veiligheidsraad) als prioritair beschouwt en op grond daarvan periodieke of thematische syntheses te maken bestemd voor de bevoegde overheden. De noodzaak aan een betere coördinatie van en informatie-uitwisseling tussen de politie- en inlichtingendiensten was ook gebleken naar aanleiding van een gemeenschappelijk onderzoek van de Vaste Comités I en P betreffende de coördinatie tussen de verschillende inlichtingen- en politiediensten in de strijd tegen het terrorisme. De resultaten van deze onderzoeken hebben grotendeels uitvoering gekregen via de creatie van het OCAD bij Wet van 10 juli 2006. Sinds zijn oprichting heeft het Vast Comité I, samen met het Vast Comité P, een aantal aanbevelingen geformuleerd die de werking van het OCAD moeten verbeteren. Het betrof onder meer volgende thema's:

- het aanstellen van een duidelijk centraal contactpunt in elke ondersteunende dienst;
- het centrale contactpunt moet een volledig zicht hebben op de uitgewisselde info;
- binnen elke ondersteunende dienst moet de traceerbaarheid van de inlichtingen gegarandeerd worden;

- het begrip 'relevante inlichtingen' moet uitgeklaard worden;
- 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;
- de punctuele dreigingsevaluaties dienen op een gestandaardiseerde manier tot stand te komen;
- er dient in een beveiligd communicatienetwerk te worden voorzien;
- de verwarring omtrent de identiteit en de 'buitenlandopdracht' van het OCAD moet worden opgelost door een richtlijn van de Nationale Veiligheidsraad[179];
- de vertegenwoordiging van veiligheidsdiensten op internationale fora dient gecoördineerd te verlopen;
- de werking van de *Joint Information Box* (dit is een lijst met gegevens over radicaliserende personen en organisaties in onze samenleving) moet gevoelig herzien worden.[180]

Ook hier werd op meerdere punten door de wetgever of de regering uitvoering gegeven aan de aanbevelingen.

Samenwerking tussen de VSSE en de ADIV onderling en met andere Belgische politie- en overheidsdiensten

In de strijd tegen terreur en extremisme is het natuurlijk essentieel dat de verschillende bevoegde diensten optimaal samenwerken en hun acties coördineren. Diverse aanbevelingen van het Vast Comité I moeten hieraan bijdragen:

- de bevoegde ministers en de Nationale Veiligheidsraad dienen de voorwaarden voor samenwerking, informatie-uitwisseling en technische bijstand te regelen en op die wijze uitvoering geven aan de verplichtingen opgenomen in de artikelen 19 en 20 W.I&V[181];
- 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;

179 Inmiddels heeft de Nationale Veiligheidsraad dergelijke richtlijn uitgevaardigd.

180 Ook deze aanbeveling werd ter harte genomen onder meer door de creatie van een dynamische gegevensbank FTF (zie hierover 'Hoofdstuk VI. De controle van gemeenschappelijke gegevensbanken') en door de op til zijnde omvorming van de JIB.

181 In diverse protocols en richtlijnen werd reeds (gedeeltelijk) uitvoering gegeven aan deze aanbeveling.

- er dienen protocolakkoorden te worden afgesloten met de Dienst Vreemdelingenzaken en het Commissariaat-Generaal voor de Vluchtelingen en de Staatslozen[182];
- het protocolakkoord tussen de VSSE en het Directoraat-generaal Penitentiaire Inrichtingen is in zijn huidige vorm achterhaald en dient te worden aangepast of herschreven. Ook de ADIV dient een dergelijk akkoord te sluiten;
- 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.
- de verschillende deelnemers aan de *local task force* in de strijd tegen terrorisme en extremisme moeten elkaar goed informeren over elkaars noden, behoeften, mogelijkheden en beperkingen;
- om het extremisme intern het leger adequaat op te volgen, 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.

Samenwerking met buitenlandse diensten

Ook wat betreft de samenwerking met buitenlandse diensten heeft het Comité meermaals aanbevolen dat uitvoering zou worden gegeven aan de bepalingen van de artikelen 19 en 20 W.I&V. In 2017 heeft de Nationale Veiligheidsraad ter zake een belangrijke richtlijn goedgekeurd waarin nader bepaald wordt onder welke voorwaarden de Belgische inlichtingendiensten moeten of kunnen samenwerken met buitenlandse diensten. Wel wordt daarin nog onvoldoende ingegaan op het doorgeven van persoonsgegevens aan buitenlandse diensten. In het kader van de strijd tegen terrorisme vormt dit uiteraard een essentieel aspect.

Verder wees het Comité erop dat de inlichtingendienst die gegevens ontvangt uit het buitenland, minimale inspanningen moet leveren om te achterhalen op welke wijze de betrokken inlichtingen werden verkregen, dit om toe te laten gegevens van derde landen die op (manifest) onrechtmatige wijze zijn verzameld, desgevallend niet te aanvaarden.

Tot slot formuleerde het Comité recent een aanbeveling voor meer gestructureerde en internationaal gestandaardiseerde procedures voor informatie-uitwisseling met het buitenland.

182 Sinds 2011 bestaat er een dergelijk akkoord tussen de VSSE en de Dienst Vreemdelingenzaken.

Van collecte en analyse: de producten van het inlichtingenwerk

Het Comité formuleerde zes aanbevelingen die erop gericht zijn de collecte en de analyse dermate te organiseren dat er een duidelijke meerwaarde ontstaat op het vlak van de producten van het inlichtingenwerk:
- 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 verzamelen (collectemethoden) en hoe men de informatie zal analyseren (analysemethoden)(cf. II.1.3.3);
- beide inlichtingendiensten moeten hun 'klanten' expliciet bevragen over welke inlichtingen deze precies willen beschikken en hoe ze de inlichtingen evalueren (*feedback*);
- er dienen gestandaardiseerde analysetechnieken te worden gebruikt om cognitieve of feitelijke fouten te voorkomen;
- er moeten voorspellende inlichtingen worden geproduceerd voor de diverse overheden aangezien dit tot de essentie van het inlichtingenwerk behoort;
- de diensten moeten strategische analyses opstellen inzonderheid over het radicaal islamisme en over de strategieën die islamitische extremisten hanteren;
- met het oog op de *business continuity* moeten fenomeenanalyses worden opgesteld en geactualiseerd.

Informatiestromen en ICT

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.

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 ICT-middelen die het geheel ondersteunen.

Organisatorische randvoorwaarden voor een optimale werking

In het kader van de audit bij de ADIV[183] formuleerde het Vast Comité I talrijke concrete aanbevelingen aangaande de organisatorische voorwaarden noodzakelijk voor een goede inzet van de middelen, het beheer en de leiding van het personeel, de informatiestromen en ICT (zie hoger) en ten slotte het risicobeheer.

De aanbevelingen die het Vast Comité I formuleerde n.a.v. de *performance audit* bij de VSSE werden in vier thema's onderverdeeld: leiderschap, informatiehuishouding, werkprocessen en kwaliteitstevredenheid. Verschillende van deze aanbevelingen werden volledig of gedeeltelijk geïmplementeerd.

Een uitwerkte regeling voor alle aspecten van de informantenwerking

Het Vast Comité I heeft over de jaren talrijke aanbevelingen geformuleerd in verband met de informantenwerking. Deze blijven hun belang behouden aangezien de collectemogelijkheid ook in het domein van het extremisme en terrorisme essentieel blijft.

- er dient een duidelijke wettelijke regeling te komen inzake informantenwerking;
- daarnaast dient er 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;
- 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;

183 VAST COMITÉ I, *Activiteitenverslag 2011*, 7-14 ('Een audit bij de militaire inlichtingendienst').

– 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 (veiligheid van de betrokkene en aan de mogelijkheid dat hij 'verleid' wordt illegale handelingen te stellen). 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;
– er dient 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 informatie kunnen beschikken die cruciaal is voor de veiligheid van de rechtstaat, een welomschreven – al dan niet geldelijke – 'tegenprestatie' te verlenen;
– 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.

Een aantal punctuele aanbevelingen

– in het kader van de opvolging van het terrorisme en extremisme is het absoluut noodzakelijk de anonimiteit van de inlichtingenagenten te kunnen garanderen teneinde hen tegen bedreigingen te beschermen;
– de personeelsleden van inlichtingendiensten en het OCAD moeten de grootste omzichtigheid aan de dag leggen in hun activiteiten op de sociale netwerken vooral in de huidige context van verhoogde dreiging met terroristische aanslagen;
– de diensten moeten criteria uitwerken voor het in kennis stellen van personen die het voorwerp zijn van een dreiging (art. 19 W.I&V);
– personeel van bedrijven of instellingen die stoffen behandelen die kunnen worden gebruikt bij het ontwikkelen van NRBC-wapens, zouden systematisch aan veiligheidsonderzoeken of -verificaties moeten worden onderworpen;
– 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;
– de VSSE moet haar informatie systematisch *up-to-date* houden, dit met het oog op haar rol bij erkenningsaanvragen van geloofsgemeenschappen (bijv. erkenning moskee);
– de diensten moeten voldoende personeel met kennis van specifieke talen (kunnen) aanwerven.

V.1.3. DOORGEEFLUIK VOOR DE RAADPLEGING VAN GEHEIME DOCUMENTEN

Op grond van haar brede taak, de omvang van haar bevoegdheden en het feit dat haar werd opgedragen aanbevelingen te formuleren, oordeelde de parlementaire onderzoekscommissie het nuttig om toegang te hebben tot die onderzoeken, dewelke verslagen, inlichtingen of geheime documenten bevatten, ongeacht of het ging om geclassificeerde informatie dan wel om dossiers over gerechtelijke onderzoeken of informatie in handen van deze instanties waarvan het werk in essentie geheim is (zoals de Veiligheid van de Staat, het OCAD, de Vaste Comités I en P, de Cel voor Financiële Informatieverwerking …).[184]

Wat de inzage in geclassificeerde informatie betrof, diende een *modus vivendi* te worden gezocht aangezien de Commissieleden niet over de vereiste veiligheidsmachtiging beschikten.[185] Hierover vonden verschillende overlegmomenten plaats, die uiteindelijk hebben geleid tot het afsluiten van een protocol.[186] Specifiek wat de inlichtingendiensten betreft, werd besloten dat de geclassificeerde informatie ter raadpleging beschikbaar zou worden gehouden binnen de lokalen van het Vast Comité I. De Commissie kon daarbij rekenen op de hulp van één van haar deskundigen, die houder was van een veiligheidsmachtiging. Hij heeft *'met die instanties contact kunnen leggen en heeft kennis kunnen nemen van documenten waaruit hij heeft kunnen afleiden wat hij daarover aan de commissie mocht meedelen zonder de geheime aard ervan te verraden*'.[187]

V.1.4. GETUIGENIS(SEN) VOOR DE ONDERZOEKSCOMMISSIE

Op 21 december 2016 werd de voorzitter van het Vast Comité I gehoord en dit achter gesloten deuren. Hij gaf de commissie toelichting bij het toezichtonderzoek

184 *Parl. St.* Kamer 2016-17, 54K1752/008, 27.

185 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).

186 *Parl. St.* Kamer 2016-17, 54K1752/008, 27. '*Aangaande de informatie in lopende dossiers, alsook dewelke in handen is van politie- of inlichtingendiensten, heeft de commissie op 27 mei 2016, overeenkomstig artikel 4 § 2 van de Wet van 3 mei 1880, een protocol uitgewerkt dat werd afgesloten tussen één van haar deskundigen en de federaal procureur, de procureur-generaal van Brussel en de door de eerste voorzitter van het hof van beroep te Brussel aangewezen magistraat. Dat protocol voorzag erin dat de gevraagde geheime informatie in een verzegelde enveloppe werd gestopt en dat die werd geopend in aanwezigheid van de over een veiligheidsmachtiging beschikkende deskundige en van de betrokken korpschefs*'. Onder korpschefs wordt in deze niet enkel politieoversten verstaan, maar ook de Administrateur-generaal van de VSSE en de Chef ADIV, die van deze procedure gebruik maakten.

187 *Parl. St.* Kamer 2016-17, 54K1752/008, 27.

over de informatiepositie van de twee inlichtingendiensten, voorafgaand aan 22 maart 2016, over de individuen of groepen die de aanslagen te Zaventem en Maalbeek hebben uitgevoerd of hierbij betrokken waren evenals naar de individuen of groepen die Salah Abdeslam hebben toegelaten zich in de clandestiniteit op te houden tot zijn arrestatie op 18 maart 2016.[188, 189]

V.1.5. HET UITVOEREN VAN BIJKOMENDE ONDERZOEKSOPDRACHTEN

Op verzoek van de parlementaire onderzoekscommissie werd door het Vast Comité I een tijdslijn opgemaakt aangaande documenten die – in de periode tussen 13 november 2015 en 22 maart 2016 – werden verkregen of verzonden door de Belgische inlichtingendiensten aan/van (buitenlandse) partnerdiensten met betrekking tot de protagonisten[190] van de aanslagen. Andere onderzoeksopdrachten werden uitgevoerd in de loop van 2017.

V.2. DE PARLEMENTAIRE ONDERZOEKSCOMMISSIE NAAR DE WET MINNELIJKE SCHIKKING

Op 1 december 2016 werd in de plenaire vergadering van de Kamer de tekst aangenomen met daarin het voorstel tot instelling van een tweede parlementaire onderzoekscommissie.[191] 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 zijn verricht om spoed achter de behandeling te zetten. Het Franse blad *Le Canard enchaîné* beweerde dat Kazachse autoriteiten als voorwaarde voor de bestelling van Franse helikopters geëist zouden hebben dat de Franse overheid het nodige zou doen om de vervolging in België tegen een zogenaamd 'Kazachs

188 *Parl. St.* Kamer 2016-17, 54K1752/008, 49. Tijdens een vergadering op 11 januari 2017 werd opnieuw een hoorzitting gehouden met de voorzitter van het Vast Comité I.

189 De Commissie weigerde in te gaan op het verzoek van de voorzitters van de Vaste Comités I en P om aanwezig te kunnen zijn op de hoorzittingen met gesloten deuren van leidinggevenden van diensten die onder hun controle staan.

190 De tijdslijn had betrekking op Salah Abdeslam, Mohamed Abrini, Mohamed Belkaid, Khalid en Ibrahim El Bakraoui, Osama Krayem en Najim Laachraoui.

191 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).

trio'[192] te beëindigen. Daarvoor zou de hulp zijn ingeroepen van Armand De Decker, op dat ogenblik 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 het 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 werd ermee belast een 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. Tevens moet ze nagaan hoe het Openbaar Ministerie toepassing maakte van artikel 216*bis* Sv. Ten slotte[193] moet de onderzoekscommissie een onderzoek instellen naar de wijze waarop Patokh Chodiev en Alijan Ibragimov de Belgische nationaliteit hebben gekregen.

Op 15 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 Patokh Chodiev en andere 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 naturalisatie[194] – en afkomstig uit het toezichtonderzoek Tractebel.[195]

In 2017 werd het Vast Comité I uitvoerig ingeschakeld en kreeg het diverse onderzoeksopdrachten van de parlementaire onderzoekscommissie: er werden verschillende onderzoeksrapporten opgesteld en de voorzitter van het Vast Comité I werd meermaals gehoord in dat kader. Hierover zal in het Activiteitenverslag van 2017 worden gerapporteerd.

---

192 Het betreft de heren Chodiev, Ibragimov en Machkevitch, drie uit Centraal-Azië afkomstige zakenpartners die zich begin jaren 90 in België vestigden om vennootschappen op te richten.

193 Artikel 1, § 1, derde lid van het oprichtingsbesluit (*Parl. St*. Kamer 2016-17, nr. 54K2179/006).

194 Hierover: VAST COMITÉ I, *Activiteitenverslag 2012*, 5-14 ('*De rol van de VSSE in het kader van procedures tot het verkrijgen van de Belgische nationaliteit*').

195 Over het toezichtonderzoek naar *'De werking van de inlichtingendiensten bij het beheer van eventuele gegevens in de context voorafgaand aan het afsluiten van een internationale commerciële overeenkomst'* (2000) werd tweemaal kort gerapporteerd (VAST COMITÉ I, *Activiteitenverslag 2001*, 6-8 en *Activiteitenverslag 2003*, 126-127). Het werd omwille van andere prioriteiten nooit afgerond.

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[196] de Wet van 5 augustus 1992 op het politieambt (WPA). Daarmee werd een wettelijke basis gecreëerd voor de oprichting van gemeenschappelijke gegevensbanken.

De ministers van Binnenlandse Zaken en Justitie baseerden zich op deze nieuw door de wetgever geboden mogelijkheid om, via het Koninklijk besluit van 21 juli 2016 (KB FTF)[197], de gemeenschappelijke gegevensbank '*foreign terrorist fighters*' op te richten, ook wel de dynamische databank FTF genoemd.

Artikel 44/6[198] 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'. Het betreft nieuwe opdrachten voor het Vast Comité I.

Aangezien voorliggend hoofdstuk het eerste vormt dat werd opgesteld binnen deze context, wordt eerst een beschrijving gegeven van wat moet worden begrepen onder gemeenschappelijke gegevensbanken (VI.1). Vervolgens wordt dieper ingegaan op de FTF-databank (VI.2) om ten slotte de door het COC en het Vast Comité I in dit kader gevoerde activiteiten te bespreken (VI.3).

196 *BS* 9 mei 2016.

197 K.B. 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 (KB FTF).

198 Eveneens gewijzigd door de eerder vernoemde Wet van 27 april 2016.

VI.1. WAT IS EEN GEMEENSCHAPPELIJKE GEGEVENSBANK?

VI.1.1. DOELEINDE EN REGELS

Verschillende diensten, organen of overheden oefenen opdrachten uit in het kader van de voorkoming en opvolging van terrorisme of extremisme dat kan leiden tot terrorisme. Artikel 44 § 2 WPA bepaalt dat wanneer het voor deze instanties vereist is om in het kader van de gezamenlijke uitoefening van hun opdrachten de persoonsgegevens en de beschikbare informatie te structureren '*zodat ze rechtstreeks kunnen worden teruggevonden,* [dan] *worden deze persoonsgegevens en informatie verwerkt in een of meerdere gemeenschappelijke gegevensbanken*'. De oprichting van een gemeenschappelijke gegevensbank wordt ingegeven door een van volgende doeleinden: de strategische, tactische of operationele noodzaak om gezamenlijk gegevens te verwerken dan wel de hulp bij het nemen van beslissingen door de bestuurlijke overheden of de overheden van bestuurlijke of gerechtelijke politie (art. 44/11/3*bis* WPA).

Een dergelijke gegevensbank kan evenwel alleen gezamenlijk door de ministers van Binnenlandse Zaken en Justitie worden opgericht. Zij worden dan 'verantwoordelijk voor de verwerking' in de zin van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

De gegevensbank maakt de verwerking van verschillende categorieën van persoonsgegevens mogelijk en dit onder meer met betrekking tot personen, groeperingen, organisaties en fenomenen. De wet vereist dat deze gegevens toereikend, ter zake dienend en niet overmatig zijn in verhouding tot de hierboven vermelde opdrachten.

Voorafgaand aan haar oprichting, moeten de ministers van Binnenlandse Zaken en Justitie gemeenschappelijk aangifte doen van de gegevensbank bij het COC en het Vast Comité I, die binnen 30 dagen vanaf de ontvangst van de aangifte een gezamenlijk advies dienen uit te brengen. Het betreft een vorm van *a priori* controle, dewelke wordt aangevuld met de (voortdurende) controle zoals voorgeschreven in artikel 44/6 WPA (*supra*).

Voor elke gemeenschappelijke gegevensbank bepaalt een Koninklijk besluit vastgesteld na overleg in de Ministerraad, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer, de types van verwerkte persoonsgegevens, de regels op het gebied van de verantwoordelijkheden op het vlak van de bescherming van de persoonlijke levenssfeer, de regels op het gebied van de veiligheid van de verwerkingen alsook de regels inzake het gebruik, de bewaring en de uitwissing van de gegevens.

VI.1.2. DE RAADPLEGING EN INKENNISSTELLING

Zes verschillende categorieën van diensten kunnen via raadpleging of in kennisstelling kennis krijgen van (bepaalde) gegevens uit de gegevensbank. De wet bepaalt dat de gegevensbank op basis van de 'behoefte om te kennen' (*need to know*) rechtstreeks toegankelijk is voor het OCAD, de geïntegreerde politie en de inlichtingen- en veiligheidsdiensten (art. 44/11/3*ter* § 1 WPA). Dit zijn de zogenaamde 'basisdiensten' in het KB FTF (zie VI.2.2).

Daarnaast is er sprake van volgende diensten (de zogenaamde 'partnerdiensten' in het KB FTF): de Vaste Commissie voor de lokale politie, de Algemene Directie Crisiscentrum, de Algemene Directie Veiligheid en Preventie van de FOD Binnenlandse Zaken, het Directoraat-generaal Penitentiaire Inrichtingen en de penitentiaire inrichtingen, de FOD Buitenlandse Zaken, Directoraat-generaal Consulaire Zaken, het Openbaar Ministerie, de Cel voor Financiële Informatieverwerking, de Dienst Vreemdelingenzaken en de onderzoeks- en opsporingsdiensten van de Algemene Administratie der douane en accijnzen. Ook voor hen kunnen de gegevens rechtstreeks toegankelijk zijn of het voorwerp uitmaken van een directe bevraging (zie ook VI.2.2).[199]

Daarenboven kan de Koning andere '*Belgische openbare overheden die door de wet belast zijn met de toepassing van de strafwet*' de toegang verlenen tot persoonsgegevens en informatie die ze nodig hebben voor de uitvoering van hun opdrachten '*ter voorkoming en ter opvolging van het terrorisme of van extremisme wanneer dat tot terrorisme kan leiden*' (art. 44/11/3*ter* § 3 WPA).

De wet vereist dat persoonsgegevens en informatie ingevoerd in de gemeenschappelijke gegevensbanken onverwijld worden meegedeeld aan de korpschef van elke betrokken politiezone, dewelke, op zijn beurt, de bevoegde bestuurlijke politieoverheden informeert[200] (art. 44/11/3*ter* § 4 WPA).

De wetgever laat ook toe de persoonsgegevens en informatie mee te delen '*aan een derde overheid of een derde eenheid*' en dit volgens door de Koning bepaalde nadere regels en na evaluatie (art. 44/11/3*quater* WPA).

Onverminderd de nationale en internationale rechtsregels die België verbinden, kunnen deze gegevens – op basis van de modaliteiten zoals door de Koning bepaald – ten slotte worden meegedeeld aan buitenlandse politiediensten, internationale organisaties voor gerechtelijke en politionele samenwerking, internationale rechtshandhavingsdiensten alsook aan buitenlandse inlichtingendiensten en aan organen die belast zijn met de analyse van de dreiging of hun gelijken.

199 De Koning bepaalt voor elk van deze diensten de wijze van toegang.

200 Met naleving van de voorwaarden bepaald in en met toepassing van artikel 44/1 § 4 WPA.

VI.1.3. DE VERPLICHTING OM DE GEMEENSCHAPPELIJKE GEGEVENSBANK TE VOEDEN

Gezien de onderliggende idee er een is van de noodzaak tot het delen van informatie (het zgn. *need-to-share*-principe), voorziet de wetgever in een verplichting om de gegevensbank te voeden. Vandaar dat alle diensten die rechtstreeks toegang hebben tot de gegevensbank – met name de basisdiensten en de diensten die door Koning op basis van de wet zijn aangewezen (zie VI.2.2) de hun beschikbare relevante informatie dienen toe te zenden. De opname in de gegevensbank gebeurt onder de verantwoordelijkheid van de betrokken dienst en volgens zijn interne validatieprocedure.

De wet sluit de mogelijkheid niet uit om geclassificeerde informatie te verwerken in de gemeenschappelijke gegevensbanken.[201]

Er bestaan twee uitzonderingen op de verplichting om gegevens in te voeren in de gemeenschappelijke gegevensbank. De doorzending kan worden uitgesteld wanneer en zolang de bevoegde magistraat, met instemming van de Federale Procureur, meent dat hierdoor de uitoefening van de strafvordering of de veiligheid van een persoon in het gedrang kan brengen. Dezelfde mogelijkheid gelt voor informatie afkomstig van de inlichtingendiensten: wanneer en zolang de leidinggevende oordeelt dat deze voeding de veiligheid van een persoon of de regel van de derde dienst in gevaar kan brengen, kan hij de doorzending uitstellen (art. 44/11/3*ter* § 5 WPA).

VI.1.4. BIJZONDERE ACTOREN

Los van de diensten die toegang hebben tot de gegevens en de verplichting tot voeding, bepaalt de wetgever een aantal andere actoren die een belangrijke rol toebedeeld krijgen in het kader van de werking van een gemeenschappelijke gegevensbank.

Vooreerst dient gezamenlijk door de ministers van Binnenlandse Zaken en Justitie een 'consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer' te worden aangewezen. Hij waakt in het bijzonder over de algemene voorwaarden voor de rechtmatigheid van de verwerking zoals bepaald in de arti-

---

201 De Memorie van Toelichting specifieert in dat verband: '*Deze gegevens en informatie die betrekking hebben op de verschillende gegevenscategorieën zijn in principe geen geclassificeerde persoonsgegevens of informatie. Een zo ruim mogelijke verdeling van de gegevens en de informatie moet mogelijk zijn zonder hinderpalen te plaatsen op de verwerking ervan. Evenwel, wanneer het absoluut noodzakelijk is dat dergelijke gegevens in deze gegevensbanken verwerkt worden teineinde te beantwoorden aan de doelstellingen waarvoor ze opgericht werden, dan is de Wet van 11 devember 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen van toepassing. Daarom moet elke persoon die bijvoorbeeld een toegang wenst tot deze geclassificeerde gegevens en informatie, over de gepaste veiligheidsmachtiging beschikken.*' *Parl. St.* Kamer 2016-17, 54K1727/001, 21-22.

kelen 4 tot 8 van de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer. Hij is tevens de contactpersoon voor het COC en het Vast Comité I (art. 44/3 § 2 WPA).

Verder wordt een 'beheerder' aangewezen die belast is met het technisch en functioneel beheer van de gegevensbank. Deze beheerder staat minstens in voor het creëren en het ter beschikking stellen van de gemeenschappelijke gegevensbank, het beheer en het onderhoud ervan, het in functionele regels vertalen van de regels met betrekking tot de verwerking van informatie, de bepaling van technische normen noodzakelijk voor de werking van de gegevensbank, de organisatie van de rechten en toegangen, het beheer en de behandeling van de veiligheidsincidenten alsook het verstrekken van advies en het aanbieden van documentatie en technische ondersteuning (art. 44/11/3*bis* § 9 WPA).

Ten slotte wordt ook een 'operationeel verantwoordelijke' aangeduid. Deze garandeert minstens volgende opdrachten: het controleren van de kwaliteit van de gegevens en van hun relevantie in verhouding tot de doeleinden van de gegevensbank, het uitoefenen van een coördinatiefunctie voor de voeding door de verschillende diensten, het organiseren van een passende samenwerking tussen de partnerdiensten met het oog op de verwezenlijking van de voorziene doeleinden en er op toezien dat de exploitatie van de persoonsgegevens en de informatie beantwoordt aan de geformuleerde doeleinden (art. 44/11/3*bis* § 10 WPA).

VI.2. DE GEMEENSCHAPPELIJKE GEGEVENSBANK *FOREIGN TERRORIST FIGHTERS*

Bij Koninklijk besluit van 21 juli 2016 (KB FTF) werd de gemeenschappelijke gegevensbank '*foreign terrorist fighters*' ('gegevensbank FTF') opgericht. Deze gegevensbank moet bijdragen tot de analyse, de evaluatie en de opvolging van personen gelieerd aan de problematiek van het djihadisme.

VI.2.1. DE INLICHTINGENFICHES

De gegevensbank bestaat uit inlichtingenfiches van personen gelieerd aan het fenomeen van strijders die zich naar jihadistische strijdzones begeven. Het betreft een *up-to-date* gehouden persoonsfiche die alle niet–geclassificeerde[202] persoonsgegevens en informatie[203] bevat over de betrokkenen die afkomstig zijn van alle

[202] Anders dan voorzien door de wetgever (zie de Memorie van Toelichting, *supra*), laat het KB FTF niet toe om geclassificeerde informatie te verwerken. Het KB FTF vereist niettegenstaande wel het bezit van een veiligheidsmachtiging van het niveau 'geheim' voor elkeen die toegang heeft tot de gegevensbank (art. 7§ 2 KB FTF).

[203] Persoonsgegevens, gerechtelijke of administratieve gegevens, gegevens van bestuurlijke politie en niet-geclassificeerde toereikende, ter zake en niet-overmatige inlichtingengegevens.

bevoegde diensten (cf. art. 1, 11° KB FTF). Zoals vermeld in het Verslag aan de Koning, moet deze fiche '*het niet alleen mogelijk de potentiële dreiging te beoordelen die deze personen vertonen, maar voornamelijk er een opvolging van te verzekeren met het oog op het anticiperen en het verhinderen van mogelijke terroristische acties door hen*'.[204]

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:

- ze zijn naar een jihadistische conflictzone afgereisd;
- ze hebben België verlaten om naar een jihadistische conflictzone af te reizen;
- ze zijn naar België onderweg of naar België teruggekeerd na afgereisd te zijn naar een jihadistische conflictzone;
- ze werden (gewild of ongewild) verhinderd om naar een jihadistische conflictzone af te reizen;
- ze hebben de intentie om naar een jihadistische conflictzone af te reizen (op voorwaarde dat deze intentie aangetoond wordt door ernstige aanwijzingen) (art. 6 § 1, 1° KB FTF);
  OF
- er bestaan ernstige aanwijzingen dat zij een van bovenstaande criteria kunnen vervullen (art. 6 § 1, 2° KB FTF).

VI.2.2. EEN GRADATIE VAN DE TOEGANGEN

Artikel 7 KB FTF stelt de gradatie van de toegangen zoals geregeld in de wet in plaats:

- de zogenaamde 'basisdiensten' (het OCAD, de inlichtingen- en veiligheidsdiensten, de geïntegreerde politie) alsook sommige 'partnerdiensten' (het Directoraat-generaal penitentiaire instellingen en de penitentiaire instellingen, het Openbaar Ministerie, de Cel voor Financiële Informatieverwerking en de Dienst vreemdelingenzaken), hebben rechtstreeks toegang tot de gegevensbank FTF en, daarmee samenhangend, ook de verplichting deze te voeden (VI.1.3);
- andere partnerdiensten (het DGCC, het DGVP, het DG Consulaire zaken van de FOD Buitenlandse Zaken en de onderzoeks- en opsporingsdiensten van de Algemene Administratie der douane en accijnzen), kunnen toegang hebben op basis van rechtstreekse bevraging (een soort *hit/no hit* principe). In het geval van een 'hit', neemt de betrokken dienst contact op met een van de basisdiensten;

[204] *BS* 22 september 2016, 63970.

– ten slotte is er ook een rechtstreekse toegang en een verplichting tot voeding geregeld voor de Algemene Administratie van Justitiehuizen van de Franse Gemeenschap, het Departement Justitiehuis van het Ministerie van de Duitstalige gemeenschap, de Afdeling Justitiehuizen van de bevoegde diensten van de Vlaamse overheid en het Vlaams Agentschap Jongerenwelzijn. Die toegang is evenwel beperkt tot gegevens over de FTF in het kader van de opdrachten van de betrokken dienst.

VI.2.3. DE INFORMATIEKAARTEN

Naast de inlichtingenfiches, worden ook 'informatiekaarten' (cf. de artikelen 44/11/3*quater* WPA en 11 KB FTF) 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. Het KB FTF bepaalt in dat kader dat de korpschef van de betrokken politiezone (systematisch) aan de burgemeester de informatiekaart inzake de *foreign fighters* die in zijn gemeente resideren, toestuurt. De burgemeester kan er vervolgens gebruik van maken in het kader van zijn wettelijke bevoegdheden en onder zijn verantwoordelijkheid (art. 12 KB FTF).

VI.2.4. DE INVULLING VAN DE VERSCHILLENDE ANDERE ROLLEN

De Federale Politie wordt aangeduid als beheerder van de gegevensbank FTF. Naast de opdrachten bepaald in de WPA, legt het KB FTF de Federale Politie de opdracht op een lijst bij te houden van personen die toegang hebben tot de gegevensbank, te waken over de oplijsting van de uitgevoerde verwerkingen alsook om het OCAD, de consulent voor veiligheid, het COC en het Vast Comité I in kennis te brengen van elk vastgesteld of gerapporteerd veiligheidsincident (art. 3 KB FTF).

Het OCAD op zijn beurt werd aangeduid als operationeel verantwoordelijke en staat in voor het beoordelen van de gegevens van de inlichtingenfiche, de validatie als FTF, de contacten met de verantwoordelijken voor de verwerking en de in kennisstelling van de betrokken dienst indien de doorgezonden gegevens niet (meer) toereikend, ter zake of niet-overmatig zijn (art. 4 KB FTF).

Het KB FTF definieert verder de opdrachten van de consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer: de bewustmaking van de bescherming van gegevens, de samenwerking met de Federale Politie voor de uitwerking van procedures alsook met de andere consulenten voor veiligheid. Ook

zijn statuut werd gepreciseerd: hij treedt op in alle onafhankelijkheid, maar met respect voor de bevoegdheden van de verschillende diensten (art. 5 KB FTF).

VI.2.5. EEN VALIDATIESYSTEEM VAN DE GEGEVENS

De diensten die rechtstreeks toegang hebben tot de gegevensbank FTF moeten een validatiesysteem ontwikkelen om te garanderen dat de aan de gegevensbank doorgezonden gegevens toereikend, ter zake dienend en niet overmatig zouden zijn in het licht van de opdracht om bij te dragen aan de analyse, evaluatie en opvolging van personen gelieerd aan de problematiek van het jihadisme.

Dit validatiesysteem moet worden meegedeeld aan het OCAD (de operationeel verantwoordelijke) die, op zijn beurt, het dient door te zenden aan de Federale Politie (de beheerder), aan de consulent voor de veiligheid alsook aan het COC en het Vast Comité I.

VI.2.6. GEGEVENSBEHEER

VI.2.6.1. Het toevoegen, wijzigen en verwijderen van gegevens

De gegevens aangaande een FTF zijn uiteraard onderhevig aan een permanente actualisering. In die zin wordt de gegevensbank dan ook bestempeld als zijnde 'dynamisch'. Volgens het Verslag aan de Koning diende, gezien het grote aantal diensten die onmiddellijk toegang hebben tot de gegevensbank, een onderscheid te worden gemaakt tussen die diensten die het meest op de hoogte zijn van de problematiek van de buitenlandse terroristische strijders en zij die zich eerder beperken tot het verrijken van persoonsgegevens en informatie. De afspraken hieromtrent kunnen worden samengevat als volgt:

- alleen de basisdiensten kunnen een inlichtingenfiche aanmaken (te zeggen, een persoon registreren in de gegevensbank). Indien een persoon al werd geregistreerd, kunnen de diensten die over een rechtstreekse toegang beschikken na validatie hun eigen informatie toevoegen, zonder daarbij evenwel de reeds aanwezige informatie te wijzigen of te verwijderen;
- alleen de dienst die een bepaalde informatie registreerde, kan deze ook wijzigen, verbeteren of uitwissen. Wanneer een dienst van mening is dat informatie die door een andere dienst ingevoegd werd, gewijzigd, verbeterd of uitgewist zou moeten worden, richt deze zich tot de dienst die de informatie geregistreerd heeft;
- wanneer de diensten uiteenlopende standpunten innemen over de wijziging of verwijdering van bepaalde informatie, komt het aan het OCAD toe als operationeel verantwoordeljke, om de eindbeslissing te nemen (art. 9 KB FTF).

Het KB FTF bepaalt ook wat er dient te gebeuren wanneer in de gegevensbank FTF geregistreerde informatie niet meer in de eigen databank van de dienst zelf geregistreerd is. In deze hypothese moet de dienst hiervan het OCAD op de hoogte brengen die, indien ze oordeelt dat de informatie toereikend, ter zake dienend of niet overmatig is, kan beslissen om ze vooralsnog in de gegevensbank FTF te behouden (art. 8 § 2 KB FTF).

VI.2.6.2. De bewaring en archivering van de gegevens[205]

De gegevens moeten worden gewist wanneer de finaliteit van de gegevensbank FTF verdwijnt, en dit met een maximum van dertig jaar na de laatste verwerking.[206]

Na de laatste verwerking wordt, minstens driemaandelijks, bestudeerd of de gegevens nog steeds een rechtstreeks verband houden met het vooropgestelde doel. Indien hier affirmatief kan worden op geantwoord, blijven ze bewaard.

Deze regel houdt een uitzondering in voor personen voor wie gegronde vermoedens bestaan dat ze behoren tot één van de categorieën uit artikel 6 § 1, 1° KB FTF. Voor hen wordt de maximum bewaartijd teruggebracht tot zes maanden na registratie. Na afloop van deze termijn en als hun betrokkenheid bij een categorie van FTF blijkt, worden de gegevens bewaard volgens bovenvermelde afspraken. Blijkt dat hun betrokkenheid niet vaststaat, worden hun gegevens gewist.

De persoonsgegevens en informatie dewelke moet worden gewist, kunnen maximaal voor een periode van dertig jaar worden bewaard. De gearchiveerde gegevens kunnen enkel worden geëxploiteerd voor welomschreven doeleinden (inzake politiebeleid[207], voor de verwerking van antecedenten in het kader van een onderzoek naar een terroristisch crimineel feit of om de verdediging van administratieve overheden, gerechtelijke of administratieve politie te waarborgen). Na afloop van een periode van dertig jaar, worden de gegevens gewist.[208]

In zijn hoedanigheid van beheerder van de gegevensbank, wordt de Federale Politie belast met het in functionele regels vertalen van de afspraken met betrekking tot de verwerking van informatie. Het komt hem toe om de nodige maatregelen te nemen voor een correct beheer van de gegevens.

205 Art. 13 & 14 KB FTF gelezen in combinatie met art. 44/11/3 *bis* § 5 en § 7 WPA.
206 Onverminderd de Archiefwet van 24 juni 1995.
207 In dat geval moeten de gegevens worden geanonimiseerd.
208 Onverminderd de Archiefwet van 24 juni 1995.

VI.2.7. DE INTERNATIONALE SAMENWERKING

De basisdiensten zijn de enige diensten die de gegevens opgenomen in de gegevensbank FTF mogen meedelen aan buitenlandse diensten (art. 15 KB FTF).

Voor wat de politiediensten betreft, moet de mededeling gebeuren in overeenstemming met de bepalingen uit het KB van 30 oktober 2015 betreffende de voorwaarden verbonden aan de mededeling van persoonsgegevens en informatie door de Belgische politiediensten aan de leden van Interpol en Interpol alsook met deze uit hoofdstuk 1/1 van de Wet van 9 december 2004 betreffende de wederzijdse internationale rechtshulp in strafzaken en tot wijziging van artikel 90*ter* Sv.

Wat de inlichtingendiensten betreft, legt het KB FTF op dat de mededeling aan buitenlandse inlichtingendiensten gebeurt in overeenstemming met 20 § 3 W.I&V, en dus op basis van de voorwaarden zoals gedefinieerd door de Nationale Veiligheidsraad.

Wat het OCAD betreft ten slotte, verwijst het KB FTF naar artikel 8, 3° W.OCAD dat het coördinatieorgaan toelaat om met gelijkaardige buitenlandse of internationale diensten overeenkomstig de richtlijnen van de Nationale Veiligheidsraad specifieke internationale contacten te verzekeren en de gegevens verkregen ter gelegenheid van deze contacten mee te delen aan de bevoegde Belgische diensten.

VI.2.8. EINDVERANTWOORDELIJKHEDEN EN ALGEMENE VERPLICHTINGEN

Naast het opleggen van een kwaliteitscontrole aan de hand van een intern validatiesysteem voor alle diensten met directe toegang (*supra*), bepaalt het KB FTF de verantwoordelijkheden wanneer hieraan niet wordt voldaan (art. 16 KB FTF). De verantwoordelijkheid voor de kwaliteit van de persoonsgegevens komt toe aan:

- de verantwoordelijke voor de verwerking eigen aan elke dienst die de gegevensbank FTF voedt voor wat de persoonsgegevens en informatie betreft die deze dienst heeft doorgezonden;
- de ministers van Binnenlandse Zaken en Justitie voor wat de persoonsgegevens en informatie betreft die gevalideerd zijn op de inlichtingenfiches.

Daarenboven dient elke verantwoordelijke voor de verwerking eigen aan elke dienst met directe toegang te waken over de wettelijkheid van de doorzending van zijn persoonsgegevens en informatie naar de gegevensbank FTF.

De ministers van Binnenlandse Zaken en Justitie moeten op hun beurt waken over de wettelijkheid van de doorzending van de informatie van de gegevensbank FTF, over de goede technische en operationele werking ervan alsook over de veiligheid van de toegangssystemen en de integriteit, de beschikbaarheid en de ver-

trouwelijkheid van de gegevens. Het KB schrijft voor dat het hen toekomt om bij richtlijn de noodzakelijke maatregelen met het oog op het naleven van hun verplichtingen, te bepalen.

VI.3. DE CONTROLE DOOR HET COC EN HET VAST COMITÉ I

Het KB FTF waarbij de databank FTF werd opgericht, trad pas in werking op 22 september 2016 en de verplichte voorafgaandelijke aangifte van de database, dateerde pas van 3 november 2016. De controle van het COC en het Vast Comité I beperkte zich in 2016 dan ook tot het advies over deze aangifte (VI. 3.2). Wel werd daarvoor reeds een advies verleend bij een voorlopige voorafgaandelijke aangifte (VI.3.1) (art. 44/11/3*bis* § 3 WPA).

VI.3.1. EEN EERSTE ADVIES

In mei en juni 2016 verzochten de ministers van Binnenlandse Zaken en Justitie om een advies over het ontwerp van Koninklijk besluit aangaande de gemeenschappelijke gegevensbank FTF en over de vereiste voorafgaandelijke aangifte. Het advies (integraal hernomen in bijlage F) werd uitgebracht op 20 juni 2016. Samenvattend stelden het COC en het Vast Comité I wat volgt:

- ze benadrukten dat het om een voorlopig advies ging nu bleek dat het Koninklijk besluit nog niet was gepubliceerd. Het COC en het Vast Comité I drongen aan op de noodzaak om toekomstige aangiftes van gemeenschappelijke gegevensbanken pas te doen nadat de Koninklijke besluiten hieromtrent werden gepubliceerd;
- zij stelden vast dat personen die steun verlenen aan FTF of rekruteren niet in de database zouden worden opgenomen, terwijl dit een nog grotere operationele bruikbaarheid zou kunnen genereren van de gegevensbank en dat deze categorie bovendien wel werd opgenomen in de Circulaire COL 10/2015 van het College van Procureurs-generaal betreffende de gerechtelijke aanpak van de FTF;
- ze merkten het belang op van de aanstelling van een consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer voor de gegevensbank, maar ook in de schoot van elke dienst die daartoe toegang heeft, en legden de nadruk op de aanstelling van contactpunten bij het OCAD en de Federale Politie;
- ze wezen op de moeilijkheden die zouden kunnen optreden in de mate dat het ontwerp-KB en de aangifte specifieerden dat de gegevensbank enkel niet-geclassificeerde gegevens zou bevatten, terwijl de inlichtingen- en veiligheids-

diensten hoofdzakelijk over dit type van gegevens beschikken en dat de wetgever hen verplicht om de gegevensbank te voeden met alle gegevens waarover ze beschikken;
- ze suggereerden om het ontwerp van Koninklijk besluit aan te passen door ook te voorzien in de overhandiging aan het COC en het Vast Comité I van de lijsten met personen die over een toegang tot de gegevensbank beschikken;
- ze vroegen zich af waarom een toegang voor de Vaste Commissie van de Lokale Politie was voorzien, terwijl dit een louter strategisch beleidsorgaan is;
- ze vroegen of de valideringsregels van de verschillende diensten bij de aangifte konden worden gevoegd;
- ze bevalen aan om, met het oog op de effectieve opvolging van hun controleopdracht, in de mogelijkheid te voorzien om een historiek van de inlichtingenfiches en informatiekaarten te ontvangen;
- ze merkten op dat de voorwaarden van samenwerking met buitenlandse inlichtingendiensten nog dienden bepaald te worden door de Nationale Veiligheidsraad. Eenzelfde vaststelling gold voor het OCAD voor wat betreft de samenwerking met buitenlandse homologen.

VI.3.2. EEN TWEEDE ADVIES

Na de publicatie van het KB FTF werd door de ministers op 3 november 2016 een aangepaste aangifte doorgestuurd, samen met een *user guide*.

Het tweede advies van het COC en het Vast Comité I werd uitgebracht op 1 december 2016 (zie bijlage F). Het betrof een, onder voorbehoud van enkele opmerkingen, gunstig advies. Samenvattend stelde het COC en het Vast Comité I dat:
- er (nog steeds) geen melding was gemaakt van de aanstelling van een consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer. Het belang van deze rol werd benadrukt en er werd aangedrongen op een snelle aanstelling. Daarentegen werd door de Comités met tevredenheid vastgesteld dat dergelijke consulenten er wel waren op het niveau van de diensten die toegang hebben tot de gegevensbank FTF;
- ze herhaalden dat het basisprincipe van de toegang door de verschillende diensten de '*need to know*' moet zijn;
- ze bevalen aan dat de diensten in staat moeten zijn om, elk via hun respectievelijke consulenten voor veiligheid, te vermelden voor welke concrete doeleinden de toegang legitiem is (in het bijzonder voor wat betreft de functies van de personen die over een toegang beschikken);
- er werd vastgesteld dat de modaliteiten voor de directe toegang door de justitiehuizen en het Vlaams Agentschap Jongerenwelzijn nog moesten worden gedefinieerd in een aanvullende aangifte;

- ze merkten op dat geen gewag werd gemaakt van de noodzaak voor de controlediensten om te kunnen beschikken over een historiek van de verwerkte gegevens. Er werd op gewezen dat het waken over de traceerbaarheid een van de opdrachten is van de beheerder van de FTF-gegevensbank, met name de Federale Politie;
- ze stelden vast dat de valideringssystemen zoals beschreven in de aangifte vaak te summier of zelfs helemaal onbestaand waren. Ze riepen de betrokken diensten dan ook op erover te waken dat de persoonsgegevens die de diensten inbrengen relevant, ter zake dienend en niet overmatig zijn.

HOOFDSTUK VII
ADVIEZEN, STUDIES EN ANDERE ACTIVITEITEN

Het wettelijk takenpakket van het Vast Comité I is zeer verscheiden: het uitvoeren van toezichtonderzoeken, rechtscollege inzake bijzondere inlichtingenmethoden, opdrachten in het kader van de interceptiebevoegdheid van de ADIV, de controle van de dynamische databank FTF en de gemeenschappelijke adviezen met het Controleorgaan op de politionele informatie, de invulling van gerechtelijke taken door zijn Dienst Enquêtes, zijn rol in het Beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen… Daarnaast levert het Comité ook studies af en wordt het geconsulteerd omwille van zijn expertise. Het Comité werd in 2016 viermaal verzocht een officieel advies te verlenen bij diverse kwesties.

VII.1. ADVIES OVER HET VOORONTWERP VAN WET TOT WIJZIGING VAN DE INLICHTINGENWET

In zijn brief van 22 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.[209] Het wetsontwerp '*strekt ertoe de organieke wet te verbeteren, en te verduidelijken door de ondervonden operationele problemen te ondervangen zonder te taken aan de bestaande methoden, de garanties waarin is voorzien om de fundamentele rechte van de burgers te beschermen, of de verschillende controles*'.[210]

Het Comité benadrukte in zijn advies voorstander te zijn van elk voorstel dat de efficiëntie van de Belgische inlichtingendiensten kan verhogen voor zover er voldoende waarborgen worden ingebouwd voor de vrijwaring van de fundamen-

[209] Gelet op het uiterst korte tijdsbestek 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 van het Vast Comité I dateert van 4 maart 2016. Het advies werd integraal opgenomen in de bijlagen E van onderhavig verslag.

[210] *Parl. St.* Kamer, 2015-16, 54K2043/001.

tele rechten en vrijheden. Dit geldt zeker in de huidige maatschappelijke context waarin de strijd tegen het terrorisme en het radicalisme optimaal moet kunnen gevoerd worden.

Het Comité kon vaststellen dat het ontwerp grotendeels rekening hield met zijn in de loop der jaren geformuleerde aanbevelingen, doch op een aantal vlakken werden ingrijpende wijzigingen aan de Inlichtingenwet in het vooruitzicht gesteld die verder reikten dan de bepalingen die werden toegevoegd middels de BIM-Wet van 4 februari 2010 (zoals bijvoorbeeld de collectemogelijkheden van de ADIV in het buitenland). Andere wettelijke bepalingen – eveneens voor verbetering vatbaar[211] – bleven onbesproken.

Het Comité was van oordeel dat de evaluatie van de toen actuele regeling grotendeels vanuit de efficiëntie van de inlichtingendiensten gebeurde. Dit vertaalde zich in een ontwerp dat vooral resulteert in méér (soms nuttige en noodzakelijke) bevoegdheden en wettelijke mogelijkheden voor de twee inlichtingendiensten, waarbij er niet steeds voldoende aandacht is voor de externe controle en de noodzakelijke *checks and balances*. Meer nog, deze externe controle bleek soms te worden afgebouwd.[212]

VII.2. ADVIES BIJ HET WETSONTWERP TOT REGELING VAN DE PRIVATE VEILIGHEID

Eind september 2016[213] verzocht de minister van Veiligheid en Binnenlandse Zaken de voorzitter van het Vast Comité I, die tevens voorzitter is van Beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, om zijn advies te formuleren bij de bepalingen van het Wetsontwerp tot regeling van de private veiligheid die het Beroepsorgaan aanbelangen.[214] Het was immers de intentie van de regering om het contentieux inzake het onderzoek naar de veiligheidsvoorwaarden voor het bekomen van een vergunning in de sector van de private bewaking over te dragen aan het Beroepsorgaan. De krachtlijnen van

---

211 Zoals bijvoorbeeld de aanbeveling dat de artikelen 19 en 20 W.I&V nader zouden worden uitgewerkt door de uitvoerende en de wetgevende macht. Deze cruciale bepalingen regelen onder meer de informatieoverdracht (inbegrepen persoonsgegevens) naar andere (buitenlandse) diensten en de medewerking/technische bijstand die beide Belgische diensten kunnen verlenen aan de gerechtelijke autoriteiten of aan buitenlandse homologen.

212 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 werd gepubliceerd in het Belgisch Staatsblad van 28 april 2017.

213 Brief van de minister van Veiligheid en Binnenlandse Zaken aan de Voorzitter van het Beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen d.d. 28 september 2016.

214 *Parl. St.* Kamer 2016-17, nr. 54K2388/007 (Wetsontwerp tot regeling van de private en bijzondere veiligheid).

het advies werden doorgesproken met de leden van het Vast Comité P en de Privacycommissie die zetelen in het Beroepsorgaan.[215]

In zijn advies benadrukte het Beroepsorgaan op zich niet weigerachtig te staan tegenover het voorstel om een deel van het administratieve contentieux inzake de private veiligheid naar het Beroepsorgaan over te hevelen. Gezien dit een aanzienlijke bijkomende werklast zou betekenen, werden in het advies voorstellen tot efficiëntiewinst geformuleerd (de invoering van een eenvoudige beroepsakte, verplichte antwoordtermijnen, een hoorplicht door de betrokken overheid…). Eveneens werden voorstellen toegevoegd over de wijziging van de Classificatiewet van 11 december 1998 alsook over de wijziging van de Wet van 11 december 1998 tot oprichting van het Beroepsorgaan. Ten slotte werden een aantal bedenkingen geformuleerd tot de voorgestelde regeling in verband met het 'onderzoek naar de veiligheidsvoorwaarden'. De nieuwe Wet tot regeling van de private en bijzondere veiligheid werd op 8 juni 2017 aangenomen in plenaire zitting. Het contentieux werd uiteindelijk niet overgedragen aan het Beroepsorgaan en bleef bij de Raad van State.

VII.3. INFORMATIEDOSSIERS

Naast toezichtonderzoeken (Hoofdstuk II), 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.[216] 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 verder gevolg.

In 2016 werd bijvoorbeeld een informatiedossier geopend naar de problematiek van het wetenschappelijk en economisch belang van het land en de rapportage van de VSSE over de eventuele participatie in EANDIS door een Chinees energiebedrijf, werd informatie verzameld over de problematiek van informantenwerking en rekrutering alsook over de contacten met ambassades. Deze dossiers kregen geen verdere opvolging.

---

215 Het advies werd integraal opgenomen in de bijlagen D van onderhavig verslag. Er werd voor geopteerd om dit advies op bijzonder korte termijn te verlenen, gezien het snel op de Ministerraad ging worden besproken. Hierdoor kon niet op elk aspect in detail worden ingegaan. Zie hierover eveneens 'Hoofdstuk VIII. De griffie van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en –adviezen'.

216 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…

VII.4. EXPERT OP DIVERSE FORA

Leden van het Vast Comité I en van zijn personeel werden in 2016 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 mei 2016 organiseerde het BISC een studiedag over 'Big Data en de inlichtingendiensten: perspectieven en toekomstige uitdagingen';
- er werd eveneens een beroep gedaan op de expertise van het Comité in een praktijkseminarie bestemd voor politie, magistratuur en advocatuur inzake de 'screening van personen' en dit in de context van de Wet betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen;
- de griffier nam eind januari 2016 deel aan een panelgesprek over 'Intelligence services' surveillance in the EU: fundamental rights, safeguards and remedies' in het kader van de internationale conferentie 'Computers, Privacy & Data Protection. [In]visibilities & Infrastructures' georganiseerd in Brussel;
- de voorzitter van het Comité nam in maart 2016 in het Europees Parlement, samen met onder meer de *EU Counter-Terrorism Coordinator* en de directeur van Europol deel aan een panelgesprek over '*The EU response to counter terrorism and the parliament's right to scrutinity*' in het kader van de conferentie '*Counter terrorism, security and human rights*';
- een delegatie van het Vast Comité I nam deel aan expertenmeetings 'National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies', georganiseerd op initiatief van het hoofd van de Sector of Information Society, Privacy and Data Protection Freedoms and Justice Department van het European Union Agency for Fundamental Rights (FRA). Deze is, in opdracht van het Europees Parlement en naar aanleiding van de Resolutie van 12 maart 2014, belast met een vergelijkende studie over democratisch toezicht op de inlichtingendiensten in de Europese lidstaten[217];
- de griffier van het Vast Comité I werd opnieuw uitgenodigd in het kader van het opleidingsonderdeel 'Intelligence' van Master in de internationale betrekkingen en de diplomatie (Universiteit Antwerpen) om er de werking van het Comité toe te lichten;

[217] 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 voorzitter van het Comité werd door de *Organisation internationale de la francophonie* (OIF) betrokken in de organisatie van de Conferentie inzake de strijd tegen terrorisme en de preventie van gewelddadige radicalisering die plaatsvond in Parijs;
- het Comité blijft tevens deelnemen aan de vergaderingen van de *Groupe européen de recherche sur l'éthique du renseignement* (GERER). Hierin reflecteert een werkgroep, samengesteld uit vertegenwoordigers vanuit het academische wereld en practici (vertegenwoordigers vanuit de (militaire) Franse, Belgische en Luxemburgse inlichtingendiensten, het Vast Comité I…) over de relatie 'ethiek – inlichtingendiensten';
- de adjunct-directeur van de Dienst Enquêtes trad in februari 2016 op als expert voor het *Geneva Centre for the Democratic Control of Armed Forces* (DCAF) en de Republiek Tunesië in het kader van de rondetafelgesprekken '*Quelle gouverance des services de renseignement dans une société démocratique*'. Het ging er onder meer over de hervorming van de inlichtingendiensten in een gewijzigde democratische context, de controle op de inlichtingendiensten, de wijze van uitwisseling van inlichtingen in een internationale context en de prioriteitenstelling van inlichtingendiensten;
- in oktober 2016 nam de voorzitter van het Comité, op uitnodiging van de Voorzitster van de Senaat, als gastspreker deel aan het colloquium 'De impact van de nieuwe technologieën op onze privacy en de gegevensbescherming: wat staat er op het spel'. Daar werd 'De bescherming van de persoonlijke levenssfeer op het vlak van veiligheid en openbaar leven' toegelicht;
- in 2016 gaf de voorzitter op vraag van het Departement de Sciences Politiques van de Rechtsfaculteit van de Universiteit van Luik twee uiteenzettingen over *'Le renseignement, ses défis et son contrôle'* en *'Le contrôle parlementaire'*;
- 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 in november 2016 deel aan rondetafelgesprekken over *'Accès à l'information: défis et opportunités pour la communauté du renseignement'*. Volgende onderwerpen kwamen daarbij aan bod: *'Concilier transparence et sécurité de l'Etat et des citoyens'*, *'Établir un système de classification de l'information'*, *'Concilier transparence et efficacité de la communauté du renseignement'* en *'Garantir l'accès à l'information pour les acteurs de supervision et de contrôle de la communauté de renseignement'*;
- in november 2016 nam de voorzitter in Parijs het woord tijdens het *'Fourth Seminar of the Queen Mary, Reflection Group on Terrorism and Human Rights'*; hij deed dit in het kader van een panelgesprek over *'Inscribing in law oversight powers in respect of intelligence services'*.

VII.5. SAMENWERKINGSPROTOCOL MENSENRECHTEN

Het ontbreekt België – in tegenstelling tot 22 andere Europese landen – nog steeds aan een formeel, federaal mensenrechteninstituut.[218] Vergaderingen met andere instellingen met een mandaat op gebied van mensenrechten[219], resulteerde halfweg januari 2015 in een samenwerkingsprotocol[220] waarin alle deelnemende instanties overeen kwamen om hun praktijken en methoden uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen. Deze fungeren, in afwachting van een mensenrechteninstituut, als een gemeenschappelijk overlegplatform van instellingen die door een volledig of gedeeltelijk mandaat gelast zijn met het toezicht op de eerbiediging van de fundamentele rechten en vrijheden.

De activiteiten van dit platform namen in 2016 de vorm aan van maandelijkse overlegvergaderingen waarin zowel algemene problematieken (bijv. de maatregelen genomen door de federale en regionale overheden ingevolge de aanslagen in Parijs en de bestrijding van de radicalisering, het nieuwe Europese reglement inzake de bescherming van persoonsgegevens, de wijze van afhandeling van klachten en aangiften…), als zeer concrete casussen worden besproken. Ook werd de website HRights gerealiseerd, een uitwisselingsplatform voor de deelnemende instellingen.[221]

VII.6. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

In oktober 2015 vond in Bern een vergadering onder toezichthouders plaats, met delegaties vanuit Zwitserland, Nederland en België alsook de Scandinavische landen Zweden, Noorwegen en Denemarken. Er werden vijf topics geagendeerd: (het meten van) efficiëntie, de toegang voor de toezichthouders tot informatie van de betrokken inlichtingendiensten, het inzicht in lopende operaties en de internationale uitwisseling van gegevens tussen inlichtingendiensten en tussen toezichthouders en het toezicht op het gebruik van persoonsgegevens door inlichtingendiensten. De vergadering besliste een gelijkaardig toezichtonderzoek op te starten

---

218 De Mensenrechtenraad van de Verenigde Naties stelde dit vast in 2011 tijdens zijn zogenaamd 'Universeel Periodiek Onderzoek (UPO)'. In 2016 diende dit opnieuw te worden vastgesteld.

219 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.

220 Samenwerkingsprotocol van 13 januari 2015 tussen de instellingen met een volledig of gedeeltelijk mandaat belast met de eerbiediging van de rechten van de mens.

221 Het secretariaat van dit platform wordt waargenomen door de administratieve diensten van de grootste deelnemende organisaties.

in alle deelnemende landen over de internationale samenwerking tussen de diverse inlichtingendiensten met betrekking tot de strijd tegen de *foreign terrorist fighters*. Het ligt daarbij in de bedoeling dat elke toezichthouder, vanuit zijn eigen perspectief en bevoegdheid maar vanuit eenzelfde filosofie en met een zekere gemeenschappelijke aanpak, dit thema bestudeert.[222] In navolging van deze vergadering, werden in april 2016 in Den Haag de onderzoeksvragen besproken, alsook de te hanteren definities en het wettelijk kader inzake diverse vormen van samenwerking in Europa.[223] In september 2016 in Brussel en vervolgens eind november 2016 in Den Haag, werd in opvolgvergaderingen voorzien waarin onder meer de structuur van het gezamenlijk publiek rapport en de vooruitgang in de verschillende onderzoeken (*best practices*, risico's, definities…) aan de orde waren.

Op 7 april 2016 vond een bezoek plaats van de Franse onderzoekscommissie '*relative aux moyens mis en oeuvre par l'Etat pour lutter contre le terrorisme depuis le 7 janvier 2015*' van de Franse *Assemblée nationale* onder leiding van hun voorzitter. De delegatie ontmoette de voorzitter van het Vast Comité I, de ondervoorzitter van het Vast Comité P en de voorzitter en ondervoorzitters van de Commissie Terrorismebestrijding.[224]

Nog in april 2016 werd door het Vast Comité I deelgenomen aan de wetenschappelijke conferentie *'Intelligence and democratic oversight from the end of the Cold War until today – key trends and developments'* en dit naar aanleiding van het twintigjarig bestaan van het Noorse parlementair toezichtorgaan (EOS-Committee). In het verlengde daarvan vonden contacten plaats met de *Interception of Communications Commissioner's Office* (IOCCO) van het Verenigd Koninkrijk.

Verder onderhield het Vast Comité I in 2016 ook nauwe contacten met de Franse *Commission nationale de contrôle des interceptions de sécurité* (CNCIS) en de nieuwe *Commission nationale de contrôle des techniques de renseignement* (CNCTR). Op 23 juni 2016 vond een werkbezoek in Brussel plaats.

In de marge van het *International Intelligence Oversight Forum*, georganiseerd in Boekarest half oktober 2016 door de *Special Rapporteur for Privacy* (SRP) van de Verenigde Naties samen met de vier commissies van het Roemeense parlement die elk bevoegd zijn voor een aspect van de werking van de inlichtingendiensten[225], onderhield een delegatie van het Vast Comité I informele contacten met

222 Zie VAST COMITÉ I, Activiteitenverslag 2015, 80-81.

223 De vergadering werd voorafgegaan door een uiteenzetting van de directeur-generaal van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en tevens voorzitter van de Counter Terrorism Group (CTG) over de uitwisseling van persoonlijke gegevens over foreign terrorist fighters in de CTG.

224 Hun bevindingen resulteerden in een eindrapport (www.assemblee-nationale.fr/14/rap-enq/r3922-t1.asp).

225 The Joint Permanent Commission of the Chamber of Deputies and the Senate to exercise parliamentary control over the activity of the SRI, the Special Commission of the Chamber of Deputies and the Senate to exercise parliamentary control over the activity of the Foreign Intelligence Service, the Committee for Defense, Public Order, and National Security in the

toezichthouders uit Nederland, het Verenigd Koninkrijk, Canada, Denemarken, Duitsland… Het doel van dit forum bestond erin om in een vertrouwelijke omgeving een beter begrip te krijgen in de uitdagingen waarmee democratische toezichtorganen worden geconfronteerd in een digitale wereld.

Half december 2016 ten slotte bracht een Zwitserse delegatie een bezoek aan het Vast Comité I waarbij de nadruk kwam te liggen op een toelichting over de wijze waarop de controle op de toepassing van de bijzondere inlichtingenmethoden in België wordt georganiseerd.

VII.7. CONTROLE OP DE SPECIALE FONDSEN[226]

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. Sinds 2006 wordt de controle van de speciale fondsen van de ADIV alleen uitgevoerd door het hoofd van de Krijgsmacht 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 2016 was de voorzitter aanwezig bij deze controle.

VII.8. 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.

Chamber en the Committee for Defense, Public Order, and National Security in the Senate. Het initiatief werd mede ondersteund door het Department of Information Policy and Governance van de Universiteit van Malta en de Security, Technology & e-Privacy Research Group van de Universiteit van Groningen.

226 Zie hierover tevens VAST COMITÉ I, *Activiteitenverslag 2015*, 12-16 ('II.2. Het beheer, het gebruik en de controle van de speciale fondsen'). Het Comité formuleerde daarbij diverse aanbevelingen, in *Activiteitenverslag 2015*, 102-103 ('IX.2.2. Aanbevelingen inzake het beheer van en de controle op de speciale fondsen').

Datum	Onderwerp/titel	Forum
6 januari 2016	'Les services secrets belges pourront espionner les espions étrangers'	Le Soir
7 januari 2016	'Spionnen mogen collega's controleren'	Het Laatste Nieuws
12 februari 2016	'Dertigtal salafistische moskeeën in België'	Het Laatste Nieuws
26 februari 2016	'Staasveiligheid onterecht kop van Jut'	De Tijd
22 maart 2016	'Aanslagen in Brussel: kroniek van een aangekondigde dood'	Knack
24 maart 2016	'Les services de renseignements belges ont-ils failli durant leur enquête?'	Le Soir
25 maart 2016	'Police, renseignement: imbroglio à la belge'	Libération
29 maart 2016	'Politie krijgt terreurinformatie niet verwerkt'	De Morgen
2 april 2016	'La radicalisation en prison négligée depuis des années'	L'Echo
2 april 2016	'Radicalisering in gevangenis laat aangepakt'	De Tijd
17 april 2016	'Sécurité Brussels Airport: "On en va pas transformer Zaventem en Bunker mais il y a des problèmes a résoudre"'	RTBF
27 april 2016	'Terrorisme: le Comité R sévère avec les renseignements belges'	RTBF
28 april 2016	'Les services de renseignement belges sont-ils à la hauteur?'	RTBF
28 april 2016	'La Défense gratte les fonds de tiroir, mais ne peut se passer de nouveaux avions'	RTBF
12 mei 2016	'Te weinig informanten in strijd tegen terroristen'	De Tijd
12 mei 2016	'Trop peu d'indicateurs pour nos services secrets'	L'Echo
12 mei 2016	'22 nieuwe spionnen voor Staatsveiligheid, maar er is meer nodig'	De Standaard
12 mei 2016	'La Sûreté de l'État n'avait aucun informateur pour les frères Abdeslam'	Le Soir
18 mei 2016	'Kritieke infrastructuur onvoldoende beschermd'	De Tijd
19 mei 2016	'La Sûreté et le SGRS ne se parlent pas assez'	La Libre Belgique
11 augustus 2016	'De bewaking van de bewakers'	Trends

Datum	Onderwerp/titel	Forum
6 september 2016	'La commission "attentats" s'attaque à l'enquête'	Le Soir
14 september 2016	'Mag de Staatsveiligheid samenwerken met folterende inlichtingendiensten?'	Knack
17 september 2016	'Als Michael Freilich spreekt, moet iedereen zwijgen'	De Morgen
27 september 2016	'Waarom de Staatsveiligheid het moeilijk heeft met Eandis'	De Tijd
5 oktober 2016	'Renseignements: recrutement à la traîne'	L'Avenir
12 oktober 2016	'Staatsveiligheid krijgt eigen politie'	De Standaard
12 oktober 2016	'Leger mag voluit spioneren'	De Standaard
21 oktober 2016	'Staatsveiligheid: Eens geheim, altijd geheim? Onzin?'	Knack
2 november 2016	'Parijs-Brussel aller-retour – Caroline Van den Berghe & Dirk Leestmans'	De Redactie
18 november 2016	'Nog te weinig terreurinfo uitgewisseld'	VTM nieuws
16 december 2016	'Mogelijk 450 gevangenen geradicaliseerd'	De Tijd
22 december 2016	'Al vijfde valse start voor proces tegen Syriëstrijders'	Het Laatste Nieuws
22 december 2016	'Comité P, Comité I en Privacycommissie zijn "virtueel failliet" '	De Redactie
23 december2016	'Tiental salafisten in Belgische leger'	Het Laatste Nieuws
23 december 2016	'Une dizaine de salafistes dans l'armée belge'	La Libre Belgique

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.[227] 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*

---

227 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).

In 2016 voerde de Dienst Enquêtes I enkele onderzoeksdaden (een verhoor en de inventarisatie van een dossier) uit in het kader van een gerechtelijk onderzoek dat zonder gevolg werd geklasseerd in februari 2015 maar opnieuw werd geopend wegens burgerlijke partijstelling van een familielid van het slachtoffer.

HOOFDSTUK IX

DE GRIFFIE VAN HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN

De voorzitter van het Vast Comité I neemt het voorzitterschap van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen waar. De griffiefunctie wordt uitgeoefend door de griffier en door de administratie van het Vast Comité I.

Het Beroepsorgaan is bevoegd voor geschillen die betrekking hebben op 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.[228]

Deze activiteiten van het Beroepsorgaan hebben een directe impact op zowel de budgettaire als personele middelen van het Vast Comité I. Immers worden alle werkingskosten gedragen door het Vast Comité I, dat daarnaast niet enkel én de voorzitter én de griffier levert, doch ook het nodige administratief personeel dat moet instaan voor de tijdsintensieve voorbereiding, de behandeling en de afhandeling van de beroepen.

In dit hoofdstuk worden de aard van de bestreden beslissingen, de hoedanigheid van de bevoegde overheden en van de verzoekers en de aard van de beslissingen van het Beroepsorgaan binnen de verschillende beroepsprocedures cijfermatig weergegeven. Om enige vergelijking mogelijk te maken, werden de cijfers van de afgelopen vijf jaar eveneens opgenomen.

In 2016 kende het aantal beroepen en beslissingen een significante stijging tegenover het jaar voordien, te weten van respectievelijk 130 naar 169 en van 137 naar 173. Daarmee komt het aantal beroepen en beslissingen globaal terug op het

[228] Zie hierover uitgebreid VAST COMITÉ I, *Activiteitenverslag 2006,* 91-119.

niveau van 2014. De in 2016 vastgestelde verhoging doet zich in het bijzonder voor qua aantal beroepen tegen negatieve veiligheidsadviezen (van 63 naar 101). Deze stijgende tendens is ook zichtbaar bij het aantal ingestelde beroepen tegen geweigerde veiligheidsattesten met betrekking tot de nucleaire sector[229], terwijl het aantal geweigerde veiligheidsattesten die toegang verlenen tot geclassificeerde zones de tegenovergestelde beweging kent. Het opvragen van aanvullende informatie (van 7 naar 23) en het horen van de klager en zijn advocaat (van 107 naar 127) zitten op hun beurt dan weer in een stijgende lijn.

Achter deze cijfers gaat een toegenomen werklast schuil voor zowel de griffie als voor het Beroepsorgaan zelf. De te behandelen dossiers worden immers steeds complexer op het vlak van administratief beheer, de terechtzittingen en de beslissingen.

Zo voldoen heel wat verzendingen niet aan 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.[230] Hetzelfde geldt voor de administratieve dossiers die door de diverse veiligheidsoverheden worden overgezonden; deze blijken niet steeds compleet zodat de griffie ook hier bijkomende handelingen moet stellen om ze te vervolledigen. In dezelfde zin blijkt de toepassing van artikel 5 § 3 W.Beroepsorg. problematisch: het verzoek om bepaalde stukken niet ter inzage te verlenen 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.[231]

---

229 Deze laatste categorie veiligheidsattesten werd ingevoegd door de Wet van 30 maart 2011 houdende wijziging van de Wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle en houdende wijziging van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *BS* 18 april 2011. Omwille van de duidelijkheid, en rekening houdende met de toekomstige evoluties wat betreft veiligheidsattesten afgeleverd in de nucleaire sector, wordt over dit type van attesten vanaf huidig activiteitenverslag apart gerapporteerd.

230 Omwille van de zeer korte termijnen, is het beroep in deze gevallen dan ook vaak laattijdig en dus onontvankelijk.

231 Artilel 5 § 3 W.Beroepsorg. laat het Beroepsorgaan op verzoek van een inlichtingen- of politiedienst toe te beslissen sommige stukken uit het onderzoeksdossier ter inzage van de eiser (of zijn advocaat) te halen, mocht blijken dat de verspreiding ervan een gevaar zou inhouden voor de bescherming van de bronnen, de persoonlijke levenssfeer van derder 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 nog uitgebreid door het Beroepsorgaan toe te laten, nog steeds op verzoek van een betrokken dienst, de 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 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

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.

Diverse elementen leiden ertoe aan te mogen nemen dat de werklast van het Beroepsorgaan in de toekomst nog (gevoelig) zal toenemen. De regering heeft zijn voornemen aangekondigd om de moraliteitsonderzoeken ('screenings') op te drijven, in het bijzonder met het oog op de verhoging van de veiligheid van kritieke infrastructuren. Diverse ontwerpteksten in die zin circuleren reeds. Deze verhoging zal niet zonder gevolg blijven voor de middelen waarover het Vast Comité I beschikt. Het volstaat te onderlijnen dat de regering in eerste instantie overwoog om het administratieve contentieux inzake de private veiligheid (toegangspoort naar het beroep bewakingsagent) naar het Beroepsorgaan over te hevelen.[232] Uiteindelijk werd deze piste verlaten.

Tot slot dient te worden gemeld dat door het Beroepsorgaan aan de bevoegde instanties – en inzonderheid aan de Nationale Veiligheidsoverheid (NVO) – zijn grote bezorgdheid kenbaar werd gemaakt over de extreem complexe wetgeving en de soms te beperkte rechten van de burger (bijv. te korte beroepstermijnen).

gevallen waarin de betrokken dienst manifest vergeten was zich te beroepen op art. 5 § 3 W. Beroepsorg.

232 Cf. 'VII.2. Advies bij het wetsontwerp tot regeling van de private veiligheid'. Het advies werd gevoegd als bijlage D van dit activiteitenverslag.

Tabel 1. Betrokken veiligheidsoverheid

	2012	2013	2014	2015	2016
Nationale Veiligheidsoverheid	40	98	99	68	92
Veiligheid van de Staat	0	1	0	1	0
Algemene Dienst Inlichting en Veiligheid	27	78	60	47	68
Federaal Agentschap voor Nucleaire Contrôle	11	9	8	10	8
Federale Politie	1	1	3	3	1
Lokale Politie	2	2	1	1	0
Lokale Luchthavencommissie	10	–	–	–	–
TOTAAL	**91**	**189**	**171**	**130**	**169**

Tabel 2. Aard van de bestreden beslissing

	2012	2013	2014	2015	2016
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)					
Vertrouwelijk	7	5	5	9	5
Geheim	29	56	43	35	38
Zeer geheim	9	5	4	4	7
Weigering	33	41	25	36	28
Intrekking	12	5	9	7	9
Weigering en intrekking	0	4	0	0	0
Machtiging voor beperkte duur	0	1	2	3	4
Machtiging voor lager niveau	1	0	1	0	1
Geen beslissing binnen termijn	1	15	15	2	7
Geen beslissing binnen verlengde termijn	0	0	0	0	1
Subtotaal veiligheidsmachtigingen	**45**	**66**	**52**	**48**	**50**
Veiligheidsattesten toegang geclassificeerde zones (art. 22*bis*, al.1 W.C&VM)					
Weigering	23	0	4	6	1
Intrekkig	0	0	0	0	0

	2012	2013	2014	2015	2016
Geen beslissing binnen termijn	0	0	0	0	0
Veiligheidsattesten plaats of gebeurtenis (art. 22*bis*, al. 2 W.C&VM)					
Weigering	0	15	16	12	9
Intrekking	0	0	0	1	0
Geen beslissing binnen termijn	0	0	0	0	0
Veiligheidsattesten voor de nucleaire sector (art. 8*bis*, § 2 W.C&VM)					
Weigering	–	–	–	–	7
Intrekking	–	–	–	–	1
Geen beslissing binnen termijn	–	–	–	–	0
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)					
Negatief advies	23	106	99	63	101
Geen advies	0	2	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	**46**	**123**	**119**	**82**	**119**
TOTAAL BESTREDEN BESLISSINGEN	**91**	**189**	**171**	**130**	**169**

Tabel 3. Hoedanigheid van de verzoeker

	2012	2013	2014	2015	2016
Ambtenaar	5	4	0	4	2
Militair	26	26	17	29	23
Particulier	54	159	145	93	139
Rechtspersoon	6	0	6	4	5

Tabel 4. Taal van de verzoeker

	2012	2013	2014	2015	2016
Franstalig	51	92	92	75	99
Nederlandstalig	40	97	76	54	70
Duitstalig	0	0	0	0	0
Anderstalig	0	0	0	1	0

Tabel 5. Aard van de door het Beroepsorgaan genomen voorbereidende beslissingen[233]

	2012	2013	2014	2015	2016
Volledig dossier opvragen (1)	90	187	168	130	167
Aanvullende informatie opvragen (2)	5	12	16	7	23
Horen lid overheid (3)	10	3	11	7	10
Beslissing voorzitter (4)	0	0	0	0	0
Informatie uit dossier halen door Beroepsorgaan (5)	44	68	78	50	54
Informatie uit dossier halen door inlichtingendienst (6)	0	0	0	0	0

(1) Het Beroepsorgaan beschikt over de mogelijkheid het gehele onderzoeksdossier bij de veiligheidsoverheden op te vragen. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan.

233 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 2016, terwijl de beslissing pas viel in 2017.

(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 (*supra*).
(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

	2012	2013	2014	2015	2016
Dossierinzage door klager / advocaat	54	103	84	84	87
Horen van de klager / advocaat[234]	65	138	115	107	127

Tabel 7. Aard van de beslissingen van het Beroepsorgaan

	2012	2013	2014	2015	2016
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)					
Beroep onontvankelijk	0	2	0	4	0
Beroep zonder voorwerp	1	3	3	3	7
Beroep ongegrond	19	20	12	19	18
Beroep gegrond (volledige of gedeeltelijke toekenning)	23	35	14	24	24
Bijkomende onderzoeksdaden door overheid	1	0	0	0	2
Bijkomende termijn voor overheid	0	14	12	1	2
Zonder gevolg	0	0	0	1	0

234 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.

	2012	2013	2014	2015	2016
Veiligheidsattesten toegang geclassificeerde zones (art. 22*bis*, al. 1 W.C&VM)					
Beroep onontvankelijk	0	0	0	0	0
Beroep zonder voorwerp	0	0	0	0	0
Beroep ongegrond	0	0	2	4	1
Beroep gegrond (toekenning)	0	0	0	2	1
Veiligheidsattesten plaats of gebeurtenis (art. 22*bis*, al. 2 W.C&VM)					
Beroep onontvankelijk	3	1	0	0	0
Beroep zonder voorwerp	1	0	0	0	0
Beroep ongegrond	8	6	6	8	2
Beroep gegrond (toekenning)	6	11	8	10	4
Verleent akte van afstand van beroep	0	0	0	2	0
Veiligheidsattesten voor de nucleaire sector (art. 8*bis* § 2 W.C&VM)					
Beroep onontvankelijk	–	–	–	–	1
Beroep zonder voorwerp	–	–	–	–	1
Beroep ongegrond	–	–	–	–	0
Beroep gegrond (toekenning)	–	–	–	–	7
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)					
Beroep onbevoegd	5	0	4	0	0
Beroep onontvankelijk	1	4	4	6	15
Beroep zonder voorwerp	0	1	4	0	0
Bevestiging negatief advies	9	25	53	28	42
Omvorming in positief advies	4	65	41	23	46
Beroep tegen normatieve rechtshandelingen (art. 12 W.Beroepsorg.)	0	0	0	0	0
TOTAAL	**81**	**187**	**163**	**137**[235]	**173**

[235] Er waren nog twee specifieke beslissingen van verlenen akte van afstand van beroep waardoor het totaal in 2015 op 137 kwam.

HOOFDSTUK X
DE INTERNE WERKING VAN HET VAST COMITÉ I

X.1. SAMENSTELLING VAN HET VAST COMITÉ I

De samenstelling van het Comité bleef in 2016 ongewijzigd: voorzitter Guy Rapaille (F), advocaat-generaal bij het hof van beroep te Luik en raadsheren Gérald Vande Walle (F) en Pieter-Alexander De Brock (N).

Ook bij de Dienst Enquêtes I vielen er geen wijzigingen te noteren. De dienst bestond uit vijf commissaris-auditoren, waaronder de directeur Frank Franceus (N).

De administratieve staf van het Vast Comité I, onder leiding van griffier Wouter De Ridder (N), kende evenmin verschuivingen en bleef op een totaal van 16 personeelsleden.

X.2. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE

In de loop van 2016 vonden zes vergaderingen plaats met de Bijzondere commissie belast met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de veiligheids- en inlichtingendiensten. Deze telde nog steeds dertien stemgerechtigde leden[236], doch de samenstelling van de Commissie wijzigde meermaals in 2016. Ze werd als volgt aangewezen: Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Peter De Roover (N-VA), Laurette Onkelinx (PS), André Frédéric (PS), 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) en Georges

[236] 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*').

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 belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven van Brussel Nationaal en het metrostation Maalbeek te Brussel, met inbegrip van de evolutie in de aanpak van de strijd tegen het radicalisme en de terroristische dreiging'. Het mag dan ook niet verbazen dat alle vergaderingen van de Begeleidingscommissie plaatsvonden in de eerste helft van 2016, en dat vanaf dan het accent kwam te liggen op de werkzaamheden voor de onderzoekscommissie.

Tijdens de zes commissievergaderingen werden – achter gesloten deuren – diverse 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. Verder werd het *Activiteitenverslag 2015* van het Vast Comité I besproken. De Commissie nam '*akte van het activiteitenverslag 2015 van het Comité I en verleent haar goedkeuring aan de aanbevelingen van het Comité*'.[237] 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).

X.3. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITÉ P

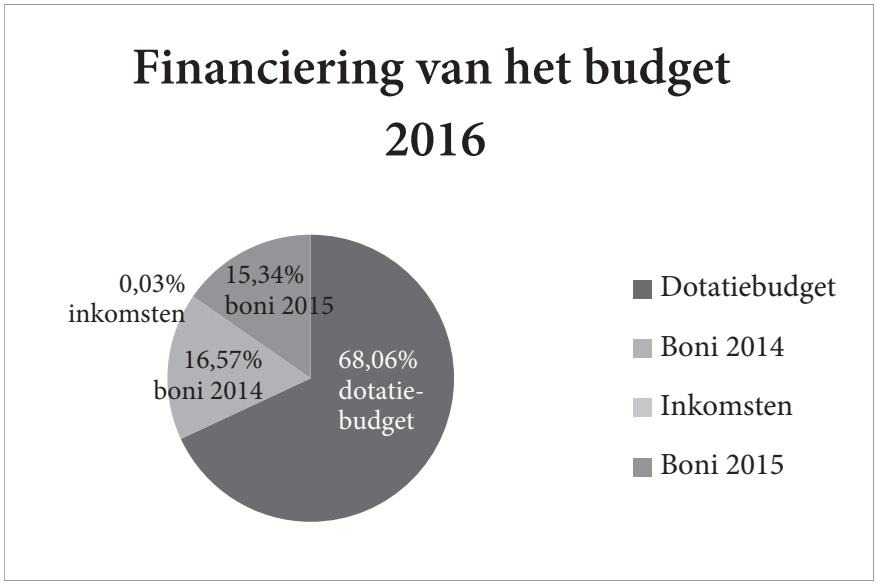
De artikelen 52 tot 55 W.Toezicht bepalen de gevallen waarin en de wijze waarop het Vast Comité I en het Vast Comité P gemeenschappelijke vergaderingen dienen te organiseren. Het voorzitterschap van deze gezamenlijke vergaderingen wordt afwisselend waargenomen door de voorzitters van beide Vaste Comités (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. Begin juli 2016 werd een bijzondere vergadering integraal gewijd aan het Coördinatieorgaan voor de dreigingsanalyse. Daartoe werden de directeur en de adjunct-directeur van het OCAD uitgenodigd om hun visie op het OCAD weer te geven. Verder werd er overlegd over de aanpak van het structureel begrotingsprobleem van alle dotatiegerichte instellingen en bleken beide comités het erover eens dat moet worden gewerkt aan een gemeenschappelijke methodologie, in de eerste plaats voor de gemeenschappelijke toezichtonderzoeken.

237 *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).

In 2016 vonden, naast de frequente informele contacten op de werkvloer, zeven gemeenschappelijke vergaderingen plaats.

X.4. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Het budget 2016 van het Vast Comité I werd vastgelegd op 3,768 miljoen euro[238], wat een vermindering inhield van 2,48% ten aanzien van het budget 2015. De financieringsbronnen van dit budget werden door de Kamer van Volksvertegenwoordigers[239] als volgt toegewezen:



Tegelijkertijd met de betrachting om een budgettaire reserve in te bouwen om zijn wettelijke opdrachten – die zowel in aantal als in volume toenamen – te financieren, engageerde het Vast Comité I zich om zijn werkingsbudget in te perken, en dit niettegenstaande een sterk wijzigende context.

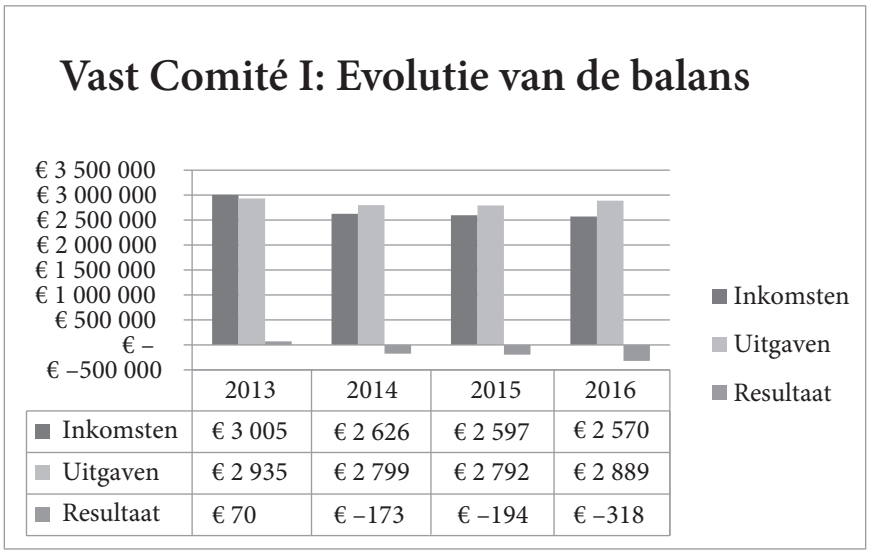
De uitvoering van het budget 2016 leverde een budgettaire bonus op van 0,880 miljoen euro, te weten het vastgestelde verschil tussen de inkomsten en de samengestelde uitgaven. Echter, de financiële realiteit leidt tot een veel minder gunstige vaststelling. Artikel 57, eerste alinea, W.Toezicht vermeldt dat de kredieten die noodzakelijk zijn voor de werking dienen te worden uitgetrokken op de begroting

238 Wet van 18 december 2015 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2016, *BS* 30 december 2015.

239 *Parl. St.* 2015-2016 Kamer, 54K1497/001, 20-22.

van de dotaties. Doch, zoals aangegeven door de bovenstaande tabel, werd het budget 2016 gebaseerd op basis van verschillende financieringsbronnen.

De enige nieuwe bijdrage in termen van eigen beheer bestaat in de dotatie ingeschreven in de algemene uitgavenbegroting van de Staat, wat zich op het niveau van de bedrijfsresultaten vertaalt in een verlies van 0,319 miljoen euro (wat een stijging inhoudt van 63,53% tegenover de budgettaire oefening 2015 (–0,195 miljoen euro)). Het betreft een tendens die reeds enkele jaren wordt vastgesteld en waarvan kan worden beaamd dat deze bij een ongewijzigd beleid tot ernstige consequenties zal leiden.



	2013	2014	2015	2016
Inkomsten	€ 3 005	€ 2 626	€ 2 597	€ 2 570
Uitgaven	€ 2 935	€ 2 799	€ 2 792	€ 2 889
Resultaat	€ 70	€ –173	€ –194	€ –318

De beslissing van de Ministerraad van 15 oktober 2014 om het dotatiebudget jaarlijks lineair met 2% te verminderen, gekoppeld aan een vermeerdering van de reële uitgaven van het Comité, zal deze tendens in de eerstvolgende jaren zeker versterken. Daarenboven wordt het Comité steeds geconfronteerd met nieuwe opdrachten (controle op de FTF-gegevensbank, controle van nieuwe bijzondere inlichtingenmethoden…) zonder dat daar een budgetverhoging tegenover staat.[240]

Aangezien de door de boni van vorige boekjaren opgebouwde reserves uitgeput geraken, is het risico reëel dat het Vast Comité I geconfronteerd wordt met liquiditeitsproblemen, wat zich onvermijdelijk zal laten vertalen naar functioneringsproblemen.

[240] De Kamercommissie Justitie werd daar expliciet van in kennis gesteld naar aanleiding van de bespreking van de wijziging aan de Wet op de inlichtingen- en veiligheidsdiensten (W.I&V).

X.5. 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.[241] Wat betreft deze laatste categorie werden onderstaande studiedagen door een of meerdere (personeels)leden van het Vast Comité I bijgewoond.

DATUM	TITEL	ORGANISATIE	PLAATS
2015-2016	Hogere Studies Veiligheid en Defensie, een multi-sectorale opportuniteit	KHID	Brussel
27-29 januari 2016	(In)visibilities & Infrastructures	Computers, Privacy & Data Protection (CPDP)	Brussel
24 februari 2016	Quelle gouvernance des services de renseignement dans une société démocratique? Table ronde	Republiek Tunesië en Centre pour le contrôle démocratique des forces armées (DCAF)	Gammarth (Tunesië)
2 maart 2016	Counter-Terrorism, Security and Human Rights	Group of the Progressive Alliance of Socialists and Democrats in the European Parliament	Brussel
12 april 2016	Intelligence and democratic oversight from the end of the Cold War until today – key trends and developments	EOS-Committee	Oslo (Noorwegen)
18 april 2016	Comment lutter contre le terrorisme et par quels moyens?	Université de Namur	Namen
29 april 2016	Protection des données à caractère personnel en 5 questions	Université de Namur	Namen
13 mei 2016	'Big data' en de inlichtingendiensten: perspectieven en toekomstige uitdagingen	Belgian Intelligence Studies Centre (BISC)	Waver

241 Er vonden ook interne opleidingen plaats, waaronder een aantal (door de medewerkers verplicht bij te wonen) veiligheidsbriefings alsook inlichtingengerelateerde opleidingen (bijv. lezing van Prof. Damien Van Puyvelde en Prof. Stephen Coulthart inzake 'Diversifying the US intelligence community workforce' en 'Implementing structured analytical techniques') en deze van Prof. Matthew Levitt. Op regelmatige tijdstippen werden eveneens lunchcauserieën georganiseerd over diverse onderwerpen (bijv. met Alain Grignard over islam, met Frank Schueremans en Koen Strobbe over politiedatabanken…).

DATUM	TITEL	ORGANISATIE	PLAATS
31 mei 2016	Radicalisering aanpakken: Nu of nooit!	Centre for Policing and Security (CPS)	Vilvoorde
11-15 september 2016	World Summit on Counter-Terrorism – Unpuzzling Terrorism	International Institue for Counter-Terrorism	Herzliya (Israël)
29 september 2016	Rapport de la commission d'enquête sur les attentats de janvier et novembre 2015	Haut Comité Français pour la Défense Civile (HCFDC)	Parijs
6 oktober 2016	Internationale samenwerking bij terrorismebestrijding en het delen van inlichtingen	Koninklijk Hoger Instituut voor Defensie (KHID)	Brussel
10 oktober 2016	Les obligations de sécurité informatique des entreprises	Université de Namur	Namen
11-12 oktober 2016	International Intelligence Oversight Forum 2016	Special rapporteur on the right to privacy (United Nations)	Boekarest (Roemenië)
17 oktober 2016	De impact van de nieuwe technologieën op onze privacy en de gegevensbescherming: wat staat erop het spel?	Senaat	Brussel
25 oktober 2016	La lutte contre le crime financier organisé: l'urgence d'une synergie des forces	Organisation internationale européenne de la lutte contre le crime financier	Brussel
28-29 oktober 2016	Witness to change. Intelligence analysis in a changing environment	Netherlands Intelligence Studies Association (NISA)	Den Haag
7-8 november 2016	Table ronde – L'accès à l'information: défis et opportunités pour la communauté du renseignement	Centre pour le contrôle démocratique des forces armées (DCAF)	Gammarth (Tunesië)
28-29 november 2016	Surveillance, Oversight, and Human Rights in Counter Terrorism	Criminal Justice Centre, The Queen Mary Reflection Group on Terrorism and Human Rights	Parijs
9 december 2016	Innovation and Information Technologies for the European security and intelligence community	Eurosint Forum	Parijs

HOOFDSTUK XI
AANBEVELINGEN

Op basis van de in 2016 afgesloten toezichtonderzoeken formuleert het Vast Comité I onderstaande aanbevelingen. Zij hebben in het bijzonder betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen (XI.1), op de coördinatie en de efficiëntie van de inlichtingendiensten, het OCAD en de ondersteunende diensten (XI.2) en – ten slotte – op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I (XI.3).

XI.1. AANBEVELINGEN IN VERBAND MET DE BESCHERMING VAN DE RECHTEN DIE DE GRONDWET EN DE WET AAN PERSONEN WAARBORGEN

XI.1.1. INVULLEN WETTELIJKE LACUNE IN VERBAND MET DATARETENTIE[242]

Bij de uitwerking van de regeling inzake vordering van operatoren (zie III.1.3), werd geen rekening gehouden met de nieuwe bevoegdheid van de VSSE en de ADIV om de activiteiten van buitenlandse diensten op ons grondgebied op te volgen. Het Vast Comité I beveelt aan dat de wetgever een maximale termijn voor kennisname van metadata zou bepalen.

XI.1.2. GEBRUIK VAN ONRECHTMATIG VERKREGEN INLICHTINGEN[243]

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

242 Deze aanbeveling vloeit voort uit het verslag over de toepassing van de specifieke en uitzonderlijke methoden door de inlichtingen- en veiligheidsdiensten en de controle hierop door het Vast Comité I (2016).

243 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*".

Comité er in het verleden[244] 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.[245]

XI.1.3. INFORMATIE-UITWISSELING EN SAMENWERKING MET BUITENLANDSE DIENSTEN[246]

Wat de samenwerking betreft met buitenlandse diensten, had het Comité reeds meermaals aangedrongen op een richtlijn die diende te worden uitgevaardigd door de Nationale Veiligheidsraad.[247] Op 26 september 2016 werd door de ministers van Justitie en Landsverdediging in een nota aan de Nationale 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/persoonsgegevens aan buitenlandse diensten slechts zeer summier behandeld. Het Comité houdt wat dit betreft dan ook vast aan zijn eerdere aanbevelingen en acht een initiatief prioritair. Hierbij moet alleszins aandacht zijn voor het beginsel dat de inlichtingendiensten bij de informatie-uitwisseling zorgvuldig tewerk moeten gaan.

XI.1.4. TECHNISCHE BIJSTAND AAN HET GERECHT[248]

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.[249] Hierover dienen de inlichtingendiensten permanent te waken.

---

244 VAST COMITÉ I, *Activiteitenverslag 2014*, 8-35.

245 Cf. Richtlijn van 26 september 2016 aangaande internationale samenwerking met buitenlandse inlichtingendiensten met onder meer aandacht voor het aspect 'respect voor de mensenrechten'.

246 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*'' en 'Hoofdstuk II.5. De bescherming van het wetenschappelijk en economisch potentieel en de Snowden-onthullingen'.

247 VAST COMITÉ I, *Activiteitenverslag 2014*, 112-113.

248 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*''.

249 VAST COMITÉ I, *Activiteitenverslag 2004*, 138 en *Activiteitenverslag 2006*, 59. De BIM-wetgever was het dan ook eens met de visie van het Comité ter zake: waar in een aanvankelijk voorstel de mogelijkheid voor de VSSE en de ADIV was ingebouwd om gewone en specifieke methoden aan te wenden in een strafonderzoek, werd dit niet weerhouden in de uiteindelijke regeling.

XI.1.5. NALEVING VAN ARTIKEL 36*BIS* VAN DE PRIVACYWET[250]

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*'.

XI.2. AANBEVELINGEN IN VERBAND MET DE COÖRDINATIE EN DE EFFICIËNTIE VAN DE INLICHTINGENDIENSTEN, HET OCAD EN DE ONDERSTEUNENDE DIENSTEN

XI.2.1. AANBEVELINGEN SPECIFIEK GERICHT OP DE STRIJD TEGEN TERRORISME EN RADICALISME

XI.2.1.1. De samenwerking binnen de local task forces (LTF)[251]

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. Op die manier is er wederzijds begrip mogelijk over wat een LTF al dan niet kan opleveren. Wat specifiek de VSSE betreft, blijkt dat het voor de deelnemers niet steeds duidelijk was wat ze in de vergaderingen kunnen zeggen (geclassificeerde informatie). Het Comité beveelt aan dat er intern binnen de diensten hierover duidelijkheid zou worden gegeven en dat vertegenwoordigers uit de provinciale diensten die aan de vergaderingen deelnemen, vanuit het centrale bestuur daarbij actief zouden worden ondersteund en gestuurd.

Het Vast Comité I beval ook aan dat de inlichtingendiensten voor elke informatie of inlichting die ter tafel van de LTF kan komen, zouden onderzoeken welke het correcte/gepaste classificatieniveau is.[252]

---

250 Protocolakkoord tot regeling van de samenwerking tussen de Veiligheid van de Staat (VSSE) en het Directoraat-generaal Uitvoering van Straffen en Maatregelen (DGUSM).

251 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*''Ftf EN Bataclan.

252 Een (begin) van oplossing werd gevonden in de nieuwe omzendbrief FTF. Deze bepaalt dat op het niveau van de Lokale Politie de functie van '*information officer* (InfOffr)' wordt ingevoerd. Hij vertegenwoordigt, als vervanger van de korpschef, de politiezone in de LTF. Hij stuurt transversaal in zijn organisatie de opsporings- en opvolgingsinspanning inzake de *foreign fighters* aan en waakt over de kwaliteit van de informatieflux in de zone. De *information officer*

XI.2.1.2. De samenwerking en synergiën tussen beide inlichtingendiensten[253]

De samenwerking tussen beide Belgische inlichtingendiensten in het kader van de Syriëproblematiek was 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).

XI.2.1.3. HUMINT in geradicaliseerde en terroristische milieus[254]

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.

XI.2.1.4. Personeel met taal- en terreinkennis[255]

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).

XI.2.1.5. Strategische analyses in de strijd tegen terrorisme[256]

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.

---

is het aanspreekpunt voor de inlichtingendiensten, het OCAD en de Federale Politie voor het uitwisselen van geclassificeerde informatie. Hij of zij beschikt, net als de korpschef, over een veiligheidsmachtiging.

253 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*'' en 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs'.

254 Zie 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs'.

255 Zie 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs'. Het Comité formuleerde eerder een aanbeveling in dezelfde zin: VAST COMITÉ I, *Activiteitenverslag 2007*, 76 ('VIII.2.4. De aanwerving van personeel met kennis van specifieke talen').

256 Zie 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs'.

XI.2.2. AANBEVELINGEN MET EEN ALGEMENE DRAAGWIJDTE

XI.2.2.1. Betere informatie-uitwisseling via geïnterconnecteerde databanken[257]

De uitwisseling van informatie is van groot belang. Zonder twijfel bestaat er op basis-collecteniveau 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 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.

XI.2.2.2. Voorspellende inlichtingen[258]

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.

XI.2.2.3. Gebruik van gestandaardiseerde analysetechnieken[259]

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 een 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.[260] Het beveelt dan ook aan dat de diensten een plan zouden ontwikkelen waarin duidelijk en transparant wordt bepaald hoe zij tegenover

---

257 Zie 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs'.

258 Zie 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs').

259 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*'' en 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs'.

260 De VSSE is zich bewust van het belang van dergelijke analysetechnieken: het ligt in hun doelstelling deze op een structurele wijze in de analysewerkzaamheden te integreren.

deze problematiek staan, welk beleid zij ter zake voeren en hoe ze de (analytische) risico's onder controle houden.

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.

XI.2.2.4. Planmatige aanpak van fenomenen[261]

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.

XI.2.2.5. Bevraging klanten[262]

Het Vast Comité I herhaalt haar aanbeveling[263] dat beide diensten hun 'klanten' expliciet zouden bevragen over welke inlichtingen deze precies willen 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.

---

261 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*'' en 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs'.

262 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*''.

263 Onder meer in: VAST COMITÉ I, *Activiteitenverslag 2011*, 104-105 ('IX.2.2.1. Aanbevelingen inzake organisatorische voorwaarden noodzakelijk voor een goede inzet van de middelen').

XI.2.2.6. Vorm en inhoud van analyseproducten[264]

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.

XI.2.2.7. Databeheer bij de ADIV[265]

Het Vast Comité I beveelt – niet voor de eerste maal[266] – 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.

XI.2.2.8. Gekwalificeerde vertalers voor SIGINT[267]

Het Comité stelde opnieuw de noodzaak vast aan gekwalificeerde vertalers voor de SIGINT-afdeling van de ADIV.

XI.2.2.9. Standaardisatie van procedures[268]

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 natio-

264 Zie 'Hoofdstuk II.3. De informatiepositie van de twee inlichtingendiensten voorafgaand aan de aanslagen in Parijs'.

265 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*''.

266 Hierover: VAST COMITÉ I, *Activiteitenverslag 2015*, 6 ('I.2.3. Informatiehuishouding bij de ADIV').

267 In 'Hoofdstuk IV. Het toezicht op de interceptie van communicatie uitgezonden in het buitenland'.

268 Zie 'Hoofdstuk II.2. De informatiepositie van de VSSE en de mislukte aanslag in de Thalys'.

nale en internationale lijsten. De lijsten met terroristen of geradicaliseerde personen zouden moeten worden gestandaardiseerd. Het werk dat de VSSE in dit kader heeft aangevat met haar partners moet een vervolg krijgen.

XI.2.2.10. Onderzoek naar informatiestromen en ICT-middelen[269]

Het Vast Comité I beveelt aan dat de VSSE een onderzoek instelt naar haar werkprocessen, de informatiestromen en de ICT-middelen die het geheel ondersteunen.

XI.2.3. AANBEVELINGEN IN VERBAND MET BIJZONDERE INLICHTINGENMETHODEN

XI.2.3.1. Correcte verwijzing in BIM-beslissingen[270]

Het Comité beveelt aan dat de VSSE en de ADIV in hun BIM-beslissingen desgevallend expliciet zouden verwijzen naar de nieuwe bevoegdheid om de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied op te volgen (zie III.1.1).

XI.2.3.2. Inzet van BIM-methoden in het buitenland[271]

Om in het buitenland uitgezonden communicaties te onderscheppen, bijvoorbeeld om redenen van veiligheid en bescherming van onze troepen en van deze van onze geallieerde partners tijdens de opdrachten in het buitenland, beschikt de ADIV over een specifiek wettelijk mandaat (art. 259*bis* § 5 Sw. *juncto* art. 11 § 2, 3° W.I&V). In tegenstelling tot SIGINT dat in het buitenland kan worden ingezet, zijn de BIM-methoden beperkt tot het binnenland. Het Comité herhaalde[272] zijn aanbeveling dat de wetgever een debat zou voeren over de noodzaak om bepaalde BIM-methoden mogelijk te maken in het buitenland. Met de wetswijziging van 30 maart 2017 werd hieraan tegemoet gekomen.

XI.2.3.3. Beperkingen bij inzet van inlichtingenmethoden[273]

Het Comité beveelt aan dat de overheden een onderzoek zouden voeren naar de efficiëntie van de actiemiddelen waarover de inlichtingen- en veiligheidsdiensten

---

269 Zie 'Hoofdstuk II.2. De informatiepositie van de VSSE en de mislukte aanslag in de Thalys'.

270 Deze aanbeveling vloeit voort uit het verslag over de toepassing van de specifieke en uitzonderlijke methoden door de inlichtingen- en veiligheidsdiensten en de controle hierop door het Vast Comité I (2016).

271 Zie 'Hoofdstuk II.1. De problematiek van de '*foreign terrorist fighters*''.

272 VAST COMITÉ I, *Activiteitenverslag 2013*, 114 en *Activiteitenverslag 2014*, 118.

273 Zie 'Hoofdstuk II.2. De informatiepositie van de VSSE en de mislukte aanslag in de Thalys'.

op het terrein beschikken en naar de huidige beperkingen (bijvoorbeeld anonieme vooraf betaalde GSM-kaarten).[274]

XI.2.4. AANBEVELINGEN IN HET KADER VAN DE BESCHERMING VAN HET WETENSCHAPPELIJK EN ECONOMISCH POTENTIEEL[275]

XI.2.4.1. 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 Belgisch WEP en tevens de kritieke infrastructuren in kaart te brengen.

XI.2.4.2. Een informatieplatform inzake de strategische bescherming van het WEP

Het Vast Comité I beveelt aan dat er, bijvoorbeeld onder de leiding van de Nationale Veiligheidsraad, een informatieplatform inzake de strategische bescherming van het wetenschappelijk en economisch potentieel wordt in het leven 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 zeer veel informatie beschikken die niet altijd voldoende benut wordt.

Dit platform kan dienstdoen 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 – en volgens de presentatie van dit centrum zal – 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.

---

274 Hieraan werd tegemoetgekomen wat betreft pre-paid kaart (zie 'III.1.4. De identificatie van een pre-paid kaarthouder').

275 Deze aanbeveling vloeit voort uit 'Hoofdstuk II.5. De bescherming van het wetenschappelijk en economisch potentieel en de Snowden-onthullingen'.

XI.2.4.3. 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.

XI.2.4.4. Goedkeuring WEP-lijst ADIV

De goedkeuring door de Nationale Veiligheidsraad van een lijst van actoren – zowel natuurlijke als juridische entiteiten – die in de economische en industriële sectoren actief zijn en die gerelateerd zijn aan Defensie, zoals bepaald in artikel 11 van de organieke Wet op de inlichtingen en veiligheidsdiensten, dringt zich op.

XI.2.5. AANBEVELINGEN INZAKE DE SAMENWERKING MET DE PENITENTIAIRE INRICHTINGEN[276]

XI.2.5.1. Naar een nieuw protocol

Het Vast Comité I is van oordeel dat het samenwerkingsprotocol tussen de VSSE en het DG EPI 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.

XI.2.5.2. Aanbevelingen voor een betere informatie-uitwisseling en -verwerking

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.

---

276 Aanbevelingen uit 'Hoofdstuk II. 6. De VSSE en het samenwerkingsprotocol met de Strafinrichtingen'.

XI.2.6. AANBEVELINGEN IN HET KADER VAN DE WERKING VAN HET OCAD[277]

De Vaste Comités I en P bevelen het OCAD aan om
- elke vraag om evaluatie van een dreiging die niet tot zijn wettelijke bevoegdheid hoort van de hand te wijzen;
- 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 regulariseren;
- 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.

XI.3. AANBEVELING IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

XI.3.1. HET AFLUISTERPLAN[278]

De overzending van de interceptielijst loopt al te vaak vertraging op.[279] 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.

---

277 Aanbeveling uit 'Hoofdstuk II.13. Specifieke disfuncties binnen het OCAD'.

278 In 'Hoofdstuk IV. Het toezicht op de interceptie van communicatie uitgezonden in het buitenland'.

279 VAST COMITÉ I, *Activiteitenverslag 2010*, 105 ('IX3.2. Tijdig overzenden van geviseerde veiligheidsintercepties') en *Activiteitenverslag 2015*, 71. Het Comité werd pas bij het afsluiten van de redactie van voorliggend rapport in het bezit gesteld van het Afluisterplan 2017.

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 2016 TOT 31 DECEMBER 2016)

Wet 5 februari 2016 tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie, *BS* 19 februari 2016

Wet 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, *BS* 24 februari 2016

Wet 21 april 2016 houdende diverse bepalingen Binnenlandse Zaken – geïntegreerde politie, *BS* 29 april 2016

Wet 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme, *BS* 9 mei 2016

Wet 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *BS* 18 juli 2016

Wet 12 juli 2016 houdende eerste aanpassing van de algemene uitgavenbegroting voor het begrotingsjaar 2016, *BS* 14 september 2016

Wet 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, *BS* 7 december 2016

Wet 7 december 2016 tot invoeging van een artikel 106/1 in de wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 19 december 2016

Wet 21 november 2016 tot wijziging van diverse bepalingen betreffende het statuut van de militairen, *BS* 23 december 2016

Wet 25 december 2016 houdend de algemene uitgavenbegroting voor het begrotingsjaar 2017, *BS* 29 december 2016

Uittreksel uit arrest nr. 108/2016 van 14 juli 2016, Rolnummer: 6045, Inzake: het beroep tot vernietiging van de wet van 18 maart 2014 betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van strafvordering, ingesteld door vzw "Liga voor Mensenrechten" en de vzw "Ligue des Droits de l'Homme", *BS* 13 oktober 2016

K.B. 7 maart 2016 tot wijziging van het koninklijk besluit van 26 januari 2006 tot oprichting van een Federaal Comité voor de Beveiliging van het Spoorwegvervoer en houdende diverse maatregelen voor de beveiliging van het intermodaal vervoer, *BS* 1 april 2016

K.B. 19 februari 2016 tot uitvoering van de artikelen 13, 24 en 25 van de wet van 1 juli 2011 betreffende de beveiliging en bescherming van de kritieke infrastructuren, voor de sector Vervoer, deelsector spoorvervoer, *BS* 7 april 2016

K.B. 1 mei 2016 tot vaststelling van het nationaal noodplan betreffende de aanpak van een terroristische gijzelneming of terroristische aanslag, *BS* 18 mei 2016

K.B. 23 mei 2016 tot toekenning van een overplaatsingsvergoeding aan de beschermingsassistenten van de Veiligheid van de Staat die worden overgeplaatst naar de federale politie, *BS* 27 mei 2016

K.B. 23 mei 2016 tot regeling van de overplaatsing van de beschermingsassistenten van de Veiligheid van de Staat naar de federale politie, *BS* 30 mei 2016

K.B. 4 mei 2016 houdende gedeeltelijke verdeling, betreffende schadevergoedingen en gerechtskosten van het provisioneel krediet ingeschreven in het programma 03-41-1 van de algemene uitgavenbegroting voor het begrotingsjaar 2016 en bestemd tot het dekken van niet structurele uitgaven wat betreft de veiligheid, *BS* 13 juni 2016

K.B. 6 juni 2016 tot wijziging van het koninklijk besluit van 4 juli 2014 tot vaststelling van het statuut van bepaalde burgerlijke ambtenaren van het stafdepartement inlichtingen en veiligheid van de krijgsmacht, *BS* 5 juli 2016

K.B. 27 juni 2016 tot wijziging van het koninklijk besluit van 23 januari 2007 betreffende het personeel van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 25 juli 2016

K.B. 21 juli 2016 tot aanvulling van de lijst van personen en entiteiten bedoeld in artikelen 3 en 5 van het koninklijk besluit van 28 december 2006 inzake specifieke beperkende maatregelen tegen bepaalde personen en entiteiten met het oog op de strijd tegen de financiering van het terrorisme, *BS* 28 juli 2016

K.B. 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, *BS* 3 augustus 2016

K.B. 10 juli 2016 tot wijziging van het koninklijk besluit van 5 december 2006 betreffende het algemeen bestuur en de ondersteuningscel van de Veiligheid van de Staat, *BS* 12 augustus 2016

K.B. 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Foreign Terrorist Fighters en tot uitvoering van sommige bepalingen van de afdeling I*bis* "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt, *BS* 22 september 2016

K.B. 28 september 2016 betreffende de bewapening van de agenten van politie, *BS* 4 oktober 2016

K.B. 26 september 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* 13 oktober 2016

K.B. 3 november 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* 25 november 2016

K.B. 27 november 2016 betreffende de identificatie van de eindgebruiker van mobiele openbare elektronische communicatiediensten die worden geleverd op basis van een voorafbetaalde kaart, *BS* 7 december 2016

M.B. 28 september 2016 betreffende de opleiding tot bewapening van de agenten van politie, *BS* 4 oktober 2016

M.B. 14 november 2016 houdende aanwijzing van een selectiecomité belast met de evaluatie van de kandidaturen voor de post van directeur van de analyse van de Veiligheid van de Staat, *BS* 21 november 2016

Oproep tot kandidaten voor de bestuurlijke Commissie door de inlichtingen- en veiligheidsdiensten belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, *BS* 19 januari 2016

Comité permanent de contrôle des services de renseignement et de sécurité, recrutement pour l'entrée en service immédiate et constitution d'une réserve de recrutement d'une secrétaire francophone statutaire (m/f) (niv. B), *BS* 17 februari 2016

Vergelijkende selectie van Nederlandstalige inspecteurs voor de buitendienst (m/v/x) (niveau B) voor de Veiligheid van de Staat (FOD Justitie) (ANG16050), *BS* 1 maart 2016

Vergelijkende selectie van Franstalige inspecteurs voor de buitendienst (m/v/x) (niveau B) voor de Veiligheid van de Staat (FOD Justitie) (AFG16050), *BS* 1 maart 2016

Vergelijkende selectie van Nederlandstalige vertalers (m/v/x) (niveau A) voor de Veiligheid van de Staat (ANG16056), *BS* 18 maart 2016

Vergelijkende selectie van Franstalige analisten economische inlichtingen (m/v/x) (niveau A1) voor Landsverdediging (AFG16021), *BS* 1 april 2016

Vergelijkende selectie van Nederlandstalige analisten economische inlichtingen (m/v/x) (niveau A1) voor Landsverdediging (ANG16046), *BS* 1 april 2016

Aanwerving voor onmiddellijke indiensttreding en samenstelling van een wervingsreserve van een statutaire jurist(e) (m/v) (niv. A) voor het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *BS* 13 april 2016

Vergelijkende selectie van Nederlandstalige netwerkbeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat (ANG16022), *BS* 4 mei 2016

Vergelijkende selectie van Nederlandstalige Cyber Security experten – afgesloten, *BS* 17 mei 2016

Vergelijkende selectie van Franstalige database administrator (m/v/x) voor de Veiligheid van de Staat (AFG15193), *BS* 23 mei 2016

Vergelijkende selectie van Nederlandstalige analisten (m/v/x) voor het Coördinatieorgaan voor de dreigingsanalyse (niveau A3) voor de FOD Binnenlandse Zaken (ANG16124), *BS* 27 mei 2016

Vergelijkende selectie van Franstalige analisten (m/v/x) voor het Coördinatieorgaan voor de dreigingsanalyse (niveau A3) voor de FOD Binnenlandse Zaken (AFG16096), *BS* 27 mei 2016

Vergelijkende selectie van Franstalige vertalers (m/v/x) (niveau A) voor het Coördinatieorgaan voor de dreigingsanalyse – FOD Binnenlandse Zaken (AFG16131), *BS* 15 juli 2016

Vergelijkende selectie van Franstalige IT-Helpdeskmedewerkers (m/v/x) (niveau C) voor de Veiligheid van de Staat (AFG16138), *BS* 16 augustus 2016

Vergelijkende selectie van Nederlandstalige IT-helpdeskmedewerkers (m/v/x) (niveau C) voor de Veiligheid van de Staat (ANG16169), *BS* 16 augustus 2016

Vergelijkende selectie van Franstalige adviseur-generaal Internationale Relaties A4 (m/v/x) (niveau A4) voor de Veiligheid van de Staat – FOD Justitie (AFG16156), *BS* 23 september 2016

Vergelijkende selectie van Nederlandstalige adviseur-generaal Internationale Relaties A4 (m/v/x) (niveau A4) voor de Veiligheid van de Staat – FOD Justitie (ANG16187), *BS* 23 september 2016

Huishoudelijk reglement van de bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (BIM-Commissie), *BS* 27 september 2016

Omzendbrief tot wijziging van de omzendbrief GPI 62 van 14 februari 2008 betreffende de bewapening van de geïntegreerde politie, gestructureerd op twee niveaus, *BS* 4 oktober 2016

Vergelijkende selectie van Nederlandstalige analisten (m/v/x) (niveau A), voor het Coördinatieorgaan voor de dreigingsanalyse (OCAD) (ANG16124), afgesloten op 28 september 2016, *BS* 10 oktober 2016

Vergelijkende selectie van Nederlandstalige woordvoerders (m/v/x) (niveau A) voor de Veiligheid van de Staat, *BS* 4 november 2016

Vacante betrekking van directeur van de analyse van de Veiligheid van de Staat – oproep tot kandidaten, *BS* 10 november 2016

Resultaat van de vergelijkende selectie van Nederlandstalige adviseurs-generaal Internationale Relaties (m/v/x) (niveau A4) voor de Veiligheid van de Staat, *BS* 7 december 2016

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 2016 TOT 31 DECEMBER 2016)

Senaat

Verslag over de radicalisering in België, *Parl. St.* Senaat 2015-16, nr. 6-205/1

Bij brief van 22 november 2016 heeft de voorzitter van het Vast Comité van Toezicht op de inlichtingen en veiligheidsdiensten, aan de Senaat overgezonden, het jaarverslag voor 2015, *Hand.* Senaat 2016-17, 16 december 2016, n° 6-24, p. 40

Kamer van Volksvertegenwoordigers

Beleidsverklaring van de staatssecretaris voor Bestrijding van de sociale fraude, Privacy en Noordzee, *Parl. St.* Kamer 2015-16, nr. 54K0020/063

Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, aangaande het toezicht op de activiteiten van de buitenlandse inlichtingendiensten in België, *Parl. St.* Kamer 2015-16, nrs. 54K0553/004, 54K0553/005, 54K0553/006 en 54K0553/007.

Wetsontwerp houdende wijzigingen van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie, *Parl. St.* Kamer 2015-16, nr. 54K1418/009.

Wetsontwerpen en voorstellen ingediend, *Hand.* Kamer 2015-16, 14 januari 2016, CRIV54PLEN094, 34.

Verzending van een voorstel naar de commissie voor advies, *Hand.* Kamer 2015-16, 14 januari 2016, CRIV54PLEN094, 41.

Inoverwegingneming van voorstellen, *Hand.* Kamer 2015-16, 14 januari 2016, CRIV54PLEN094, 41.

Wetsontwerp houdende wijzigingen van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie (1418/1-17) – Wetsvoorstel tot wijziging van het Wetboek van Strafvordering wat de uitbreiding van het mini-onderzoek tot de huiszoeking betreft (108/1-4) – Wetsvoorstel tot wijziging van de wet van 17 april 1878 houdende de Voorafgaande titel van het Wetboek van strafvordering wat betreft betere verjaringstermijnen bij seksueel misbruik van minderjarige personen in geval van eenheid van opzet (758/1-2) – Wetsvoorstel tot wijziging van de artikelen 399, 400 en 405*bis* van het Strafwetboek, wat de vrijwillige slagen en verwondingen betreft (969/1-2) – Wetsvoorstel tot wijziging van artikel 35, § 2, van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme (1139/1-2) – Wetsvoorstel tot wijziging van de wet van 29 juni 1964 betreffende de opschorting, het uitstel en de probatie wat betreft de afwezigheid van voorafgaande veroordelingen (1368/1-2) – Wetsvoorstel tot wijziging van het Strafwetboek wat betreft de tijdelijke en de blijvende ongeschiktheid (1369/1-2) – Wetsvoorstel tot wijziging van het Gerechtelijk Wetboek met het oog op het verzekeren van de goede en continue werking van het federaal parket (1385/1-2), *Hand.* Kamer 2015-16, 28 januari 2016, CRIV54PLEN096, 51.

Wetsvoorstel tot verbetering van de samenwerking tussen de Cel voor Financiële Informatieverwerking en de instellingen ter bestrijding van het terrorisme, *Parl. St.* Kamer 2015-16, nr. 54K1544/003

Wetsontwerp betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *Parl. St.* Kamer 2015-16, nrs. 54-1567/12, 54-1567/13 en 54-1567/14

Verzending van het wetsvoorstel met het oog op een ruimere aanwending van de gegevens verkregen in het kader van de automatische uitwisseling van inlichtingen naar de tijdelijke commissie 'terrorismebestrijding' (n° 1589/1), *Hand.* Kamer 2015-16, 4 februari 2016, CRIV54PLEN097, 53

Voorstel tot wijziging van het Reglement van de Kamer van Volksvertegenwoordigers wat betreft de samenstelling van de commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I, *Parl. St.* Kamer 2015-16, nr. 54K1598/001

Wetsvoorstel tot aanvulling van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, wat betreft het financieren van verenigingen die aanzetten tot haat, discriminatie, geweld of segregatie, *Parl. St.* Kamer 2015-16, nr. 54K1620/001

Voorstel tot wijziging van Hoofdstuk X en artikel 151 van het Reglement van de Kamer van Volksvertegenwoordigers, teneinde de bevoegdheid van de bijzondere commissie uit te breiden naar de verkoop van legermateriaal door Defensie, *Parl. St.* Kamer 2015-16, nr. 54K1621/001

Voorstel van resolutie voor een effectieve en democratische strijd tegen terrorisme, *Parl. St.* Kamer 2015-16, nr. 54K1624/001

Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met een onderzoek naar de Molenbeekse terreurcel die in Parijs een reeks terroristische aanslagen pleegde, *Parl. St.* Kamer 2015-16, nrs. 54K1626/001 tot 54K1626/003

Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, *Parl. St.* Kamer 2015-16, nr. 54K1629/001 en *Hand.* Kamer 2015-16, 4 februari 2016, CRIV54PLEN097, 54

Wetsontwerp houdende diverse bepalingen Binnenlandse Zaken – Geïntegreerde politie (1644/1-5) – algemene bespreking, *Hand.* Kamer 2015-16, 3 maart 2016, CRIV54PLEN100, 40

Wetsontwerp houdende diverse bepalingen – Binnenlandse Zaken – Geïntegreerde politie, *Parl. St.* Kamer 2015-16, nr. 54K1644/001

Wetsvoorstel tot oprichting van een Vast Comité van Toezicht op de veiligheid van de federale openbare infrastructuur, *Parl. St.* Kamer 2015-16, nr. 54-1660/001

Wetsvoorstel tot wijziging van de wet van 5 augustus 1992 op het politieambt met betrekking tot een sluitende informatiedoorstroming over foreign terrorist fighters, *Parl. St.* Kamer 2015-16, nr. 54-1711/001

Wetsontwerp inzake aanvullende maatregelen ter bestrijding van terrorisme, *Parl. St.* Kamer 2015-16, nrs. 54-1727/1 tot 54-1727/8

Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de informatie waarover de onderzoekers beschikten vóór de aanslagen in Parijs en naar de manier waarop met die informatie werd omgegaan, *Parl. St.* Kamer 2015-16, nr. 54-1742/001

Gedachtewisseling met de heer Miguel De Bruycker, directeur van het Centrum voor Cybersecurity België, *Parl. St.* Kamer 2015-16, nr. 54-1744/001

Inoverwegingneming van voorstellen tot oprichting van een 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, nr. 1752/1, *Hand.* Kamer 2015-16, 12 april 2016, CRIV54PLEN104, 2

Voorstel tot oprichting van een 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, *Parl. St.* Kamer 2015-16, nr. 54K1752/005

Voorstel van resolutie tot aanstelling van een regeringscommissaris voor de coördinatie van de opvolging van de foreign terrorist fighters en het wegwerken van dysfuncties in het veiligheidsbeleid, *Parl. St.* Kamer 2015-16, nr. 54-1785/001

Verzending van wetsvoorstellen naar een andere commissie van het wetsvoorstel (de heren Marco Van Hees en Raoul Hedebouw) tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, nr. 1629/1, *Hand.* Kamer 2015-16, 28 april 2016, CRIV54PLEN108, 112

Wetsontwerp betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie (1567/1-14), *Hand.* Kamer 2015-16, 4 mei 2016, CRIV54PLEN109, 47

Wetsontwerp houdende de aanpassing van de Middelenbegroting voor het begrotingsjaar 2016, *Parl. St.* Kamer 2015-16, nr. 54K1804/003

Wetsontwerp houdende eerste aanpassing van de Algemene uitgavenbegroting van het begrotingsjaar 2016, *Parl. St.* Kamer 2015-16, nrs. 54K1805/003 en 54K1805/005

Wetsvoorstel tot wijziging van de wet van en bijzondere veiligheid wat betreft de uitoefeningsvoorwaarden voor functies binnen de private en bijzondere veiligheid, *Parl. St.* Kamer 2015-16, nr. 54K1829/001

Voorstel van resolutie betreffende de bestrijding van islamitische satellietzenders, radiostations en websteks die op het Belgische en Europese grondgebied antiwesterse haat- en geweldspropaganda verspreiden, *Parl. St.* Kamer 2015-16, nr. 54K1874/001

Wetsvoorstel tot wijziging van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, wat betreft de werking van het Controleorgaan op de politionele informatie, *Parl. St.* Kamer 2015-16, nr. 54K1943/002

Wetsontwerp tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, *Parl. St.* Kamer 2015-16, nrs. 54K1964/001 tot 54K1964/003 en *Hand.* Kamer 2015-16, 20 juli 2016, CRIV54PLEN123, 42

Gedachtewisseling over het Nationaal Veiligheidsplan en de Kadernota Integrale Veiligheid 2016-2019, *Parl. St.* Kamer 2015-16, nr. 54K2026/001

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 2015-16, nrs. 54K2043/001 en 54K2043/002

Wetsontwerp houdende diverse bepalingen inzake ambtenarenzaken, *Parl. St.* Kamer 2016-17, nr. 54K2064/003

Wetsontwerp betreffende de verwerking van passagiersgegevens, *Parl. St.* Kamer 2015-16, nrs. 54K2069/001 tot 54K2069/003 en 54K2069/005

Voorstel van resolutie over de oprichting van een federaal inlichtingenagentschap, *Parl. St.* Kamer 2016-17, nr. 54K2086/001

Urgentieverzoeken vanwege de regering bij de indiening van het wetsontwerp betreffende de verwerking van passagiersgegevens, nr. 2069/1, *Hand.* Kamer 2016-17, 13 oktober 2016, CRIV54PLEN130, 74

Bespreking van de verklaring van de regering, *Hand.* Kamer 2016-17, 17 oktober 2016, CRIV54PLEN132, 4 en *Hand.* Kamer 2016-17, 17 oktober 2016, CRIV54PLEN134, 1

Wetsontwerp betreffende de verwerking van passagiersgegevens (2069/1-8), *Hand.* Kamer 2016-17, 23 november 2016, CRIV54PLEN140, 105

Wetsvoorstel tot wijziging van het Strafwetboek wat betreft de bestraffing van terrorisme (1579/1-12), *Hand.* Kamer 2016-17, 1 december 2016, CRIV54PLEN142, 44

Wetsontwerp houdende de Middelenbegroting voor het begrotingsjaar 2017, *Parl. St.* Kamer 2016-17, nrs. 54K2108/001, 54K2108/003 en 54K2108/005

Ontwerp van algemene uitgavenbegroting voor het begrotingsjaar 2017, *Parl. St.* Kamer 2016-17, nrs. 54K2109/001 en 54K2109/003

Verantwoording van de algemene uitgavenbegroting voor het begrotingsjaar 2017, *Parl. St.* Kamer 2016-17, nr. 54K2110/002

Algemene beleidsnota Justitie, *Parl. St.* Kamer 2016-17, nrs. 54K2111/006, 54K2111/007, 54K2111/017, 54K2111/020 en 54K2111/021

Voorstel van resolutie betreffende de terugtrekking van Landsverdediging uit de operatie Vigilant Guardian en de vervanging van die mankracht door een specifiek politiekorps, *Parl. St.* Kamer 2016-17, nr. 54K2156/001

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, nr. 54K2179/006

Wetsontwerp tot goedkeuring van de algemene rekening van het algemeen bestuur van het jaar 2015 en van de uitvoeringsrekeningen van de begrotingen van Staatsdiensten met afzonderlijk beheer voorgaande jaren, *Parl. St.* Kamer 2016-17, nr. 54K2192/001

Wetsvoorstel tot wijziging van het Strafwetboek wat betreft de bestraffing van terrorisme (1579/1-12), *Hand.* Kamer 2016-17, 1 december 2016, CRIV54PLEN142, 44

Wetsontwerp betreffende de verwerking van passagiersgegevens (2069/1-9), *Hand.* Kamer 2016-17, 21 december 2016, CRIV54PLEN148, 1

Wetsontwerp betreffende de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet- en elektronische en telecommunicaties (1966/1-10), *Hand.* Kamer 2016-17, 21 december 2016, CRIV54PLEN150, 5

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, BIM-Commissie, Controleorgaan op de politionele informatie en Federale Deontologische Commissie – Rekeningen van het begrotingsjaar 2015 – Begrotingsaanpassingen van het begrotingsjaar 2016 – Begrotingsvoorstellen voor het begrotingsjaar 2017, *Parl. St.* Kamer 2016-17, nrs. 54K2225/001 tot 54K2225/003 en *Hand.* Kamer 2016-17, 22 december 2016, CRIV54PLEN151, 25 en 39

Rekeningen van het begrotingsjaar 2015 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten (2225/1), *Hand.* Kamer 2016-17, 22 december 2016, CRIV54PLEN151, 58

Begrotingsvoorstellen voor het begrotingsjaar 2017 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten (2225/1), *Hand.* Kamer 2016-17, 22 december 2016, CRIV54PLEN151, 59

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 2016 TOT 31 DECEMBER 2016)

Senaat

Schriftelijke vraag van J.-J. De Gucht aan de minister van Binnenlandse Zaken over de 'radicalisering – ambts- en beroepsgeheim – mogelijkheid om radicalisering te melden – privacy' (Senaat 2015-16, 13 januari 2016, Vr. nr. 6-802)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over de 'radicalisering – ambts- en beroepsgeheim – mogelijkheid om radicalisering te melden – privacy' (Senaat 2015-16, 13 januari 2016, Vr. nr. 6-803)

Schriftelijke vraag van J.-J. De Gucht aan staatssecretaris voor Bestrijding van de sociale fraude over de 'radicalisering – ambts- en beroepsgeheim – mogelijkheid om radicalisering te melden – privacy' (Senaat 2015-16, 13 januari 2016, Vr. nr. 6-804)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over de 'vluchtelingenopvang – radicalisering – steun – ronselpraktijken – voorbeeld van de stichting Al-Ighaatha – gevangenen – samenwerking met de Nederlandse overheid' (Senaat 2015-16, 4 februari 2016, Vr. nr. 6-823)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Binnenlandse Zaken over de 'salafisme – giften aan veroordeelde terroristen – opvolging en screening – bevriezen fondsen' (Senaat 2015-16, 31 maart 2016, Vr. nr. 6-901)

Schriftelijke vraag van P. Van Rompuy aan de minister van Binnenlandse Zaken over de 'uitgeweken Syriëstrijders – bevolkingsregister – schrapping – procedure – cijfers' (Senaat 2015-16, 25 april 2016, Vr. nr. 6-934)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Binnenlandse Zaken over de 'radicalisering – voorbereidingsfase van jihadisten – kleine criminaliteit – knipperlichtfunctie voor detectie en preventie' (Senaat 2015-16, 7 juli 2016, Vr. nr. 6-998)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Binnenlandse Zaken over de 'haatpredikers – cijfers – strijd – veroordeling – intrekken visa Europese lijst' (Senaat 2015-16, 7 juli 2016, Vr. nr. 6-1000)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Buitenlandse Zaken over de 'haatpredikers – cijfers – strijd – veroordeling – intrekken visa Europese lijst' (Senaat 2015-16, 7 juli 2016, Vr. nr. 6-1001)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over de 'haatpredikers – cijfers – strijd – veroordeling – intrekken visa Europese lijst' (Senaat 2015-16, 7 juli 2016, Vr. nr. 6-1002)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Binnenlandse Zaken over de 'jihadistische netwerken – beginstadia – snellere detectie – nader onderzoek – toegang tot vertrouwelijke informatie voor onderzoekers' (Senaat 2015-16, 12 juli 2016, Vr. nr. 6-1009)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over 'jihadistische netwerken – beginstadia – sneller detectie – nader onderzoek – toegang tot vertrouwelijke informatie voor onderzoekers' (Senaat 2015-16, 12 juli 2016, Vr. nr. 6-1010)

Schriftelijke vraag van B. Anciaux aan de minister van Mobiliteit over de 'beveiliging van de Koning en andere hoogwaardigheidsbeklederś – verkeersveiligheid – veiligheid van gewone weggebruikers – gevaar – reglementering' (Senaat 2015-16, 21 oktober 2016, Vr. nr. 6-741)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Binnenlandse Zaken over 'het terrorisme – crimineel verleden – rekrutering van criminelen in jihadistische netwerken – nieuwe studie – gevangenisbeleid overbevolking – detectie van radicalisering – opleiding van de personeelsleden van de gevangenissen' (Senaat 2016-17, 26 oktober 2016, Vr. nr. 6-1072)

Schriftelijke vraag van J.-P. Wahl aan de minister van Justitie over 'gevangenissen – radicalisering – bestrijding – Directoraatgeneraal Penitentiaire Inrichtingen (DG EPI) – Coördinatoren – rol – evolutie – opleiding – aantal' (Senaat 2016-17, 24 november 2016, Vr. nr. 6-1140)

Kamer van Volksvertegenwoordigers

Vraag van S. Van Hecke aan de minister van Justitie over 'het protocolakkoord tussen de nationale Bank en de Staatsveiligheid' (*Hand.* Kamer 2015-16, 6 januari 2016, CRIV-54COM301, 3, Vr. nr. 8170)

Vraag van M. Van Hees aan de minister van Binnenlandse Zaken over de 'geradicaliseerde Belgen – waakzame gemeenten' (*Vr. en Ant.* Kamer 2015-16, 11 januari 2016, QRVA 057, 188, Vr. nr. 732)

Vraag van R. Deseyn aan de minister van Ontwikkelingssamenwerking over de 'ombudsdienst – dataretentie' (*Vr. en Ant.* Kamer 2015-16, 11 januari 2016, QRVA 057, 230, Vr. nr. 296)

Vraag van A. Top aan de minister van Defensie over de 'werking van het BINII-systeem' (*Vr. en Ant.* Kamer 2015-16, 11 januari 2016, QRVA 057, 503, Vr. nr. 505)

Gedachtewisseling met de minister van Defensie en samengevoegde vragen van S. Pirlot, W. De Vriendt, P. Buysrogge, A. Top, V. Yüksel, R. Hedebouw en G. Dallemagne over 'het strategisch plan van Defensie' (*Hand.* Kamer 2015-16, 13 januari 2016, CRIV-54COM305, 1, Vr. nrs. 97, 8140, 8154, 99, 8417, 8425 en 8447)

Vraag van S. Van Hecke aan de minister van Justitie over 'de overdracht van de dienst protectie van de Veiligheid van de Staat naar de politie' (*Hand.* Kamer 2015-16, 13 januari 2016, CRIV54COM306, 7, Vr. nr. 8253)

Samengevoegde vragen van P. Vanvelthoven, É. Thiébaut, J.-M. Nollet, M. Van Hees en K. Jadin aan de minister van Binnenlandse Zaken over 'de technische incidenten in sommige Belgische kerncentrales' (*Hand.* Kamer 2015-16, 13 januari 2016, CRIV-54COM309, 15, Vr. nrs. 8113, 8131, 8141, 8142, 8143, 8158, 8220, 8221, 100 en 8151)

Vraag van A. Top aan de minister van Justitie over 'de mogelijkheid voor agenten van de Veiligheid van de Staat op anoniem te surfen op het internet' (*Hand.* Kamer 2015-16, 20 januari 2016, CRIV54COM314, 8, Vr. nr. 8460)

Vraag van K. Metsu aan de minister van Justitie over 'imam Tarik Ibn Ali' (*Hand.* Kamer 2015-16, 20 januari 2016, CRIV54COM314, 28, Vr. nr. 8602)

Vraag van P. Pivin aan de minister van Binnenlandse Zaken over 'het dreigingsniveau en de beroepsverenigingen van handelaars' (*Hand.* Kamer 2015-16, 20 januari 2016, CRIV54COM316, 29, Vr. nr. 8397)

Samengevoegde vragen van G. Dallemagne, H. Bonté en N. Ben Hamou aan de minister van Binnenlandse Zaken over 'de initiatieven ter bestrijding van terrorisme' (*Hand.* Kamer 2015-16, 21 januari 2016, CRIV54PLEN095, 7, Vr. nrs. 0937 tot 0939)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'verhoogd dreigingsniveau voor de opvangcentra' (*Vr. en Ant.* Kamer 2015-16, 25 januari 2016, QRVA 059, 147, Vr. nr. 910)

Vraag van V. Yüksel aan de minister van Justitie over de 'fraudeschandaal – de gevolgen voor het wagenpark FOD Justitie' (*Vr. en Ant.* Kamer 2015-16, 25 januari 2016, QRVA 059, 170, Vr. nr. 617)

Vraag van A. Carcaci aan de eerste minister over 'twaalf maatregelen om het terrorisme efficiënter te bestrijden' (*Hand.* Kamer 2015-16, 26 januari 2016, CRIV54COM317, 14, Vr. nr. 8720)

Vraag van R. Hedebouw aan de eerste minister over 'de transparantie en de parlementaire controle over de Nationale Veiligheidsraad en de bepaling van het terreurniveau' (*Hand.* Kamer 2015-16, 26 januari 2016, CRIV54COM317, 37, Vr. nr. 8840)

Vraag van V. Van Peel aan de minister van Middenstand over 'het beroepsgeheim versus de meldingsplicht van OCMW's' (*Hand.* Kamer 2015-16, 27 januari 2016, CRIV-54COM323, 4, Vr. nr. 8014)

Vraag van B. Pas aan de eerste minister over 'het feit dat de Belgische veiligheidsdiensten al jaren op de hoogte waren van het bestaan en de plannen van de terreurcel in Parijs' (*Hand.* Kamer 2015-16, 28 januari 2016, CRIV54PLEN096, 23, Vr. nr. 970)

Vraag van F. Schepmans aan de minister van Binnenlandse Zaken over de 'resultaten van het BELFI-project' (*Vr. en Ant.* Kamer 2015-16, 1 februari 2016, QRVA 060, 110, Vr. nr. 856)

Vraag van Ph. Pivin aan de minister van Justitie over 'de Veiligheid van de Staat en de samenwerking met de Dienst Vreemdelingenzaken' (*Hand.* Kamer 2015-16, 3 februari 2016, CRIV54COM334, 30, Vr. nr. 9089)

Vraag van E. Kir aan de minister van Binnenlandse Zaken over 'de uitspraken van de minister in de pers en het beeld dat hij daarin geeft van de moslimgemeenschap' (*Hand.* Kamer 2015-16, 3 februari 2016, CRIV54COM335, 7, Vr. nr. 8624)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over 'het effectieve toezicht op de 'foreign terrorist fighters' via taskforces in de Brusselse gemeenten' (*Hand.* Kamer 2015-16, 3 februari 2016, CRIV54COM335, 30, Vr. nr. 8640)

Samengevoegde vragen van V. Yüksel en V. Matz aan de minister van Binnenlandse Zaken over 'de oprichting van het 'European Counter Terrorism Centre' (*Hand.* Kamer 2015-16, 3 februari 2016, CRIV54COM335, 43, Vr. nrs. 8912 en 8980)

Vraag van O. Chastel aan de staatssecretaris voor Asiel en Migratie over de 'opvangcentrum in de kazerne van Elsenborn' (*Vr. en Ant.* Kamer 2015-16, 8 februari 2016, QRVA 061, 478, Vr. nr. 413)

Samengevoegde vragen van W. De Vriendt en A. Top aan de minister van Defensie, over 'defensieattaché's en wapenhandel' (*Hand.* Kamer 2015-16, 17 februari 2016, CRIV-54COM337, 18, Vr. nrs. 8771 en 8790)

Samengevoegde vragen van K. Jadin, B. Hellings en Ph. Pivin aan de minister van Buitenlandse Zaken over 'de screening van de personen die in kerncentrales werken' (*Hand.* Kamer 2015-16, 17 februari 2016, CRIV54COM340, 36, Vr. nrs. 8 994, 9000 en 9088)

Samengevoegde vragen van M. de Lamotte, J.-M. Nollet en Ph. Pivin aan de minister van Binnenlandse Zaken over 'de veiligheid in en rond de kerncentrales' (*Hand.* Kamer 2015-16, 18 februari 2016, CRIV54PLEN098, 20, Vr. nrs. 1004, 1005 en 1006)

Vraag van K. Metsu aan de minister van Justitie over de 'vervolgingen voor posten propagandafilmpjes Islamitische Staat (IS)' (*Vr. en Ant.* Kamer 2015-16, 23 februari 2016, QRVA 063, 236, Vr. nr. 687)

Vraag van D. Ducarme aan de minister van Defensie over de 'resolute support-missie' (*Vr. en Ant.* Kamer 2015-16, 23 februari 2016, QRVA 063, 430, Vr. nr. 548)

Vraag van N. Lanjri aan de staatssecretaris voor Asiel en Migratie over 'de uitvoering van het Europees spreidingsplan' (*Vr. en Ant.* Kamer 2015-16, 23 februari 2016, QRVA 063, 464, Vr. nr. 453)

Vraag van A. Top aan de minister van Defensie over 'de militairen in de straten' (*Vr. en Ant.* Kamer 2015-16, 29 februari 2016, QRVA 064, 408, Vr. nr. 560)

Vraag van B. Pas aan de staatssecretaris voor Asiel en Migratie over de 'bezoeken van jihadsympathisanten aan asielcentra' (*Hand.* Kamer 2015-16, 2 maart 2016, CRIV-54COM353, 15, Vr. nr.8690)

Gedachtewisseling en samengevoegde vragen van A. Top, G. Vanden Burre, R. Hedebouw, N. Ben Hamou, E. Kir, O. Maingain, K. Degroote, F. Schepmans, G. Dallemagne, S. Lahaye-Battheu en W. Demeyer aan de minister van Binnenlandse Zaken over 'het Kanaalplan' (*Hand.* Kamer 2015-16, 2 maart 2016, CRIV54COM358, 1, Vr. nrs. 9115, 9335, 9357, 9526, 9529, 9630, 9725, 9728, 9809, 9831, 9849, 9859 en 9861)

Samengevoegde vragen van O. Maingain, A. Carcaci, S. Van Hecke, K. Degroote en S. Lahaye-Battheu aan de eerste minister over 'het registreren van de vingerafdruk op de identiteitskaart' (*Hand.* Kamer 2015-16, 3 maart 2016, CRIV54PLEN100, 7, Vr. nrs. 1036 tot 1040)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over de 'gerechtelijke onderzoeken – versleutelde telefoons' (*Vr. en Ant.* Kamer 2015-16, 7 maart 2016, QRVA 065, 214, Vr. nr. 904)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de terugkerende Syriëstrijders en/of leden van IS' (*Vr. en Ant.* Kamer 2015-16, 7 maart 2016, QRVA 065, 226, Vr. nr. 952)

Vraag van Ph. Goffin aan de minister van Binnenlandse Zaken over de 'toegang van de politiediensten tot de informatie van OCAD' (*Vr. en Ant.* Kamer 2015-16, 7 maart 2016, QRVA 065, 230, Vr. nr. 966)

Vraag van S. Crusnière aan de minister van Buitenlandse Zaken over 'Tunesië' (*Vr. en Ant.* Kamer 2015-16, 7 maart 2016, QRVA 065, 266, Vr. nr. 323)

Vraag van Ph. Goffin aan de minister van Binnenlandse Zaken over de 'beveiliging van het justitiepaleis van Luik' (*Vr. en Ant.* Kamer 2015-16, 14 maart 2016, QRVA 066, 132, Vr. nr. 967)

Vraag van D. Ducarme aan de minister van Ontwikkelingssamenwerking over de 'Belgische wet- en regelgeving met betrekking tot het gebruik van encryptiesoftware' (*Vr. en Ant.* Kamer 2015-16, 14 maart 2016, QRVA 066, 177, Vr. nr. 423)

Vraag van F. Dewinter aan de minister van Justitie over 'de screening van kandidaat-asielzoekers op IS-strijders' (*Vr. en Ant.* Kamer 2015-16, 14 maart 2016, QRVA 066, 199, Vr. nr. 609)

Vraag van D. Ducarme aan de staatssecretaris voor Asiel en Migratie over 'Fedasil – radicalisme' (*Vr. en Ant.* Kamer 2015-16, 14 maart 2016, QRVA 066, 363, Vr. nr. 494)

Samengevoegde vragen van É. Thiébaut, G. Dallemagne, B. Hellings, B. Pas, H. Bonte, K. Degroote, Ph. Pivin en V. Yüksel aan de minister van Binnenlandse Zaken over 'de huiszoekingen in Vorst' (*Hand.* Kamer 2015-16, 17 maart 2016, CRIV54PLEN102, 2, Vr. nrs. 1078 tot 1085)

Vraag van F. Dewinter aan de minister van Justitie over 'de financiële stromen van Arabische of radicaalislamitische landen naar moskeën of islamitische verenigingen op het grondgebied van België' (*Vr. en Ant.* Kamer 2015-16, 21 maart 2016, QRVA 067, 252, Vr. nr. 667)

Gedachtewisseling met de minister van Binnenlandse Zaken over 'de terroristische aanslagen' (*Hand.* Kamer 2015-16, 25 maart 2016, CRIV54COM373, 1)

Vraag van N. Lijnen aan de minister van Defensie over de 'NAVO en EU – cyberdefensie' (*Vr. en Ant.* Kamer 2015-16, 4 april 2016, QRVA 068, 387, Vr. nr. 574)

Vraag van Ph. Pivin aan de minister van Defensie over de 'veiligheid en beveiliging bij de federale overheidsdiensten' (*Vr. en Ant.* Kamer 2015-16, 4 april 2016, QRVA 068, 409, Vr. nr. 591)

Samengevoegde vragen van Ph. Blanchart en S. Crusnière aan de minister van Justitie over 'de ontmoeting met Mehmet Görmez, voorzitter van Diyanet' (*Hand.* Kamer 2015-16, 13 april 2016, CRIV54COM379, 65, Vr. nrs. 10206 en 10234)

Vraag van I. De Coninck aan de minister van Mobiliteit over 'terroristen onder het personeel van de spoorwegen' (*Hand.* Kamer 2015-16, 13 april 2016, CRIV54COM381, 30, Vr. nr. 10486)

Samengevoegde vragen van B. Pas, V. Yüksel en K. Lalieux aan de minister van Mobiliteit over 'de open brief van de luchtvaartpolitie omtrent het veiligheidsprobleem op Zaventem' (*Hand.* Kamer 2015-16, 13 april 2016, CRIV54COM381, 41, Vr. nrs. 138, 10561 en 10651)

Samengevoegde vragen van V. Yüksel, A. Top en V. Matz aan de minister van Binnenlandse Zaken over 'de lijst van IS-strijders' (*Hand.* Kamer 2015-16, 13 april 2016, CRIV54COM382, 28, Vr. nrs. 10093, 10095 en 10116)

Vraag van J.-J. Flahaux aan de minister van Binnenlandse Zaken over de 'controles aan de Frans-Belgische grens' (*Vr. en Ant.* Kamer 2015-16, 14 april 2016, QRVA 069, 172, Vr. nr. 1017)

Vraag van F. Schepmans aan de minister van Binnenlandse Zaken over de 'intrekking van identiteitskaarten – toepassing' (*Vr. en Ant.* Kamer 2015-16, 14 april 2016, QRVA 069, 192, Vr. nr. 1131)

Vraag van B. Pas aan de minister van Buitenlandse Zaken over het 'NVO – veiligheidsattesten – radicalisme' (*Vr. en Ant.* Kamer 2015-16, 14 april 2016, QRVA 069, 251, Vr. nr. 507)

Vraag van Ph. Goffin aan de minister van Justitie over de 'beveiliging van het justitiepaleis van Luik' (*Vr. en Ant.* Kamer 2015-16, 14 april 2016, QRVA 069, 278, Vr. nr. 777)

Vraag van Ph. Pivin aan de staatssecretaris voor Asiel en Migratie over 'de aanhouding van een asielzoeker' (*Hand.* Kamer 2015-16, 20 april 2016, CRIV54COM387, 1, Vr. nr. 9091)

Vraag van Ph. Pivin aan de staatssecretaris voor Asiel en Migratie over 'de Veiligheid van de Staat en de samenwerking met de Dienst Vreemdelingenzaken' (*Hand.* Kamer 2015-16, 20 april 2016, CRIV54COM387, 14, Vr. nr. 9582)

Vraag van K. Jadin aan de staatssecretaris voor Asiel en Migratie over 'de repatriëring van Marokkaanse illegalen' (*Hand.* Kamer 2015-16, 20 april 2016, CRIV54COM387, 45, Vr. nr. 9870)

Samengevoegde vragen van A. Top, S. Pirlot, B. Hellings, D. Clarinval en V. Yüksel aan de minister van Defensie over 'de verhoogde inzet van militairen op straat' (*Hand.* Kamer 2015-16, 20 april 2016, CRIV54COM388, 23, Vr. nrs. 10620, 10638, 10667, 10723, 10809 en 10819)

Vraag van G. Dallemagne aan de minister van Justitie over 'het toezicht op bepaalde gebedshuizen' (*Hand.* Kamer 2015-16, 20 april 2016, CRIV54COM391, 10, Vr. nr. 10238)

Vraag van L. Onkelinx aan de eerste minister over 'de persconferentie van OCAD' (*Hand.* Kamer 2015-16, 21 april 2016, CRIV54PLEN107, 8, Vr. nr. 1115)

Vraag van K. Van Vaerenbergh aan de minister van Binnenlandse Zaken over het 'beschermingsopdrachten – beveiligingsmaatregelen' (*Vr. en Ant.* Kamer 2015-16, 25 april 2016, QRVA 070, 107, Vr. nr. 823)

Vraag van F. Schepmans aan de minister van Buitenlandse Zaken over het 'EU INTCEN' (*Vr. en Ant.* Kamer 2015-16, 25 april 2016, QRVA 070, 182, Vr. nr. 517)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over de 'pesterijen tegen de Rwandese democratische oppositie in België' (*Vr. en Ant.* Kamer 2015-16, 25 april 2016, QRVA 070, 185, Vr. nr. 522)

Vraag van Ph. Pivin aan de minister van Buitenlandse Zaken over de 'Actiris – bestrijding van radicalisme' (*Vr. en Ant.* Kamer 2015-16, 25 april 2016, QRVA 070, 187, Vr. nr. 529)

Vraag van Ph. Pivin aan de minister van Buitenlandse Zaken over de 'MIVB – strijd tegen radicalisme' (*Vr. en Ant.* Kamer 2015-16, 25 april 2016, QRVA 070, 189, Vr. nr. 530)

Vraag van V. Yüksel aan de minister van Defensie over 'het gebruik van verstorende elektromagnetische straling' (*Vr. en Ant.* Kamer 2015-16, 25 april 2016, QRVA 070, 314, Vr. nr. 631)

Vraag van R. Hedebouw aan de minister van Binnenlandse Zaken over 'de aanpak van de strijd tegen het terrorisme door de regering' (*Hand.* Kamer 2015-16, 27 april 2016, CRIV54COM399, 15, Vr. nr. 10453)

Samengevoegde vragen van R. Hedebouw aan de minister van Binnenlandse Zaken over 'Belgische Syriëstrijders' (*Hand.* Kamer 2015-16, 27 april 2016, CRIV54COM399, 17, Vr. nrs. 10456 en 10457)

Vraag van A. Carcaci aan de minister van Binnenlandse Zaken over 'de opening van een secundaire afdeling in een islamitische basisschool in Schaarbeek' (*Hand.* Kamer 2015-16, 27 april 2016, CRIV54COM400, 2, Vr. nr. 10963)

Samengevoegde vragen van G. Gilkinet aan de minister van Justitie over 'de bevriezing van de tegoeden en economische middelen in het kader van de strijd tegen terrorisme' (*Hand.* Kamer 2015-16, 27 april 2016, CRIV54COM400, 11, Vr. nrs. 11070 en 11071)

Vraag van de H. Bonte aan de eerste minister over 'de opvolging van Syriëstrijders' (*Hand.* Kamer 2015-16, 28 april 2016, CRIV54PLEN108, 12, Vr. nr. 1135)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de screening van kandidaat-asielzoekers op IS-strijders' (*Vr. en Ant.* Kamer 2015-16, 29 april 2016, QRVA 071, 91, Vr. nr. 1154)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'indienstnemingsprocedure voor aspirant-inspecteurs van politie – screening' (*Vr. en Ant.* Kamer 2015-16, 29 april 2016, QRVA 071, 124, Vr. nr. 1136)

Vraag van B. Pas aan de minister van Defensie over 'de aanwezigheid van moslimextremisten in het leger' (*Vr. en Ant.* Kamer 2015-16, 29 april 2016, QRVA 071, 256, Vr. nr. 636)

Vraag van I. De Coninck aan minister van Mobiliteit over de 'radicalisering bij het luchthavenpersoneel' (*Vr. en Ant.* Kamer 2015-16, 29 april 2016, QRVA 071, 280, Vr. nr. 1241)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over 'de evolutie van het aantal foreign fighters dat vertrekt naar Syrië' (*Hand.* Kamer 2015-16, 4 mei 2016, CRIV54PLEN109, 17, Vr. nr. 1160)

Vraag van K. Gabriëls aan de eerste minister over 'de coördinatie van de strijd tegen de financiering van het terrorisme' (*Vr. en Ant.* Kamer 2015-16, 9 mei 2016, QRVA 072, 54, Vr. nr. 131)

Samengevoegde vragen van P.-O. Delannois en Ph. Blanchart aan de minister van Binnenlandse Zaken over 'de veiligheid op de in de komende maanden geplande grote evenementen' (*Hand.* Kamer 2015-16, 11 mei 2016, CRIV54COM411, 28, Vr. nrs. 10705 en 10706)

Samengevoegde vragen van V. Matz en K. Gabriëls aan de minister van Binnenlandse Zaken over 'de veiligheid van de luchthavens' (*Hand.* Kamer 2015-16, 11 mei 2016, CRIV54COM411, 39, Vr. nrs. 10823 en 10824)

Samengevoegde vragen van M. De Lamotte en Ph. Blanchart aan de minister van Binnenlandse Zaken over 'het gevaar voor cyberaanvallen op kerncentrales' (*Hand.* Kamer 2015-16, 11 mei 2016, CRIV54COM411, 47, Vr. nrs. 10905 en 11450)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over 'het dreigingsniveau voor de nucleaire sector' (*Hand.* Kamer 2015-16, 11 mei 2016, CRIV54COM411, 59, Vr. nr. 10988)

Vraag van B. Hellings aan de minister van Justitie over 'de mogelijke zwarte lijst van de Turkse regering met 1200 Belgisch Turkse burgers en de toepassing van de wet 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' (*Hand.* Kamer 2015-16, 11 mei 2016, CRIV54COM413, 21, Vr. nr. 11150)

Samengevoegde vragen van K. Metsu en C. Cassart-Mailleux aan de minister van Defensie over 'Selor' (*Hand.* Kamer 2015-16, 11 mei 2016, CRIV54COM414, 13, Vr. nrs. 10671 en 10883)

Actualiteitsdebat en samengevoegde vragen van G. Grovonius, D. Van der Maelen, W. De Vriendt, J.-J. Flahaux, S. Claerhout en N. Lijnen aan de minister van Buitenlandse Zaken over 'de missie van de minister naar Israël en Palestina' (*Hand.* Kamer 2015-16, 11 mei 2016, CRIV54COM418, 1, Vr. nrs. 10327, 10791, 10928, 11294, 11423, 11455 en 11469)

Vraag van G. Vanden Burre aan de minister van Justitie over 'de inhuldiging van de eerste afdeling voor geradicaliseerde gevangenen in de gevangenis van Itter' (*Hand.* Kamer 2015-16, 18 mei 2016, CRIV54COM423, 9, Vr. nr. 11282)

Vraag van J.-J. Flahaux aan de minister van Binnenlandse Zaken over 'de top van Washington over nucleaire veiligheid' (*Hand*. Kamer 2015-16, 18 mei 2016, CRIV-54COM424, 16, Vr. nr. 11087)

Vraag van V. Yüksel aan de minister van Binnenlandse Zaken over 'de toepassing van de wet van 10 augustus 2015 omtrent de intrekking van identiteitskaarten van Syriëgangers' (*Hand*. Kamer 2015-16, 18 mei 2016, CRIV54COM424, 61, Vr. nr. 11595)

Samengevoegde vragen van K. Calvo, O. Maingain, M. Kitir, D. Ducarme, C. Fonck, P. Dedecker en J.-M. Nollet aan de eerste minister over 'de oproep van bedrijfsleiders' (*Hand*. Kamer 2015-16, 19 mei 2016, CRIV54PLEN111, 20, Vr. nrs. 1210 tot 1214, 1216 en 1217)

Vraag van V. Matz aan de minister van Binnenlandse Zaken over 'de overheveling van de beschermingsassistenten van de Veiligheid van de Staat naar de federale politie' (*Hand*. Kamer 2015-16, 25 mei 2016, CRIV54COM428, 14, Vr. nr. 11567)

Vraag van N. Ben Hamou aan de minister van Binnenlandse Zaken over 'een alarmprotocol op risicoplaatsen' (*Hand*. Kamer 2015-16, 25 mei 2016, CRIV54COM428, 22, Vr. nr. 11613)

Vraag van N. Ben Hamou aan de minister van Binnenlandse Zaken over 'het intrekken van de identiteitskaart van personen die geradicaliseerd zijn' (*Hand*. Kamer 2015-16, 25 mei 2016, CRIV54COM428, 46, Vr. nr. 11690)

Samengevoegde vragen van V. Matz en G. Vanden Burre aan de minister van Binnenlandse Zaken over 'het nationaal noodplan betreffende de aanpak van een terroristische gijzelneming of terroristische aanslag' (*Hand*. Kamer 2015-16, 25 mei 2016, CRIV54COM428, 54, Vr. nrs. 11752 en 11775)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over 'de diefstallen van identiteitskaarten bij de administraties' (*Hand*. Kamer 2015-16, 25 mei 2016, CRIV-54COM428, 64, Vr. nr. 11780)

Vraag van G. Gilkinet aan minister van Ontwikkelingssamenwerking over de 'veiligheid van de ambtenaren van de FOD's' (*Vr. en Ant*. Kamer 2015-16, 30 mei 2016, QRVA 075, 120, Vr. nr. 505)

Vraag van R. Deseyn aan minister van Energie over de 'inspectiedienst kritieke infrastructuur' (*Vr. en Ant*. Kamer 2015-16, 30 mei 2016, QRVA 075, 217, Vr. nr. 267)

Vraag van D. Ducarme aan minister van Defensie over de 'aanwerving van personeel bij Defensie' (*Vr. en Ant*. Kamer 2015-16, 30 mei 2016, QRVA 075, 245, Vr. nr. 685)

Samengevoegde vragen van K. Jadin, V. Yüksel, S. Pirlot en T. Vandenput aan de minister van Defensie over 'het gebruik van drones voor bewakingsopdrachten' (*Hand*. Kamer 2015-16, 31 mei 2016, CRIV54COM430, 22, Vr. nrs. 11092, 11183, 11313 en 11948)

Vaag van S. Pirlot aan de minister van Defensie over 'het door de regering beloofde extra budget voor veiligheid' (*Hand*. Kamer 2015-16, 31 mei 2016, CRIV54COM430, 32, Vr. nr. 11484)

Samengevoegde vragen van K. Gabriëls en M. De Coninck aan de staatssecretaris voor Asiel en Migratie over 'de omzetting van de richtlijn met betrekking tot de gecombineerde vergunning' (*Hand*. Kamer 2015-16, 1 juni 2016, CRIV54COM435, 5, Vr. nrs. 11145 en 11328)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de evenementen van Halal Events in de Ardennen' (*Hand*. Kamer 2015-16, 2 juni 2016, CRI-V54PLEN113, 37, Vr. nr. 1265)

Vraag van Ph. Blanchart aan de eerste minister over de 'bezoek aan Marokko – bestrijding van het terrorisme' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 168, Vr. nr. 141)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'aantal jihadisten in Libië' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 291, Vr. nr. 1247)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'mogelijk vertrek van Belgische foreign fighters naar Libië' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 294, Vr. nr. 1265)

Vraag van V. Yüksel aan de minister van Ontwikkelingssamenwerking over de 'stoorzenders' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 329, Vr. nr. 528)

Vraag van G. Gilkinet aan de minister van Buitenlandse Zaken over de 'veiligheid van de ambtenaren van de FOD's' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 341, Vr. nr. 548)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over de 'afluisterpraktijken van het NSA' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 352, Vr. nr. 574)

Vraag van J.-M. Nollet aan de minister van Buitenlandse Zaken over de 'intrekking van veiligheidsmachtigingen in de nucleaire sector' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 354, Vr. nr. 576)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over de 'bestand met IS-strijders' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 362, Vr. nr. 587)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over de 'inzet van de volgende NAVO-top in Warschau' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 366, Vr. nr. 602)

Vraag van V. Yüksel aan de minister van Defensie over de 'stoorzenders' (*Vr. en Ant.* Kamer 2015-16, 6 juni 2016, QRVA 076, 499, Vr. nr. 688)

Vraag van A. Top aan de minister van Binnenlandse Zaken over 'de terugtrekking van onbemande vliegtuigen uit de Antwerpse haven' (*Hand.* Kamer 2015-16, 8 juni 2016, CRIV54COM441, 48, Vr. nr. 11877)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over 'de beveiliging van de vertoningen op groot scherm van de voetbalwedstrijden in het kader van Euro 2016' (*Hand.* Kamer 2015-16, 8 juni 2016, CRIV54COM441, 31, Vr. nr. 11984)

Vraag van J. Penris aan de minister van Binnenlandse Zaken over 'de mededeling van namen van jihadisten aan de banken' (*Hand.* Kamer 2015-16, 9 juni 2016, CRIV54PLEN114, 19, Vr. nr. 1280)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'lijst van 22.000 jihadisten' (*Vr. en Ant.* Kamer 2015-16, 13 juni 2016, QRVA 077, 289, Vr. nr. 1261)

Vraag van V. Yüksel aan de minister van Justitie over 'het aantal teruggekeerde Syriëstrijders in ons land' (*Hand.* Kamer 2015-16, 15 juni 2016, CRIV54COM444, 22, Vr. nr. 12399)

Vraag van J. Klaps aan de minister van Werk over 'de schadeafwikkeling van terroristische daden' (*Hand.* Kamer 2015-16, 15 juni 2016, CRIV54COM446, 28, Vr. nr. 12040)

Samengevoegde vragen van V. Matz, M. Kitir, K. Degroote en Ph. Pivin aan de minister van Binnenlandse Zaken over 'de terreurdreiging' (*Hand.* Kamer 2015-16, 16 juni 2016, CRIV54PLEN115, 23, Vr. nrs. 1301 tot 1304)

Vraag van V. Matz aan de minister van Binnenlandse Zaken over 'de mogelijkheden om te verhinderen dat radicale groeperingen trainingen organiseren op ons grondgebied' (*Hand.* Kamer 2015-16, 22 juni 2016, CRIV54COM453, 9, Vr. nr. 12038)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over 'de woonstcontrole bij teruggekeerde Syriëstrijders' (*Hand.* Kamer 2015-16, 22 juni 2016, CRIV54COM453, 50, Vr. nr. 12338)

Vraag van K. Gabriëls aan de minister van Binnenlandse Zaken over 'het hoge aantal deserties bij IS' (*Hand.* Kamer 2015-16, 23 juni 2016, CRIV54PLEN116, 34, Vr. nr. 1327)

Samengevoegde vragen van E. Massin en Ph. Goffin aan de minister van Justitie over 'het journalistieke bronnengeheim' (*Hand.* Kamer 2015-16, 23 juni 2016, CRIV54PLEN116, 38, Vr. nrs. 1329 en 1330)

Vraag van V. Scourneau aan de minister van Binnenlandse Zaken over de 'dreiging met verontreiniging van watertorens en -reservoirs' (*Vr. en Ant.* Kamer 2015-16, 24 juni 2016, QRVA 079, 97, Vr. nr. 1243)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'IS – Belgische vrouwelijke strijders' (*Vr. en Ant.* Kamer 2015-16, 24 juni 2016, QRVA 079, 105, Vr. nr. 1259)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over de 'kinderen bij IS' (*Vr. en Ant.* Kamer 2015-16, 24 juni 2016, QRVA 079, 111, Vr. nr. 1279)

Vraag van O. Chastel aan de minister van Binnenlandse Zaken over de 'overeenkomst over de veiligheid en gegevensuitwisseling tussen België en Marokko' (*Vr. en Ant.* Kamer 2015-16, 24 juni 2016, QRVA 079, 121, Vr. nr. 1301)

Vraag van A. Top aan de minister van Defensie over 'de Belgische Systema-centra' (*Hand.* Kamer 2015-16, 29 juni 2016, CRIV54COM457, 1, Vr. nr. 11182)

Vraag van A. Top aan de minister van Defensie over 'de Belgische intercepties op Russische vliegtuigen' (*Hand.* Kamer 2015-16, 29 juni 2016, CRIV54COM457, 16, Vr. nr. 12160)

Vraag van S. Van Hecke aan de minister van Justitie over 'de terugkeer van magistraten na een detachering' (*Hand.* Kamer 2015-16, 29 juni 2016, CRIV54COM459, 31, Vr. nr. 12762)

Vraag van B. Hellings aan de minister van Binnenlandse Zaken over 'de 'luchtsteun' van drones van de federale politie om de bewegingen van migranten in de provincie West-Vlaanderen in het oog te houden' (*Hand.* Kamer 2015-16, 29 juni 2016, CRIV54COM461, 4, Vr. nr. 12313)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over 'de OCAD-analyses van het dreigingsniveau voor politiebureaus' (*Hand.* Kamer 2015-16, 29 juni 2016, CRIV54COM461, 25, Vr. nr. 12626)

Vraag van V. Yüksel aan de minister van Binnenlandse Zaken over 'de intrekking van identiteitskaarten van Syriëgangers (bis)' (*Hand.* Kamer 2015-16, 29 juni 2016, CRIV54COM461, 47, Vr. nr. 12810)

Vraag van D. Ducarme aan de minister van Justitie over de 'maatregelen tegen versleutelde gegevens op computers van verdachten in het kader van de strijd tegen het terrorisme' (*Vr. en Ant.* Kamer 2015-16, 1 juli 2016, QRVA 080, 231, Vr. nr. 867)

Vraag van P. Buysrogge aan de eerste minister over 'het verslag van het Comité I over het onderzoek naar de aandacht (of het gebrek daaraan) die de Belgische inlichtingen-

diensten hebben voor de mogelijke bedreigingen die elektronische programma's voor monitoring van communicatie- en informatiesystemen die vreemde mogendheden en/of buitenlandse inlichtingendiensten op grote schaal ontwikkelen, kunnen vormen voor het Belgisch wetenschappelijk en economisch potentieel' (*Hand.* Kamer 2015-16, 5 juli 2016, CRIV54COM463, 16, Vr. nr. 12275)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'Federal Computer Crime Unit' (*Vr. en Ant.* Kamer 2015-16, 8 juli 2016, QRVA 081, 126, Vr. nr. 1332)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'Syriëstrijders' (*Vr. en Ant.* Kamer 2015-16, 8 juli 2016, QRVA 081, 132, Vr. nr. 1381)

Vraag van G. Calomne aan de minister van Defensie over de 'beveiliging van de communicatie tussen de militaire attachés en de diensten van Defensie' (*Vr. en Ant.* Kamer 2015-16, 8 juli 2016, QRVA 081, 283, Vr. nr. 729)

Vraag van G. Dallemagne aan de minister van Middenstand over 'het beroepsgeheim en het doorspelen van gegevens door OCMW-werknemers' (*Hand.* Kamer 2015-16, 13 juli 2016, CRIV54COM477, 5, Vr. nr. 11216)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'de mededeling van namen van moslimextremisten aan de banken in verband met de financiering van terrorisme' (*Hand.* Kamer 2015-16, 13 juli 2016, CRIV54COM478, 4, Vr. nr. 12690)

Vraag van P.-O. Delannois aan de minister van Binnenlandse Zaken over 'de veiligheidsmachtiging voor burgemeesters in het kader van de veiligheid bij grote evenementen' (*Hand.* Kamer 2015-16, 13 juli 2016, CRIV54COM478, 23, Vr. nr. 13075)

Vraag van D. Ducarme aan de minister van Werk over de 'intrekking van veiligheidsmachtigingen bij de FOD Economie' (*Vr. en Ant.* Kamer 2015-16, 15 juli 2016, QRVA 082, 244, Vr. nr. 919)

Vraag van Ch. D'Haese aan de minister van Justitie over de 'Federale overheidsdiensten en openbare instellingen – personeelsbeleid' (*Vr. en Ant.* Kamer 2015-16, 15 juli 2016, QRVA 082, 281, Vr. nr. 865)

Vraag van F. Dewinter aan de minister van Defensie over de 'werkingsmiddelen veiligheidsdiensten' (*Vr. en Ant.* Kamer 2015-16, 15 juli 2016, QRVA 082, 451, Vr. nr. 737)

Vraag van F. Dewinter aan de minister van Defensie over de 'personeel veiligheidsdiensten – Arabisch' (*Vr. en Ant.* Kamer 2015-16, 15 juli 2016, QRVA 082, 453, Vr. nr. 738)

Vraag van P. Buysrogge aan de minister van Defensie over de 'VSSE en ADIV – fondsen om informanten te vergoeden – verslag toezichtonderzoek' (*Vr. en Ant.* Kamer 2015-16, 15 juli 2016, QRVA 082, 455, Vr. nr. 742)

Vraag van V. Scourneau aan de minister van Justitie over de 'versleuteling van smartphones' (*Vr. en Ant.* Kamer 2015-16, 25 juli 2016, QRVA 083, 165, Vr. nr. 888)

Vraag van V. Yüksel aan de minister van Defensie over de 'naamlinten op uniformen – het gebruik van sociale media bij militairen' (*Vr. en Ant.* Kamer 2015-16, 25 juli 2016, QRVA 083, 301, Vr. nr. 761)

Vraag nr. 671 van O. Chb astel aan de staatssecretaris voor Asiel en Migratie over de 'cel radicalisme' (*Vr. en Ant.* Kamer 2015-16, 25 juli 2016, QRVA 083, 372, Vr. nr. 671)

Vraag van F. Dewinter aan de minister van Justitie over 'Sharia4Belgium' (*Vr. en Ant.* Kamer 2015-16, 1 augustus 2016, QRVA 084, 141, Vr. nr. 1199)

Vraag van F. Dewinter aan de minister van Justitie over de 'Belgische jihadstrijders op buitenlands grondgebied' (*Vr. en Ant.* Kamer 2015-16, 1 augustus 2016, QRVA 084, 142, Vr. nr. 1201)

Vraag van F. Dewinter aan de minister van Justitie over de 'screening van moskeeën, moskeeverenigingen en islamitische organisaties' (*Vr. en Ant.* Kamer 2015-16, 1 augustus 2016, QRVA 084, 143, Vr. nr. 1203)

Vraag van D. Ducarme aan de minister van Justitie over de 'intrekking van veiligheidsmachtigingen bij de Veiligheid van de Staat' (*Vr. en Ant.* Kamer 2015-16, 1 augustus 2016, QRVA 084, 153, Vr. nr. 1275)

Vraag van V. Scourneau aan de minister van Financiën over de 'veiligheidskosten – dreigingsniveau 4' (*Vr. en Ant.* Kamer 2015-16, 1 augustus 2016, QRVA 084, 191, Vr. nr. 703)

Vraag van D. Ducarme aan de minister van Defensie over de 'intrekking van veiligheidsmachtigingen bij de Algemene Dienst Inlichting en Veiligheid (ADIV)' (*Vr. en Ant.* Kamer 2015-16, 1 augustus 2016, QRVA 084, 266, Vr. nr. 768)

Vraag van F. Schepmans aan de minister van Binnenlandse Zaken over de 'versleuteling van whatsapps' (*Vr. en Ant.* Kamer 2015-16, 16 augustus 2016, QRVA 085, 245, Vr. nr. 1330)

Vraag van D. Van der Maelen aan de minister van Binnenlandse Zaken over 'de bevoegdheid van Britse inlichtingendiensten op Belgisch grondgebieds' (*Vr. en Ant.* Kamer 2015-16, 16 augustus 2016, QRVA 085, 250, Vr. nr. 1386)

Vraag van B. Pas aan de minister van Buitenlandse Zaken over de 'maatregelen naar aanleiding van terrorisme – veiligheidscertificaten' (*Vr. en Ant.* Kamer 2015-16, 16 augustus 2016, QRVA 085, 326, Vr. nr. 678)

Vraag van P. Pivin aan de minister van Buitenlandse Zaken over de 'screening bij de overheidsbedrijven – NVO' (*Vr. en Ant.* Kamer 2015-16, 16 augustus 2016, QRVA 085, 327, Vr. nr. 633)

Vraag van D. Ducarme aan de minister van Buitenlandse Zaken over de 'intrekking van paspoorten' (*Vr. en Ant.* Kamer 2015-16, 16 augustus 2016, QRVA 085, 351, Vr. nr. 663)

Vraag van D. Ducarme aan de minister van Buitenlandse Zaken over de 'intrekking van veiligheidsmachtigingen bij de FOD Buitenlandse Zaken' (*Vr. en Ant.* Kamer 2015-16, 16 augustus 2016, QRVA 085, 352, Vr. nr. 670)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over 'de uitspraken tegen extreemrechts' (*Vr. en Ant.* Kamer 2015-16, 26 augustus 2016, QRVA 086, 153, Vr. nr. 1331)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over de 'kerncentrales – onderaanbesteding in de IT-sector' (*Vr. en Ant.* Kamer 2015-16, 26 augustus 2016, QRVA 086, 162, Vr. nr. 1377)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over de 'inlichtigendiensten – dataverwerking' (*Vr. en Ant.* Kamer 2015-16, 26 augustus 2016, QRVA 086, 165, Vr. nr. 1382)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over de 'screening van moskeën, moskeeverenigingen en islamitische organisaties' (*Vr. en Ant.* Kamer 2015-16, 26 augustus 2016, QRVA 086, 167, Vr. nr. 1391)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over de 'werkingsmiddelen veiligheidsdiensten' (*Vr. en Ant.* Kamer 2015-16, 26 augustus 2016, QRVA 086, 180, Vr. nr. 1413)

Vraag van O. Chastel aan de minister van Binnenlandse Zaken over 'Benelux – samenwerking tegen het terrorisme' (*Vr. en Ant.* Kamer 2015-16, 26 augustus 2016, QRVA 086, 206, Vr. nr. 1460)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'intrekking van identiteitskaarten' (*Vr. en Ant.* Kamer 2015-16, 26 augustus 2016, QRVA 086, 208, Vr. nr. 1473)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'toegang tot de gegevens van versleutelde berichtendiensten' (*Vr. en Ant.* Kamer 2015-16, 26 augustus 2016, QRVA 086, 218, Vr. nr. 1493)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'radicalisering in de Grote Moskee in het Jubelpark' (*Vr. en Ant.* Kamer 2015-16, 26 augustus 2016, QRVA 086, 225, Vr. nr. 1507)

Vraag van K. Gabriëls aan de minister van Binnenlandse Zaken over 'de cyberveiligheid van onze kerncentrales' (*Vr. en Ant.* Kamer 2015-16, 5 september 2016, QRVA 087, 56, Vr. nr. 1287)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over 'politieonderzoeken – samenwerkingsprotocollen inzake technieken en technologieën' (*Vr. en Ant.* Kamer 2015-16, 5 september 2016, QRVA 087, 60, Vr. nr. 1310)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'Internet – radicale islam' (*Vr. en Ant.* Kamer 2015-16, 5 september 2016, QRVA 087, 78, Vr. nr. 1396)

Vraag van P. Buysrogge aan de minister van Binnenlandse Zaken over de 'VSSE – investeringen in de infrastructuur' (*Vr. en Ant.* Kamer 2015-16, 5 september 2016, QRVA 087, 97, Vr. nr. 1438)

Vraag van N. Ben Hamou aan de minister van Binnenlandse Zaken over de 'strijd tegen terrorisme – verzamelen van passagiersgegevens' (*Vr. en Ant.* Kamer 2015-16, 5 september 2016, QRVA 087, 118, Vr. nr. 1520)

Vraag van V. Scourneau aan de minister van Buitenlandse Zaken over de 'veiligheidskosten – dreigingsniveau 4' (*Vr. en Ant.* Kamer 2015-16, 12 september 2016, QRVA 088, 172, Vr. nr. 428)

Vraag van R. Deseyn aan de minister van Buitenlandse Zaken over de 'rekruteren Russische spionnen' (*Vr. en Ant.* Kamer 2015-16, 12 september 2016, QRVA 088, 198, Vr. nr. 647)

Vraag van J.-M. Nollet aan de minister van Buitenlandse Zaken over de 'intrekking van veiligheidsmachtigingen in de Belgische kerncentrales' (*Vr. en Ant.* Kamer 2015-16, 12 september 2016, QRVA 088, 202, Vr. nr. 652)

Vraag van S. Lahaye-Battheu aan de minister van Buitenlandse Zaken over 'de rol van de ambassades in het promoten van België in het buitenland' (*Vr. en Ant.* Kamer 2015-16, 12 september 2016, QRVA 088, 204, Vr. nr. 655)

Vraag van C. Fonck aan de minister van Buitenlandse Zaken over de 'reizen naar landen waar het zikavirus heerst' (*Vr. en Ant.* Kamer 2015-16, 12 september 2016, QRVA 088, 244, Vr. nr. 748)

Vraag van K. Metsu aan de minister van Justitie over de 'inlichtingendiensten – opvolging' (*Vr. en Ant.* Kamer 2015-16, 12 september 2016, QRVA 088, 251, Vr. nr. 554)

Vraag van B. Pas aan de minister van Justitie over de 'maatregelen naar aanleiding van terrorisme – ondersteuning rechercheurs' (*Vr. en Ant.* Kamer 2015-16, 12 september 2016, QRVA 088, 284, Vr. nr. 1180)

Vraag van Ph. Pivin aan de minister van Justitie over de 'samenwerking tussen de Belgische inlichtingendiensten en Europol' (*Vr. en Ant.* Kamer 2015-16, 12 september 2016, QRVA 088, 313, Vr. nr. 1301)

Vraag van B. Hellings aan de minister van Justitie over 'de toepassing van de wet van 29 januari 2016 aangaande het toezicht op de activiteiten van de buitenlandse inlichtingendiensten in België in het licht van de recente politieke gebeurtenissen in Turkije' (*Hand*. Kamer 2015-16, 21 september 2016, CRIV54COM492, 25, Vr. nr. 13599)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'infiltratie van terroristen via de asielzoekersstroom' (*Vr. en Ant.* Kamer 2015-16, 23 september 2016, QRVA 089, 73, Vr. nr. 1392)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'Ibrahim El Bakraoui' (*Vr. en Ant.* Kamer 2015-16, 23 september 2016, QRVA 089, 77, Vr. nr. 1385)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'Belgische jihadstrijders op buitenlands grondgebied' (*Vr. en Ant.* Kamer 2015-16, 23 september 2016, QRVA 089, 80, Vr. nr. 1388)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over de 'personeel Veiligheidsdiensten – Arabisch' (*Vr. en Ant.* Kamer 2015-16, 23 september 2016, QRVA 089, 84, Vr. nr. 1414)

Vraag van E. Lachaert aan de minister van Buitenlandse Zaken over de 'afleveren van veiligheidscertificaten voor personeelsleden door de Nationale Veiligheidsoverheid' (*Vr. en Ant.* Kamer 2015-16, 23 september 2016, QRVA 089, 174, Vr. nr. 741)

Vraag van J.-M. Nollet aan de minister van Justitie over de 'samenwerking met privébedrijven in het kader van politieonderzoeken' (*Vr. en Ant.* Kamer 2015-16, 23 september 2016, QRVA 089, 199, Vr. nr. 1278)

Vraag van F. Dewinter aan de minister van Justitie over de 'registratie Syriëstrijders' (*Vr. en Ant.* Kamer 2015-16, 23 september 2016, QRVA 089, 200, Vr. nr. 1202)

Vraag van D. Geerts aan minister van Mobiliteit over de 'luchthavens in België – toekenning en intrekking van badges' (*Vr. en Ant.* Kamer 2015-16, 23 september 2016, QRVA 089, 363, Vr. nr. 1517)

Vraag van F. Dewinter aan de staatssecretaris voor Asiel en Migratie over de 'migranten uit OIC-landen – screening' (*Vr. en Ant.* Kamer 2015-16, 23 september 2016, QRVA 089, 457, Vr. nr. 702)

Vraag van B. Vermeulen aan de minister van Binnenlandse Zaken over 'het gebruik van het internet door extreem linkse groeperingen en activisten' (*Hand*. Kamer 2015-16, 21 september 2016, CRIV54COM493, 9, Vr. nr. 13200)

Samengevoegde vragen van K. Calvo en S. Lahaye-Battheu aan de minister van Justitie over de 'informatie over State Grid' (*Hand*. Kamer 2015-16, 28 september 2016, CRIV54COM497, 40, Vr. nrs. 13912 tot 13927)

Samengevoegde vragen van L. Onkelinx, F. Dewinter, H. Bonte, G. Vanden Burre en K. Degroote aan de minister van Binnenlandse Zaken over 'de aanval op agenten in Schaarbeek' (*Hand*. Kamer 2015-16, 6 oktober 2016, CRIV54PLEN128, 19, Vr. nrs. 1484 tot 1489)

Vraag van O. Chastel aan de minister van Binnenlandse Zaken over de 'missie naar Turkije' (*Vr. en Ant.* Kamer 2016-17, 7 oktober 2016, QRVA 090, 60, Vr. nr. 1149)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'maatregelen naar aanleiding van terrorisme – extra aanwervingen veiligheidsdiensten' (*Vr. en Ant.* Kamer 2016-17, 7 oktober 2016, QRVA 090, 73, Vr. nr. 1364)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'maatregelen naar aanleiding van terrorisme – jongeren verhinderen te vertrekken' (*Vr. en Ant.* Kamer 2016-17, 7 oktober 2016, QRVA 090, 76, Vr. nr. 1366)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de opvolging van terugkerende Syriëstrijders' (*Vr. en Ant.* Kamer 2016-17, 7 oktober 2016, QRVA 090, 78, Vr. nr. 1383)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over de 'registratie Syriestrijders' (*Vr. en Ant.* Kamer 2016-17, 7 oktober 2016, QRVA 090, 82, Vr. nr. 1390)

Vraag van K. Jadin aan de minister van Ontwikkelingssamenwerking over de 'illegaal gebruik van gsm-stoorders door DOVO' (*Vr. en Ant.* Kamer 2016-17, 7 oktober 2016, QRVA 090, 127, Vr. nr. 637)

Vraag W. De Vriendt aan de minister van Defensie over de 'Centraal-Afrikaanse Republiek – operatie EUTM-CAR' (*Vr. en Ant.* Kamer 2016-17, 7 oktober 2016, QRVA 090, 480, Vr. nr. 799)

Vraag D. Ducarme aan de minister van Defensie over de 'implementatie van het protocol tot oprichting van de Belgian Intelligence Academy' (*Vr. en Ant.* Kamer 2016-17, 7 oktober 2016, QRVA 090, 518, Vr. nr. 833)

Vraag F. Schepmans aan de minister van Defensie over de 'Open Source and Social Media Collect and Analyse Tool' (*Vr. en Ant.* Kamer 2016-17, 7 oktober 2016, QRVA 090, 525, Vr. nr. 847)

Vraag van Ph. Pivin aan de minister van Justitie over 'de werving van minderjarigen door Daesh' (*Hand.* Kamer 2016-17, 13 oktober 2016, CRIV54PLEN130, 57, Vr. nr. 1515)

Vraag van L. Van Biesen aan de minister van Justitie over de 'administraties – overheidsbedrijven – aanwervingen van personen met een arbeidshandicap' (*Vr. en Ant.* Kamer 2016-17, 14 oktober 2016, QRVA 091, 292, Vr. nr. 48)

Vraag van K. Jadin aan de minister van Buitenlandse Zaken over 'de aanslagen van 1 juli 2016 in Dhaka, Bangladesh' (Hand. Kamer 2016-17, 19 oktober 2016, CRIV54COM513, 8, Vr. nr. 12971)

Vraag van O. Maingain aan de minister van Binnenlandse Zaken over 'de bedreigingen aan het adres van scholen waarvan men acht dat ze gelieerd zijn aan de Gülenbeweging' (*Hand.* Kamer 2016-17, 19 oktober 2016, CRIV54COM514, 1, Vr. nr. 13574)

Samengevoegde vragen van F. Dewinter en A. Carcaci aan de minister Binnenlandse Zaken over 'de terugkeer van jihadisten' (*Hand.* Kamer 2016-17, 20 oktober 2016, CRIV54PLEN136, 16, Vr. nrs. 1531 en 1532)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'de dreiging van chemische en biologische wapens' (*Vr. en Ant.* Kamer 2016-17, 21 oktober 2016, QRVA 092, 72, Vr. nr. 1181)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over de 'raadpleging van het Rijksregister' (*Vr. en Ant.* Kamer 2016-17, 21 oktober 2016, QRVA 092, 91, Vr. nr. 1579)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'databank in de strijd tegen radicalisering' (*Vr. en Ant.* Kamer 2016-17, 21 oktober 2016, QRVA 092, 101, Vr. nr. 1598)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'opvolging van teruggekeerde Syriëstrijders en van personen die er niet in slaagden Syrië te bereiken' (*Vr. en Ant.* Kamer 2016-17, 21 oktober 2016, QRVA 092, 129, Vr. nr. 1629)

Vraag van K. Jadin aan de minister van Defensie over de 'open source and social media collect and analyse tool' (*Vr. en Ant.* Kamer 2016-17, 21 oktober 2016, QRVA 092, 317, Vr. nr. 872)

Vraag van D. Ducarme aan de staatssecretaris voor Asiel en Migratie over 'Syrische paspoorten' (*Vr. en Ant.* Kamer 2016-17, 21 oktober 2016, QRVA 092, 344, Vr. nr. 636)

Vraag van S. Smeyers aan de staatssecretaris voor Asiel en Migratie over 'de screening van asielzoekers op radicalisme' (*Hand.* Kamer 2016-17, 26 oktober 2016, CRIV54COM518, 16, Vr. nr. 14630)

Samengevoegde vragen van B. Pas et A. Frédéric aan de staatssecretaris voor Asiel en Migratie over 'de uitzetting van haatpredikers' (*Hand.* Kamer 2016-17, 26 oktober 2016, CRIV54COM518, 13, Vr. nrs. 14150 en 14554)

Vraag van S. Van Hecke aan de staatssecretaris voor Bestrijding van de sociale Fraude over 'het advies van de Privacycommissie met betrekking tot de mogelijkheid tot kabeltap' (*Hand.* Kamer 2016-17, 26 oktober 2016, CRIV54COM519, 1, Vr. nr. 11741)

Vraag van Z. Demir aan de minister van Werk over 'Syriëstrijders – werkloosheidsuitkeringen' (*Vr. en Ant.* Kamer 2016-17, 28 oktober 2016, QRVA 093, 144, Vr. nr. 995)

Vraag van Ph. Pivin aan de minister van Financiën over de 'samenwerking tussen de Algemene Administratie van de Douane en Accijnzen van de FOD Financiën en Europol' (*Vr. en Ant.* Kamer 2016-17, 28 oktober 2016, QRVA 093, 278, Vr. nr. 1252)

Vraag van G. Dallemagne aan de minister van Defensie over de 'impact van operatie-Vigilant Guardian op Defensie en mogelijke oprichting van een veiligheidskorps voor de gebouwen' (*Vr. en Ant.* Kamer 2016-17, 28 oktober 2016, QRVA 093, 330, Vr. nr. 864)

Vraag van N. Lijnen aan de minister van Defensie over 'thuiswerk.' (*Vr. en Ant.* Kamer 2016-17, 28 oktober 2016, QRVA 093, 335, Vr. nr. 867)

Vraag van B. Hellings aan de minister van Buitenlandse Zaken over 'de Belgische acties en standpunten ten aanzien van het lopende onderzoek naar het verdachte overlijden in 1961 van VN-secretaris-generaal Dag Hammarskjöld' (*Hand.* Kamer 2016-17, 8 november 2016, CRIV54COM523, 50, Vr. nr. 14329)

Vraag van B. Hellings aan de minister van Buitenlandse Zaken over 'de zogenaamde Afrikaanse archieven' (*Hand.* Kamer 2016-17, 8 november 2016, CRIV54COM523, 52, Vr. nr. 14555)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over 'het toezicht op de sekten' (*Hand.* Kamer 2016-17, 9 november 2016, CRIV54COM529, 14, Vr. nr. 14723)

Vraag van V. Yüksel aan de minister van Binnenlandse Zaken over 'de opvolging van Syriëstrijders' (*Hand.* Kamer 2016-17, 9 november 2016, CRIV54COM533, 15, Vr. nr. 14371)

Samengevoegde vragen van G. Dallemagne en H. Bonte aan de minister van Binnenlandse Zaken over 'de middelen die worden ingezet voor de veiligheid en de terreurbestrijding' (*Hand.* Kamer 2016-17, 10 november 2016, CRIV54PLEN138, 17, nrs. 1574 en 1597)

Vraag van V. Yüksel aan de minister van Justitie over 'de bevriezing van de tegoeden van de terrorist Oussama Atar' (*Hand.* Kamer 2016-17, 10 november 2016, CRIV54PLEN138, 20, nr. 1575)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'bescherming van de gebedsplaatsen' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 094, 100, Vr. nr. 1640)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'Foreign terrorist fighters' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 094, 108, Vr. nr. 1690)

Vraag van D. Ducarme aan de minister van Binnenlandse Zaken over de 'screening van personen die in de nucleaire sector werken' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 094, 110, 1693)

Vraag van D. Ducarme aan de minister van Justitie over de 'toegang tot versleutelde smartphonegegevens in het kader van de strijd tegen terrorisme' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 094, 121, Vr. nr. 868)

Vraag van F. Dewinter aan de minister van Justitie over de 'radicale islam' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 094, 124, Vr. nr. 1195)

Vraag van D. Ducarme aan de minister van Defensie over de 'gebruik van UAV's boven de Noordzee' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 094, 241, Vr. nr. 876)

Vraag van R. Deseyn aan de minister van Ontwikkelingssamenwerking over de 'inspectiedienst kritieke infrastructuur' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 095, 94, Vr. nr. 698)

Vraag van S. Crusnière aan de minister van Buitenlandse Zaken over de 'intrekking van paspoorten en verblijfstitels' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 095, 101, Vr. nr. 624)

Vraag van F. Dewinter aan de minister van Justitie over de 'terreuraanslagen door IS in Europa' (*Vr. en Ant.* Kamer 2016-1, 16 november 2016, QRVA 095, 120, Vr. nr. 1197)

Vraag van J.J. Flahaux aan de minister van Justitie over 'ransomwareaanvallen' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 095, 149, Vr. nr. 1467)

Vraag van B. Pas aan de minister van Justitie over 'de inzet van nieuwe technologie in de strijd tegen terrorisme' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 095, 157, Vr. nr. 1482)

Vraag van B. Pas aan de minister van Justitie over de 'extra aanwervingen voor de veiligheidsdiensten' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 095, 158, Vr. nr. 1483)

Vraag van B. Pas aan de minister van Justitie over 'de screening van haatpredikers' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 095, 160, Vr. nr. 1485)

Vraag van R. Deseyn aan de minister van Financiën over de 'inspectiedienst kritieke infrastructuur' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 095, 278, Vr. nr. 1226)

Vraag van R. Deseyn aan de minister van Energie over de 'inspectiedienst kritieke infrastructuur' (*Vr. en Ant.* Kamer 2016-17, 16 november 2016, QRVA 095, 290, Vr. nr. 356)

Vraag van F. Dewinter aan de minister van Justitie over de 'werkingsmiddelen veiligheidsdiensten' (*Vr. en Ant.* Kamer 2016-17, 23 november 2016, QRVA 096, 146, Vr. nr. 1210)

Vraag van G. Dallemagne aan de minister van Defensie over de 'agressie tegen drie politieagenten door een ex-militair in Schaarbeek' (*Vr. en Ant.* Kamer 2016-17, 23 november 2016, QRVA 096, 278, Vr. nr. 925)

Vraag van B. Pas aan de minister van Justitie over 'het protocol tussen de Vlaamse onderwijsadministratie en de Veiligheid van de Staat' (*Vr. en Ant.* Kamer 2016-17, 23 november 2016, QRVA 097, 289, Vr. nr. 998)

Vraag van B. Pas aan de minister van Justitie over de 'maatregelen naar aanleiding van terrorisme en nieuwe technologie' (*Vr. en Ant.* Kamer 2016-17, 23 november 2016, QRVA 097, 300, Vr. nr. 1184)

Samengevoegde vragen van G. Gilkinet aan de minister van Justitie over 'de mogelijke verjaringsdatum in het dossier-Chodiev' (*Hand*. Kamer 2016-17, 30 november 2016, CRIV54COM545, 7, nrs. 15247 tot 15252)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'de sociale voordelen voor Syriëstrijders' (*Vr. en Ant.* Kamer 2016-17, 7 december 2016, QRVA 098, 205, Vr. nr. 1738)

Vraag van J.-M. Nollet aan de minister van Binnenlandse Zaken over het 'onderzoek van de Veiligheid van de Staat in bedrijven' (*Vr. en Ant.* Kamer 2016-17, 7 december 2016, QRVA 098, 211, Vr. nr. 1798)

Vraag van R. Deseyn aan de minister van Ontwikkelingssamenwerking over de 'anonieme simkaarten' (*Vr. en Ant.* Kamer 2016-17, 7 december 2016, QRVA 098, 212, Vr. nr. 697)

Vraag van D. Ducarme aan de minister van Justitie over de 'brandstichting bij het NICC' (*Vr. en Ant.* Kamer 2016-17, 7 december 2016, QRVA 098, 251, Vr. nr. 1383)

Vraag van S. Pirlot aan de minister van Defensie over 'het wetsontwerp tot wijziging van de wet houdende regeling van de inlichtingen- en veiligheidsdiensten van 30 november 1998 en inzonderheid artikel 21/1' (*Hand*. Kamer 2016-17, 14 december 2016, CRIV54COM550, 25, Vr. nr. 15451)

Vraag van B. Hellings aan de minister van Defensie over 'de deelname van Defensie aan het onderzoek dat het Internationaal Strafhof waarschijnlijk zal instellen naar de sinds 2003 in Afghanistan gepleegde misdaden' (*Hand*. Kamer 2016-17, 14 december 2016, CRIV54COM550, 31, Vr. nr. 14988)

Vraag van K. Van Vaerenbergh aan de minister van Justitie over 'de radicalisering in de gevangenissen' (*Hand*. Kamer 2016-17, 14 december 2016, CRIV54COM552, 21, Vr. nr. 15460)

Vraag van L. Onkelinx aan de eerste minister over 'de reiswaarschuwing van het Amerikaanse State Department voor Europa' (*Hand*. Kamer 2016-17, 14 december 2016, CRIV54COM555, 12, Vr. nr. 15160)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de eventuele sluiting van de Grote Moskee in het Jubelpark in Brussel' (*Vr. en Ant.* Kamer 2016-17, 14 december 2016, QRVA 099, 81, Vr. nr. 1470)

Vraag van G. Calomne aan de minister van Binnenlandse Zaken over 'de beveiliging van drinkwatervoorzieningen' (*Vr. en Ant.* Kamer 2016-17, 14 december 2016, QRVA 099, 82, Vr. nr. 1498)

Vraag van S. de Coster-Bauchau aan de minister van Justitie over 'tekort aan islamconsulenten in de gevangenissen van Itter, Vorst en Nijvel' (*Vr. en Ant.* Kamer 2016-17, 14 december 2016, QRVA 099, 134, Vr. nr. 1509)

Samengevoegde vragen van F. Dewinter en P. De Roover aan de minister van Justitie over 'de spionagerol van de Turkse Diyanetmoskeeën' (*Hand*. Kamer 2016-17, 15 december 2016, CRIV54PLEN144, 24, Vr. nrs. 1704 en 1705)

Vraag van K. Metsu aan de minister van Justitie over de 'radicalisme in de gevangenis' (*Vr. en Ant.* Kamer 2016-17, 23 december 2016, QRVA 100, 279, Vr. nr. 1535)

BIJLAGE D.
ADVIES BIJ HET WETSONTWERP TOT REGELING VAN DE PRIVATE VEILIGHEID

De voorzitter van het Vast Comité I, die tevens voorzitter is van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen, werd bij brief van 28 september 2016 door de minister van Veiligheid en Binnenlandse Zaken gevraagd om een advies te formuleren bij de bepalingen van het Wetsontwerp tot regeling van de private veiligheid die het Beroepsorgaan aanbelangen.

Aangezien het voorontwerp binnen enkele weken in eerste lezing op de Ministerraad zal worden besproken, werd ervoor geopteerd dit advies op bijzonder korte termijn te verlenen. Hierdoor kon niet op elk aspect in detail worden ingegaan.

De krachtlijnen van het advies en van het bijgevoegde voorstel tot wijziging van de Wet van 11 december 1998 werden doorgesproken met de (plaatsvervangende) leden van het Vast Comité P en de Privacycommissie die zetelen in het Beroepsorgaan. Zij konden hiermee instemmen.

Bijkomende werklast opvangen door efficiëntiewinst

Het Beroepsorgaan wenst vooreerst te benadrukken dat het niet weigerachtig staat tegenover het voorstel om een deel van het administratieve contentieux inzake de private veiligheid naar het Beroepsorgaan over te hevelen.

Wel betekent deze overheveling een aanzienlijke bijkomende werklast voor het Beroepsorgaan dat niet over een specifiek budget of personeelsbestand beschikt. De kosten voor de werking van het Beroepsorgaan komen immers ten laste van de begroting van het Vast Comité I, dat in deze de griffiefunctie waarneemt. Uiteraard betekent een bijkomende werklast ook extra werk voor de drie leden van het Beroepsorgaan of hun respectieve plaatsvervangers.

De werkdruk van het Beroepsorgaan is de laatste jaren stelselmatig toegenomen, vooral doordat de te behandelen dossiers steeds complexer zijn geworden op het vlak van administratief beheer, de behandeling ter terechtzitting en de redactie van de beslissingen. Zo bijvoorbeeld zijn de administratieve dossiers die door de veiligheidsoverheden worden overgemaakt, niet steeds compleet zodat de griffie bijkomende handelingen moet stellen om ze te vervolledigen. Hetzelfde geldt voor de toepassing van artikel 5 § 3 van de Wet op het Beroepsorgaan: het verzoek om bepaalde stukken niet ter inzage te verlenen van de verzoeker, is zelden gemotiveerd of gaat uit van de verkeerde instantie, zodat de griffie ook hier bijkomende informatie moet inwinnen. Verder dient te worden vastgesteld dat de zittingen veel meer tijd in beslag nemen dan een aantal jaren geleden. Dit heeft verschillende oorzaken. Steeds meer verzoekers laten zich bijstaan door een advocaat die ter zitting het standpunt van zijn cliënt toelicht. Ook vragen de betrokken politie- of inlichtingendiensten steeds vaker om te worden gehoord. Gelet op de complexiteit van sommige zaken, wordt hier veel tijd aan besteed. Ten slotte moeten – anders dan vroeger – veel zaken op

een tweede of derde zitting worden hernomen, ofwel omdat een verzoeker uitstel vraagt ofwel omdat in het dossier gewacht wordt op bijkomende informatie. Ook het beslissingsproces zelf vergt meer tijd dan een aantal jaren geleden. Hiervoor zijn twee belangrijke redenen aan te halen. Enerzijds worden er meer procedurele kwesties opgeworpen (bijvoorbeeld het debat over ontvankelijkheid, de taalproblematiek, de rechten van verdediging, de 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.

Zowel het Vast Comité I als het Beroepsorgaan willen er op wijzen dat de werklast in de nabije toekomst nog zal toenemen. Enerzijds valt te verwachten dat het contentieux van personen werkzaam in de private opsporing kortelings zal moeten overgeheveld worden naar het Beroepsorgaan. Zoniet lijkt een moeilijk te verantwoorden onderscheid te worden ingebouwd in twee verwante sectoren die steeds aan dezelfde regeling werden onderworpen. Anderzijds heeft de Regering reeds meermaals aangekondigd dat het aantal veiligheidsscreenings zal toenemen (bijvoorbeeld voor personen werkzaam in kritieke infrastructuren). Aangezien het hier over tienduizenden bijkomende screenings gaat, zal dit zich laten gevoelen in een toenemend aantal beroepen.

Het Beroepsorgaan is van oordeel dat de bijkomende werklast deels kan ondervangen worden door een aanpassing van de bestaande regeling waardoor een zekere efficiëntiewinst kan gerealiseerd worden. Het Beroepsorgaan denkt daarbij vooral aan de introductie van een eenvoudige en duidelijke beroepsakte en aan verplichte antwoordtermijnen voor de partijen. Het is immers zo dat de griffie van het Beroepsorgaan momenteel veel tijd en middelen moet investeren in het bekomen van de vereiste stukken (rappels, mails, telefoongesprekken …). Ook de invoering van een beperkt rolrecht – zoals dat bijvoorbeeld geldt voor de Raad van State – kan een aantal nutteloze beroepen voorkomen. Verder wordt voorzien in twee louter schriftelijke procedures: wanneer de eis manifest gegrond is of wanneer ze kennelijk onontvankelijk is, wordt voorgesteld uitspraak te kunnen doen op basis van een schriftelijke procedure. Hierdoor worden nodeloze zittingen vermeden.

Maar de grootste efficiëntiewinst zou ongetwijfeld bestaan uit de invoering van een hoorplicht door de betrokken overheid wanneer zij een negatief veiligheidsoordeel wenst te formuleren. Het Beroepsorgaan wordt immers al te vaak geconfronteerd met dossiers die hadden kunnen uitgeklaard worden door de betrokken administratie op basis van een eenvoudig gesprek, gekoppeld aan een (beperkte) toegang tot het administratieve dossier. In de meeste zaken heeft de betrokkene vooraf geen enkele inzagemogelijkheid gehad: dit is op puur principieel vlak discutabel, zeker wanneer het een intrekking van een eerder toegekende toelating betreft. Daarbij moet ook opgemerkt worden dat de beslissingen van de meeste veiligheidsoverheden dermate beknopt gemotiveerd zijn, dat de betrokkene nauwelijks begrijpt waarom hij of zij het voorwerp uitmaakt van een negatieve beslissing. Deze praktijk zou moeten veranderen.

Om deze efficiëntiewinst te realiseren dient niet alleen het Wetsontwerp tot regeling van de private veiligheid te worden gewijzigd maar ook de Classificatiewet van 11 december

1998 én de Wet van 11 december 1998 tot oprichting van het Beroepsorgaan en – nadien – de uitvoeringsbesluiten. Bijgaand bij dit advies is een voorstel tot ontwerp tot wijziging van de Wet van 11 december 1998 tot oprichting van het Beroepsorgaan gevoegd. Er is trouwens ook een juridisch-technische reden waarom deze wet via een apart ontwerp, en niet via een aantal bepalingen in het Wetsontwerp tot regeling van de private veiligheid, moet worden gewijzigd.

Noodzakelijke wijziging van de Wet van 11 december 1998 tot oprichting van het Beroepsorgaan

Het Wetsontwerp tot regeling van de private veiligheid, dat naar luid van artikel 1 een aangelegenheid regelt zoals voorzien in artikel 74 van de Grondwet, wijzigt in zijn artikelen 75 tot 80 *de facto* de regels die betrekking hebben op het Beroepsorgaan, al was het maar door een bijkomende bevoegdheid toe te kennen aan dit administratieve rechtscollege. Echter, '*de wetten op de Raad van State en op de federale administratieve rechtscolleges*' zijn onderworpen aan artikel 78 van de Grondwet waardoor het door de Kamer aangenomen ontwerp naar de Senaat moet worden gezonden. Het voorliggend ontwerp moet dan ook gesplitst worden en de bepalingen die betrekking hebben op het beroep tegen de beslissing van de minister, moeten in de Wet van 11 december 1998 gevoegd worden.

De in deze wet door het Beroepsorgaan voorgestelde wijzigingen zullen niet alleen een efficiëntiewinst opleveren, maar ook meer duidelijkheid en uniformiteit brengen. Zo worden bijvoorbeeld de termijnen voor alle beroepen gelijkgeschakeld. Ook zullen enkele bestaande lacunes worden weggewerkt.

Ook wordt het recht op tegenspraak verscherpt en dit onder meer door een wijziging van de regels in verband met het horen van leden van de betrokken overheden (zoniet zouden de ambtenaren van de FOD Binnenlandse Zaken niet kunnen gehoord worden door het Beroepsorgaan), door de regels in verband met het overzenden van stukken en door een explicitering van de uitzonderingen op het inzagerecht.

Deze laatste wijziging betekent ook een verbetering op het vlak van de rechten van verdediging. Het Beroepsorgaan heeft immers vastgesteld dat de voorziene uitzonderingsgronden steeds vaker worden ingeroepen, terwijl dit nauwelijks gemotiveerd wordt. Dit wordt met het ontwerp verholpen. Daarenboven wordt de betrokken overheid verplicht om in algemene bewoordingen kenbaar te maken wat de aard is van de afgeschermde informatie. Het Beroepsorgaan zal er uiteraard op toezien dat de overheid hier niet vervalt in betekenisloze standaardformules. Het blijft uiteindelijk het Beroepsorgaan dat beslist welke gegevens ter inzage worden gegeven en welke niet. Wat het recht van verdediging betreft, wordt het voor de eiser soms ook mogelijk gemaakt om zich te laten vertegenwoordigen door zijn advocaat. Momenteel kan hij zich alleen laten bijstaan.

Een aantal bedenkingen met betrekking tot de voorgestelde regeling in verband met het 'onderzoek naar de veiligheidsvoorwaarden'

De artikelen 66 e.v. van het Wetsontwerp tot regeling van de private veiligheid regelen de administratieve procedure voor het zogenaamde onderzoek naar de veiligheidsvoorwaarden.

Het Beroepsorgaan stelt vast dat er op heel wat (en steeds meer) domeinen van het maatschappelijke leven veiligheidsscreenings worden vereist waarvan de finaliteit grotendeels gelijklopend is maar waarvan de procedure op vele vlakken enorm verschilt: er zijn veiligheidsonderzoeken, veiligheidsverificaties, screenings van kandidaat-politieagenten, onderzoek naar kandidaat-Belgen, screenings van vreemdelingen … waarbij steeds andere regels gelden in verband met welke informatie mag ingewonnen worden, bij welke overheden, via welke methoden, binnen welke termijnen, na al dan niet te zijn gehoord …

Ook het onderzoek naar de veiligheidsvoorwaarden hoort thuis in dit rijtje. Vanuit zijn ervaring met vele andere veiligheidsscreenings wil het Beroepsorgaan over de voorgestelde regeling volgende bedenkingen formuleren:

- Artikel 67 van het ontwerp houdt in dat op basis van harde politionele en gerechtelijke gegevens zal besloten worden of er een onderzoek wordt gevoerd en, met andere woorden, of gegevens zullen worden ingewonnen bij de inlichtingendiensten. Dit betekent dat het mogelijk is dat er géén onderzoek wordt gevoerd (en de betrokkene dus zijn vergunning krijgt) terwijl de inlichtingendiensten mogelijk wel over relevante informatie beschikken (bijvoorbeeld contacten in extremistische milieus die niet gekend zijn in politiedatabanken). Het Beroepsorgaan acht het aangewezen om – net zoals voor veiligheidsverificaties – onmiddellijk alle relevante diensten te bevragen zodat de betrokken ambtenaar op basis van een volledig dossier een evaluatie kan verrichten.
- Daarenboven acht het Beroepsorgaan het aangewezen te onderzoeken in welke mate tot een gelijkschakeling kan gekomen worden met de screenings van kandidaat-politieagenten of van veiligheidsverificaties, zeker wat betreft de aard van de gegevens die kunnen ingewonnen worden.
- Het Beroepsorgaan acht het aangewezen dat de artikelen 68 en 71 zouden worden gepreciseerd omdat niet duidelijk is wie wat moet of mag doen en wie de uiteindelijke evaluatie verricht. Zo wordt in artikel 68 bijvoorbeeld wel melding gemaakt van de Veiligheid van de Staat, maar komen de elementen waar deze dienst over beschikt niet terug in de opsomming van artikel 71.
- Het Beroepsorgaan merkt op dat er geen termijnen zijn bepaald waarbinnen de diverse diensten en de bevoegde minister moeten beslissen. Het Beroepsorgaan wijst erop dat in de procedures die het actueel behandelt, het stilzitten van de overheid aanleiding kan geven tot een beroep.
- De weigering (of intrekking) van een vergunning voor bewakingsondernemingen en interne bewakingsdiensten kan ook gebaseerd zijn op informatie afkomstig van de inlichtingendiensten, meer bepaald van de Veiligheid van de Staat (artikel 18 van het ontwerp). Ook dit advies van de Veiligheid van de Staat kan gevoelige en zelfs geclassificeerde informatie bevatten. Aangezien het ontwerp in deze niets specifiek bepaalt, zal een eventueel beroep nog steeds voor de Raad van State behandeld worden. Het Beroepsorgaan stelt zich de vraag of dit effectief de bedoeling is. Daarenboven kan de vraag gesteld worden waarom in deze niet het advies van de Algemene Dienst inlichting en veiligheid wordt ingewonnen.
- De voorgestelde regeling laat, net zoals momenteel bij de veiligheidsverificaties die voorafgaan aan de afgifte van een veiligheidsattest of –advies, alleen toe bestaande informatie op te vragen bij de verschillende diensten; er mag geen bijkomend inlich-

tingenwerk verricht worden. Die informatie kan echter gedateerd of vaag zijn. Zeker in de meest gevoelige dossiers ervaart het Beroepsorgaan regelmatig de nood tot meer accurate en actuele informatie, en dit zowel in het belang van de betrokkene als in het belang van de veiligheid. De mogelijkheid om bepaalde diensten bijkomende informatie te laten inwinnen, moet echter het voorwerp uitmaken van een duidelijke wettelijke regeling. Momenteel kan dit alleen in het kader van een veiligheidsonderzoek voorafgaand aan de afgifte van een veiligheidsmachtiging.
- Bij de kennisgeving van de beslissing (artikel 74 ontwerp) dient ook rekening te worden gehouden met elementen die voortkomen uit een lopend opsporings- of gerechtelijk onderzoek. Deze uitzonderingsgrond werd recent terecht toegevoegd in de Classificatiewet en in de Wet op het Beroepsorgaan.
- Het ontwerp eist periodiek een nieuw onderzoek (elke drie jaar) en laat blijkbaar een permanente tussentijdse evaluatie toe (artikelen 89 en 90). Het Beroepsorgaan is van oordeel dat dit systeem zou moeten uitgebreid worden tot alle veiligheidsverificaties.

Memorie van Toelichting

Tot slot wenst het Beroepsorgaan nog enkele bedenkingen te formuleren bij een aantal passages uit de Memorie van Toelichting die betrekking hebben op het onderzoek naar de veiligheidsvoorwaarden en de nieuwe bevoegdheid voor het Beroepsorgaan:
- Onder de artikelsgewijze bespreking van de artikelen 66-69 staat de volgende passage waarvan de draagwijdte voor het Beroepsorgaan niet duidelijk is: '*Om deze redenen werd er in 1998, toen de Wet betreffende de veiligheidsmachtigingen tot stand kwam, geopteerd om de veiligheidsonderzoeken aangaande actoren in de private veiligheid te laten uitvoeren door de FOD Binnenlandse Zaken en dit in het kader van de private veiligheidswet.*'
- Onder de artikelsgewijze bespreking van de artikelen 74-75 worden de wijzigingen als noodzakelijk voorgesteld omdat de betrokkene zowel op het niveau van de administratie als voor de Raad van State onbeperkte toegang moet krijgen tot alle (en dus ook gevoelige) informatie. Het Beroepsorgaan wil evenwel wijzen op de reeds bestaande wettelijke mogelijkheden om bepaalde informatie af te schermen (bijvoorbeeld de Wet op de openbaarheid van bestuur en de Wet houdende de motivering van bestuurshandelingen) en op de rechtspraak van de Raad van State die soms aanvaardt om bepaalde informatie (zakengeheim, geclassificeerde informatie) niet aan tegenspraak te onderwerpen. Daar tegenover staat natuurlijk dat het Beroepsorgaan in deze over een klare en volledige wettelijk basis beschikt. Het Beroepsorgaan wijst er evenwel op dat bij de beoordeling van kandidaat-agenten dezelfde motiverings- en inzageproblematiek speelt.
- Onder de artikelsgewijze bespreking van de artikelen 74-75 wordt ten onrechte gesteld dat het Beroepsorgaan reeds over een bepaalde expertise beschikt inzake private veiligheid. De expertise situeert zich eerder op het vlak van de veiligheid in het algemeen.
- Onder diezelfde artikelen wordt de '*noodzakelijke snelheid van beslissingen bij veiligheidsbeoordelingen*' als element aangehaald. Het Beroepsorgaan wijst erop dat dit effect kan verloren gaan indien een verzoeker zich niet alleen tot het Beroepsorgaan moet wenden voor het onderzoek naar zijn veiligheidsvoorwaarden, maar ook tot de Raad van State voor de beoordeling van de andere criteria.

BIJLAGE E.
ADVIES VAN HET VAST COMITÉ I BIJ HET VOORONTWERP VAN WET TOT WIJZIGING VAN DE WET VAN 30 NOVEMBER 1998 HOUDENDE REGELING VAN DE INLICHTINGEN- EN VEILIGHEIDSDIENST (W.I&V)

Bij brief van 22 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. Er werd verzocht om het advies uiterlijk op 4 maart 2016 over te zenden. Gelet op het uiterst korte tijdsbestek enerzijds en op de uitgebreidheid en complexiteit van de voorgestelde wijzigingen – waaraan lange tijd is gewerkt door de betrokken administraties – 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 opteerde er dan ook voor om een aantal krachtlijnen te formuleren en die, waar nuttig, te stofferen met concrete voorbeelden. Het Comité staat uiteraard ter beschikking van de bevoegde overheden om nadere toelichting of commentaren te verschaffen bij voorliggend advies.

Ook omwille van het beperkte tijdsbestek heeft het Comité het advies alleen in het Nederlands opgesteld.

Het Comité wenst vooraf te benadrukken dat het voorstander is van elk voorstel dat de efficiëntie van de Belgische inlichtingendiensten kan verhogen in de mate waarin er voldoende waarborgen worden ingebouwd voor de vrijwaring van de fundamentele rechten en vrijheden. Dit geldt zeker in de huidige maatschappelijke context waarin de strijd tegen het terrorisme en het radicalisme optimaal moet kunnen gevoerd worden. Verder wijst het Comité op het feit dat de voorgestelde regeling – die een performanter optreden mogelijk moet maken – niet alleen zal gelden in de strijd tegen het terrorisme en het radicalisme, maar tevens voor alle domeinen waarop de Veiligheid van de Staat (VSSE) en de Algemene Dienst inlichting en veiligheid (ADIV) actief zijn.

In het Regeerakkoord van 10 oktober 2014 werd aangekondigd dat '*de wet betreffende de Bijzondere Inlichtingenmethoden […]word[t] geëvalueerd en desgevallend aangepast*.' In de Memorie van Toelichting bij de ontwerptekst wordt verwezen naar een '*eerste evaluatie*'. Het Comité was op de hoogte van het bestaan van een werkgroep die belast was met dergelijke evaluatie, maar het is nooit in kennis gesteld van haar resultaten. In die optiek was het voor het Comité moeilijk te beoordelen op welk vlak de huidige bevoegdheden en mogelijkheden van de inlichtingendiensten ontoereikend of onwerkbaar zouden zijn en daarom een wijziging van de BIM-Wet van 4 februari 2010 of van de globale Inlichtingenwet van 30 november 1998 zouden rechtvaardigen. Buiten de concrete aanbevelingen die het Comité de afgelopen jaren zelf heeft geformuleerd (zie hieronder 1-7), heeft het in zijn rol van 'toezichthouder' noch van 'controle-instantie op de BIM-methoden' ervaren dat de actuele wettelijke regeling '*soms een snel en doeltreffend gebruik van de methoden in de weg [zou] staan*' (Memorie van Toelichting) waardoor bepaalde van de in het ontwerp voorgestelde wijzigingen zouden genoodzaakt zijn.

Wat betreft de voorstellen die het Comité de afgelopen jaren zelf formuleerde in het kader van de BIM-werking, kan verwezen worden naar onderstaande voorbeelden. Het ontwerp houdt grotendeels rekening met deze aanbevelingen.

1. De identificatie van de abonnee of de gebruiker van een elektronische communicatiedienst of van het gebruikte elektronische communicatiemiddel zou, gelet op de beperkte impact op de privacy, als een gewone methode kunnen aanzien worden. Deze aanbeveling werd recent gerealiseerd bij Wet van 5 februari 2016 tot wijziging van het strafrecht en de strafvordering en houdende diverse bepalingen inzake justitie (*BS* 19 februari 2016).

2. De wet zou een duidelijk, werkbaar en uniform kader moeten instellen voor de inzet van bijzondere methoden in geval van hoogdringendheid (Vast Comité I, *Activiteitenverslag 2011*, 78). Het ontwerp komt hieraan tegemoet. Wel stelt het Comité vast dat de voorziene regeling wat betreft de uitzonderlijke methoden bijzonder veel ruimte laat aan de diensten. Het Comité merkt ook op dat het had aanbevolen uitdrukkelijk in een duidelijke sanctie te voorzien indien de hoogdringendheid nadien niet kon worden aangetoond. Het Comité herhaalt dan ook deze aanbeveling.

3. Artikel 13/1 § 2, derde lid W.I&V verleent de (voltallige) BIM-Commissie de mogelijkheid om aan inlichtingenagenten de uitdrukkelijke toelating te verlenen om strafbare feiten te begaan die strikt noodzakelijk zijn voor de efficiëntie van de uitvoering van een BIM-methode of ter verzekering van hun eigen veiligheid of die van andere personen. De wet heeft hierbij echter niet voorzien in een procedure van hoogdringendheid. Het Comité was van oordeel dat wanneer de bijzondere methode zelf bij hoogdringendheid kan worden ingezet, ook in de mogelijkheid moet worden voorzien dat de accessoire bevoegdheid uit artikel 13/1 § 2, derde lid, W.I&V bij hoogdringendheid kan worden uitgeoefend. Het ontwerp komt hieraan tegemoet, maar gaat nog een stap verder door het plegen van misdrijven toe te laten zonder voorafgaande goedkeuring (zie verder 28).

4. Het Comité heeft gewezen op het feit dat door het arrest van het Grondwettelijk Hof van 22 september 2011 de notificatieverplichting is vervallen waardoor in een nieuwe wettelijke regeling diende te worden voorzien (Vast Comité I, *Activiteitenverslag 2011*, 52). Het ontwerp gaat niet in op deze problematiek.

5. Artikel 18/17 § 7 W.I&V voorziet dat gegevens die verzameld zijn via een tapmaatregel binnen een jaar en twee maanden moeten vernietigd worden. Het Comité had destijds aanbevolen deze beperking te schrappen onder meer omdat inlichtingendiensten op lange termijn werken en een verplichting om relevante inlichtingen te wissen omdat ze via een uitzonderlijke methode werden verzameld, hiertegen ingaat. Het voorstel komt hieraan tegemoet. Wel wijst het Comité op het verbod om gegevens die niet nuttig zijn vanuit de inlichtingenfinaliteit in de documentatie op te nemen. Dergelijke gegevens moeten – los van de wijze waarop ze werden ingewonnen – in alle gevallen zo snel mogelijk vernietigd worden.

6. De actuele regeling maakt dat uitzonderlijke methoden niet kunnen ingezet worden in geval van extremisme en inmenging. Het Comité heeft voorgesteld af te stappen van dit verbod. Het ontwerp volgt deze aanbeveling.

7. Het Comité had in 2013 aanbevolen dat de wetgever een debat zou voeren over de noodzaak om bepaalde BIM-methoden mogelijk te maken in het buitenland. Het ontwerp doet in dit verband een aantal voorstellen (zie verder 23 en 24).

Het Comité stelt vast dat het voorontwerp op een aantal vlakken ingrijpende wijzigingen aan de Inlichtingenwet van 30 november 1998 in het vooruitzicht stelt die verder reiken dan de bepalingen die in 2010 werden toegevoegd middels de BIM-Wet. Het Comité verwijst slechts naar volgende voorbeelden:

8. De wettelijke opdracht van de ADIV en zijn collectemogelijkheden in het buitenland worden zeer sterk uitgebreid (zie verder 18, 24 en 31).

9. De mogelijkheid wordt gecreëerd om zowel binnen de VSSE als de ADIV een zogenaamd 'interventieteam' op te richten. De eigenlijke doelstelling en noodzaak hiervoor werden nooit aangekaart of aangetoond bij het Comité. De leden van dit interventieteam krijgen taken en bevoegdheden van bestuurlijke politie, net nu de beschermingsopdracht als taak van bestuurlijke politie, op verzoek van de VSSE, bij haar zal worden weggehaald.

10. De bestaande gewone methoden worden aangepast in die zin dat de diensten makkelijker informatie kunnen bekomen van – vooral – particulieren (zie verder).

11. Er wordt een bepaling ingevoerd met betrekking tot de archivering van documenten van de inlichtingendiensten. In dat kader had het Comité zich destijds voorstander getoond van een systeem waarbij classificaties na een bepaalde termijn – bijvoorbeeld 30 jaar voor documenten die 'geheim' zijn geclassificeerd en 50 jaar voor 'zeer geheime' documenten – van rechtswege vervallen, tenzij zij expliciet worden hernieuwd.

Het Comité wil wijzen op aan een aantal andere wettelijke bepalingen, die in het ontwerp onbesproken blijven, terwijl ze ook voor verbetering vatbaar zijn. Het Comité verwijst in dit kader naar onderstaande voorbeelden. Sommige ervan maakten reeds het voorwerp uit van een aanbeveling van het Comité.

12. Het Vast Comité I heeft talloze malen aanbevolen dat de artikelen 19 en 20 W.I&V nader zouden worden uitgewerkt door de uitvoerende maar ook door de wetgevende macht. Deze cruciale bepalingen regelen onder meer de informatieoverdracht (inbegrepen persoonsgegevens) naar andere (buitenlandse) diensten en de medewerking/technische bijstand die beide Belgische diensten kunnen verlenen aan bijvoorbeeld de gerechtelijke autoriteiten of aan buitenlandse homologen. Gelet op de groeiende samenwerking tussen alle actoren van het veiligheidsdomein én gelet op de voorgenomen uitbreiding van de mogelijkheden van de militaire inlichtingendienst in het buitenland, beveelt het Comité nogmaals aan dat de twee wetsartikelen zouden verduidelijkt worden zodat er geen twijfel bestaat over eenieders rol en mogelijkheden.

13. Artikel 19/1 W.I&V voorziet in een bijzondere aangifteverplichting indien een misdrijf aan het licht komt via een bijzondere methode; komt ditzelfde misdrijf aan het licht via een gewone methode, dan geldt artikel 29 Sv. Het moment en de wijze waarop

de vermeende misdrijven moeten gemeld worden, verschilt fundamenteel. Verder is niet duidelijk wat er dient te gebeuren wanneer een misdrijf aan het licht komt via een gewone methode en naderhand bijkomende elementen worden verzameld via een bijzondere methode. Het Vast Comité I beveelt aan deze regeling te herbekijken.

14. Destijds had het Comité aangedrongen op een meer uitgewerkte regeling voor de informantenwerking. De toenmalige Regering heeft er echter voor geopteerd om de nadere regeling over te laten aan het Ministerieel Comité voor inlichting en veiligheid, nu de Nationale Veiligheidsraad. Dit is nog steeds niet gebeurd. Hetzelfde geldt voor vele andere belangrijke aspecten van de Inlichtingenwet. Het Comité is in kennis gesteld van het feit dat de Nationale Veiligheidsraad instructies heeft gegeven om waar nodig richtlijnen op te stellen. Toch blijft het Comité van mening dat het op sommige vlakken aan de wetgever toekomt de krijtlijnen uit te zetten. Wat betreft de informantenwerking, stelt het Comité meer specifiek een expliciet verbod voor om via de inzet van informanten gegevens te verzamelen en daarbij bepalingen die een geheimhoudingsverplichting in het leven roepen, te omzeilen of de garanties van de BIM-Wet ter zijde te schuiven.

15. De regeling inzake de bevoegdheid van het Comité als jurisdictioneel orgaan dient in die zin te worden verduidelijkt dat het Comité zich ook kan vatten wanneer een dienst een methode inzet die volgens de wet als een bijzondere methode moet beschouwd worden, zonder hiervoor een toelating te hebben bekomen en waarvoor dus geen formele beslissing of machtiging voorligt. Het Comité wijst er op dat de inzet van maatregelen die als een bijzondere methode moeten worden beschouwd, maar waarvoor geen toelating werd verleend, een misdrijf kan uitmaken met alle gevolgen vandien.

16. Het inzagerecht dat aan personen is toegekend die het Comité vatten in zijn hoedanigheid van jurisdictioneel orgaan, is dermate ruim dat het lopende inlichtingenoperaties in het gedrang kan brengen. Het Comité beveelt aan deze regeling aan te passen, ook al heeft deze situatie zich actueel nog maar éénmaal voorgedaan.

Het Comité is van oordeel dat de evaluatie van de actuele regeling grotendeels vanuit de efficiëntie van de inlichtingendiensten is gebeurd. Dit heeft zich vertaald in een ontwerp dat vooral resulteert in méér (soms nuttige en noodzakelijke) bevoegdheden en wettelijke mogelijkheden voor de twee inlichtingendiensten, waarbij er niet steeds voldoende aandacht is voor de externe controle en de noodzakelijke *checks and balances*. Meer nog, deze externe controle wordt soms zelfs teruggeschroefd.

Wat betreft de bijkomende bevoegdheden, taken en (collecte)mogelijkheden verwijst het Comité bij wijze van voorbeeld naar volgende voorstellen:

17. Er wordt voorgesteld een interventieteam te creëren (zie hoger punt 9.).

18. De taakomschrijving van de ADIV wordt sterk verruimd. De juiste draagwijdte van de diverse ingrepen in artikel 11 W.I&V vereist een meer grondige studie. Het Comité heeft de indruk dat de actieradius van de ADIV wordt uitgebreid tot buiten het 'militaire' domein (bijvoorbeeld inlichtingen inwinnen inzake het binnen- en buitenlands veiligheidsbeleid). Het Comité is zich terdege bewust van de groeiende internationalisering van de veiligheidsproblemen en het ontbreken van een burgerlijke buitenlandse

inlichtingendienst maar wijst er op dat dit een fundamentele heroriëntatie zou betekenen tegenover de actuele regeling en daarom verdere reflectie vereist. Hierbij moet ook bekeken worden of de ADIV over de middelen beschikt om die nieuwe taak waar te nemen en of het toezicht hierop op een adequate manier kan gebeuren.

19. Het voorgestelde artikel 13/2 verleent inlichtingenagenten de mogelijkheid een fictieve naam, identiteit en hoedanigheid te gebruiken, los van de inzet van een andere methode. Deze – zeer summiere – regeling biedt bijvoorbeeld de mogelijkheid te infiltreren in groeperingen. Tot op heden hielden de diensten voor dat zij deze techniek niet wensten te gebruiken. Indien dit nu wel het geval is, dient dit expliciet te worden vermeld en moet de maatregel als een bijzondere methode worden beschouwd. Tevens dient de nodige aandacht te worden besteed aan de (rechts)bescherming van het betrokken personeel.

20. Hierbij aansluitend stelt het Comité zich de vraag of de mogelijkheid zoals bepaald in het nieuwe artikel 13/4, ook moet toelaten om tot burgerinfiltratie over te gaan. Uit de Memorie van Toelichting blijkt niet dat dit het geval is. De tekst van het ontwerpartikel sluit deze mogelijkheid echter niet uit. Mocht dit alsnog de bedoeling zijn, is een diepgaande reflectie over de opportuniteit en de (wettelijke) omkadering aangewezen.

21. Artikel 14 verduidelijkt dat het beroepsgeheim of een andere geheimhoudingsplicht geen obstakel vormt voor openbare besturen (zoals een OCMW) om op verzoek informatie mee te delen aan de inlichtingendiensten. Het Comité is voorstander van deze verduidelijking, maar stelt wel vast dat de mogelijkheid voor die openbare besturen om 'akkoorden' af te sluiten of 'regels' op te stellen, vervalt. Indien het de bedoeling is van het voorstel dat overheden niet langer over een appreciatiebevoegdheid beschikken, dient hierover een grondige reflectie plaats te vinden. Er moet immers rekening mee worden gehouden dat sommige overheidsdiensten over zeer gevoelige persoonsgegevens beschikken (bijvoorbeeld medische gegevens) die voor een welbepaalde finaliteit werden verzameld.

22. De wijziging van artikel 16 houdt vooreerst in dat privé-personen of private organisaties te allen tijde persoonsgegevens mogen meedelen aan de inlichtingendiensten, ook al beschikken deze privé-actoren over deze gegevens in functie van een welbepaalde finaliteit (wijziging van het 'doelbindingsprincipe'). Ten tweede lijkt het de bedoeling dat een eventuele discretie- of geheimhoudingsverplichting die zou rusten op de houder van bepaalde gegevens, niet geldt in zijn relatie met een inlichtingendienst. Vooral wat dit tweede aspect betreft, gaat deze regeling zeer ver en vereist ze een zorgvuldige afweging van de diverse in het geding zijnde belangen (bijvoorbeeld het medisch geheim van een arts, het beroepsgeheim van een advocaat of het bronnengeheim van een journalist). Het wijst er tevens op dat dergelijke gegevens via artikel 19 W.I&V ook aan het gerecht zouden kunnen worden overgezonden.

23. De inzet van bijzondere methoden buiten het Belgische grondgebied wordt voor beide diensten uitgebreid. Voor de VSSE wordt een beperking ingebouwd: de methoden moeten 'vanaf' het grondgebied worden ingezet zodat blijkbaar voornamelijk de collectemogelijkheid voor digitale informatie/communicatie wordt verbreed. Maar betekent deze regeling bijvoorbeeld dat de VSSE vanuit België buitenlandse communicaties kan onderscheppen? Dit dient te worden verduidelijkt.

24. Wat betreft de inzet van bijzondere methoden buiten België geldt geen beperking voor de ADIV. Daar waar het Comité destijds had aanbevolen dat er moest bestudeerd worden of *bepaalde* BIM-methoden ook in het buitenland konden worden ingezet, bepaalt het huidige ontwerp dat deze dienst *alle* specifieke én uitzonderlijke methoden kan inzetten in het buitenland. In principe vallen dergelijke methoden onder de administratieve controle van de BIM-Commissie en de jurisdictionele controle van het Vast Comité I (al is het zeer de vraag hoe dit in de praktijk zal moeten verlopen). Maar voor de interceptie van bepaalde communicatie, het binnendringen in informaticasystemen en het maken van beelden, geldt een specifieke (minder verregaande) controleregeling (zie verder 31). Tot slot wijst het Comité op het feit dat de uitbreiding van de mogelijkheden voor de inlichtingendiensten om bijzondere methoden in te zetten in het buitenland, vragen oproept naar de problematiek van de soevereiniteit van andere Staten en de strafbaarstelling van in het buitenland gevestigde organisaties wiens medewerking wordt gevorderd. Indien dergelijke in het buitenland ingewonnen inlichtingen in een strafdossier belanden, moet bekeken worden hoe dit zich verhoudt tot rechtshulpverdragen en de verplichting om te werken via rogatoire commissies.

25. Het voorstel voert een nieuwe specifieke methode in: de vordering van vervoers- en reisgegevens bij private actoren. Het Comité begrijpt het nut van deze regeling voor de werking van inlichtingendiensten. Gelet op de privacygevoeligheid van de te bekomen gegevens, is het Comité van oordeel dat het inwinnen ervan inderdaad als een specifieke methode moet gecatalogeerd worden. Het Comité benadrukt dat de verkrijging van deze gegevens *steeds* als een specifieke methode dient te worden beschouwd, ook al zou men deze in de toekomst via een publieke overheid – en dus via de gewone methode *ex* artikel 14 W.I&V – kunnen bekomen (zie Wetsontwerp inzake PNR).

26. Hierbij aansluitend is het Comité in het algemeen van oordeel dat het niveau van 'bescherming' dat geboden wordt in de BIM-Wet, moet verbonden zijn met 'de aard van de gegevens' (minder of meer privacygevoelig) en niet zozeer met 'de manier waarop ze worden ingewonnen' (via eigen collectemogelijkheden, via een vordering, via rechtstreekse toegang tot een bestand …). Zoniet zou men tot de situatie komen dat de collecte van eenzelfde privacygevoelig gegeven nu eens als een gewone methode en dan weer als een specifieke methode moet beschouwd worden en de diensten aan 'methode-*shopping*' kunnen doen. Net om die reden beveelt het Comité ook aan dat artikel 18/15 W.I&V zou aangepast worden in die zin dat het inwinnen van bepaalde financiële gegevens een specifieke methode is, die onder meer kan gerealiseerd worden via een vordering aan bankinstellingen.

Wat betreft de problematiek van de *checks and balances* haalt het Comité volgende voorbeelden aan:

27. Het ontwerp brengt op sommige plaatsen wijzigingen aan waardoor specifieke methoden gewone methoden worden en waarbij uitzonderlijke methoden verworden tot specifieke methoden. Het gevolg is uiteraard dat de externe controle minder verregaand reikt. Het Comité geeft volgende voorbeelden:
    - Het openen van gesloten voorwerpen blijft slechts een specifieke methode in de mate waarin deze voorwerpen 'vergrendeld' zijn.

- Mobiele camera's worden, net als fototoestellen, niet meer beschouwd als een technisch middel zodat de inzet ervan de aard van de observatie niet verandert. Dit betekent bijvoorbeeld dat het filmen van een *target* geen specifieke methode is, ongeacht de duur en de frequentie van de observaties. Het Comité heeft hiertegen geen principiële bezwaren, maar wijst er op dat langdurige of frequente observaties van eenzelfde target of groepering zeer ingrijpend kunnen zijn en daarom mogelijkerwijze als een bijzondere methode dienen te worden beschouwd.
- De observatie van hetgeen zich afspeelt in aanhorigheden kan een specifieke methode zijn in plaats van een uitzonderlijke. Door in het ontwerp een nieuwe categorie van plaatsen in te voeren (met name '*niet voor het publiek toegankelijke plaats die (niet) aan het zicht onttrokken is*') worden aanhorigheden van woningen (zoals de tuin) minder beschermd in functie van de afsluiting die de bewoner plaatste. Tot op heden genieten aanhorigheden dezelfde bescherming als de woning. De invoering van dergelijke nieuwe categorie of een nieuwe juridische notie kan tot onduidelijkheden en interpretatieproblemen leiden. Het Comité heeft geen weet van voorbeelden waarin deze nieuwe regeling kan tegemoetkomen aan een evidente operationele nood. Immers, hetgeen zich afspeelt binnen aanhorigheden kan nu reeds gecollecteerd worden, weze het via een uitzonderlijke methode. Tot slot wil het Comité wijzen op het arrest van het Grondwettelijk Hof (nr. 178/2015) waarbij art. 464/27 Sv. i.v.m. het strafuitvoeringsonderzoek werd vernietigd. De motieven van dit arrest zijn uitermate relevant in het licht van de hier voorgestelde wijziging.
- Het ontwerp voorziet in een specifieke regeling voor personen die erkend zijn als beroepsjournalist maar die volgens de inlichtingendiensten die erkenning niet verdienen. Het Comité stelt zich vragen bij de wettelijkheid en het nut van dergelijke regeling. Deze regeling zal overigens een bijkomende werklast inhouden voor de diensten die moeten aantonen dat een persoon geen beroepsjournalist is.
- Het ontwerp stelt voor om bij de evaluatie van de subsidiariteit rekening te houden met de risico's die de uitvoering van de inlichtingsopdracht met zich meebrengt voor de veiligheid van de agenten van de diensten en van derden. Dat rekening wordt gehouden met risico's voor de fysieke veiligheid is niet nieuw; dit is reeds bepaald bij artikel 18/9 § 3 W.I&V. Maar door deze bepaling naar artikel 2 over te brengen, kan de betrokken dienst voortaan beslissen een uitzonderlijke methode in te zetten (en dus gegevens in te winnen die zeer privacygevoelig zijn), omdat de gewone of specifieke methoden (die betrekking hebben op minder privacygevoelige gegevens) te veel gevaar inhouden. Indien dit de bedoeling is van het voorstel, dient er nauw op te worden toegezien dat met deze bepaling omzichtig wordt omgesprongen.

28. Het Comité stelt zich ernstige vragen bij de regeling waarbij een inlichtingenagent een misdrijf begaat dat nadien – en bijvoorbeeld buiten eventuele schadelijders om – zou kunnen 'gedekt' worden door de BIM-Commissie. Het Comité is van oordeel dat deze regeling fundamenteel moet worden herbekeken. Het is van oordeel dat in de gevallen die het ontwerp wil regelen, kan teruggegrepen worden naar bestaande rechtsfiguren (bijvoorbeeld noodtoestand of wettige verdediging).

29. Het Comité kan zich allerminst vinden in de voorgestelde wijziging van artikel 43/5 § 4 W.I&V. De huidige regeling, die destijds op voorstel van de Senaat werd ingevoerd, bepaalt dat inlichtingenagenten *alle* informatie moeten meedelen aan het Comité wanneer deze de wettelijkheid van een bijzondere methode controleert. Deze regeling

geldt ook voor informatie of documenten van de inlichtingendiensten die onder het geheim van het onderzoek vallen. Wel moet de voorzitter van het Comité in dat geval overleg plegen met de bevoegde magistraat. Op die wijze kan hij rekening houden met diens bekommernissen. Dezelfde regeling geldt overigens voor het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen. De voorgestelde wijziging zou tot gevolg kunnen hebben dat het Comité als jurisdictioneel orgaan moet oordelen over de wettelijkheid van een methode, *zonder* dat het over alle informatie die werd ingewonnen of aangemaakt door de inlichtingendiensten, beschikt. Het Comité benadrukt dat het geen weet heeft van gevallen waarin de actuele regeling tot problemen aanleiding heeft gegeven voor het geheim van het onderzoek. Het Comité wijst er overigens op dat dergelijke informatie *nooit* wordt gedeeld met derden.

30. Zoals reeds vermeld (zie 4), laat het ontwerp na een regeling te voorzien voor de notificatie van *targets* van geheime methoden.

31. De regeling die de ADIV toelaat buitenlandse communicaties te intercepteren, is tot stand gekomen in een tijd waarin voornamelijk radiosignalen werden onderschept. Sindsdien is er op technologisch vlak dermate veel veranderd dat het Comité aan de wetgever reeds had aanbevolen de regeling te herzien. De onthullingen van Edward Snowden en de intenties van de ADIV om aan *cable-tapping* te doen, maken die herziening alleen maar dringender. Het Comité stelt vast dat het bevoegdheidsdomein van de ADIV sterk wordt uitgebreid (zie 8) én dat de dienst – terecht – meer collectemogelijkheden krijgt. Evenwel betekent deze dubbele vaststelling voor het Comité dat duidelijk moet gedefinieerd worden wat wel en wat niet kan én dient een reële toezichtmogelijkheid te worden gecreëerd. Elementen die hierbij alleszins moeten bestudeerd worden, zijn de mate waarin intercepties al dan niet gericht moeten gebeuren en op wiens verzoek dit kan, de mate van precisering van het jaarlijkse Afluisterplan (bijvoorbeeld selectoren in plaats van landen of generieke bewoordingen), de mogelijkheid om aan data-*mining* te doen in bulkinformatie en de vraag of buitenlandse SIGINT-operaties steeds moeten kaderen binnen een gewapend conflict of een 'internationaal mandaat'. Het Comité is van oordeel dat de voorgestelde regeling onvoldoende ingaat op die aspecten. Het Comité herhaalt dat het er in de feiten over eens is dat de feitelijke capaciteiten van de ADIV op SIGINT-vlak veel te beperkt zijn, maar dat het huidige ontwerp een algemene interceptie-bevoegdheid installeert over alle (uitgebreide) bevoegdheden van de dienst, met de verplichte medewerking van de operatoren. Het gevolg is dat de ADIV kan overgaan tot *mass surveillance* van alle communicatiemiddelen vanuit of naar het buitenland. Daartegenover staat een te summiere wettelijke regeling met beperkte toezichtsmogelijkheden die naar het oordeel van het Comité niet voldoen aan de eisen van bijvoorbeeld het EVRM. Over al deze kwesties is een grondig en geïnformeerd parlementair debat noodzakelijk.

BESLUIT

In het toegemeten tijdsbestek heeft het Comité zich moeten beperken tot de wijzigingen die een kritische aandacht verdienden. In algemene zin beveelt het Comité aan dat de wijzigingsvoorstellen die hiervoor werden aangehaald, beter geduid worden naar finaliteit en in bepaalde gevallen meer in detail worden geregeld in het ontwerp. Ook dient grondiger gereflecteerd te worden over sommige fundamentele opties. Daarnaast beveelt het Comité aan

dat het toezicht en de controle op een adequaat niveau gebracht worden. Deze bedenkingen moeten gekaderd worden in de bekommernis om te voldoen aan de fundamentele eisen zoals die voortvloeien uit nationale en internationaal rechtsnormen. Tot slot wil het Comité benadrukken dat het uitgebreide ontwerp tal van positieve elementen bevat en dit zowel op legistiek vlak als vanuit het oogpunt van de operationele noden van beide inlichtingendiensten.

BIJLAGE F.
GEZAMENLIJK ADVIES NR. 01/2016 VAN 20 JUNI 2016 BETREFFENDE DE VOORAFGAANDELIJKE AANGIFTE VAN DE GEMEENSCHAPPELIJKE DATABANK '*FOREIGN TERRORIST FIGHTERS*'

Het Controleorgaan op de politionele informatie (hierna COC) en het Vast Comité van toezicht op de inlichtingen– en veiligheidsdiensten (hierna Comité I);

Gelet op de wet van 5 augustus 1992 op het politieambt (hierna WPA), inzonderheid artikel 44/11/3*bis*, § 3;

Gelet op het verzoek om advies van de Minister van Binnenlandse Zaken en de Minister van Justitie door het COC ontvangen op 30/5/2016 en door het Comité I op 14/06/2016;

Brengen op 20 juni 2016 het volgend advies uit:

A. VOORWERP VAN DE AANVRAAG EN PROCEDURELE ASPECTEN

1. Op 30 mei jl. hebben de ministers van Justitie en Binnenlandse Zaken een vraag tot advies overgemaakt aan het COC en het Comité I overeenkomstig artikel 44/11/3*bis*, § 3 WPA aangaande de voorafgaande aangifte van de gemeenschappelijke databank 'Foreign Terrorist Fighters' (hierna FTF-databank). Het COC en Comité I dienen vervolgens overeenkomstig voormeld artikel binnen de dertig dagen een gezamenlijk advies uit te brengen.

2. Artikel 44/11/3*bis*, § 4 WPA[280] schrijft evenwel voor dat voor elke gemeenschappelijke gegevensbank een Koninklijk besluit de regels bepaalt op het gebied van de verantwoordelijkheden op het vlak van de bescherming van de persoonlijke levenssfeer van de organen, diensten, overheden en organismen die gegevens verwerken, de regels op het gebied van de veiligheid van de verwerkingen, de regels van het gebruik, de bewaring en de uitwissing van de gegevens. Een dergelijk Koninklijk besluit dient aan de Commissie voor de bescherming van de persoonlijke levenssfeer (hierna CBPL) te zijn voorgelegd voor advies.

3. Op datum van vandaag is er nog geen Koninklijk besluit dat de regels bepaalt voor de FTF-databank. Overeenkomstig het voormelde schrijven van de ministers van Binnenlandse Zaken en Justitie wordt dit voorgelegd aan de CBPL. De mogelijkheid bestaat derhalve dat de CBPL (fundamentele) opmerkingen heeft bij het ontwerp van Koninklijk besluit, en dat dit ontwerp vervolgens nog (ingrijpend) kan worden veranderd. Dit heeft uiteraard een invloed op de aangifte van de FTF-databank en het aan-

280 Ingevoerd door de Wet van 14 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme.

sluitend advies door het C.O.C en Comité I. Vandaar dat het COC en het Comité I voor toekomstige aangiftes van gemeenschappelijke databanken er op aandringen om deze aangiftes pas te doen nadat het Koninklijk besluit met betrekking tot deze databank werd gepubliceerd. Dit om te vermijden dat premature aangiftes nadien nog dienen te worden gewijzigd en het COC en Comité I toe te laten een advies uit te brengen omtrent de definitieve versie en structuur van de gemeenschappelijke databank en zijn verwerkingsmodaliteiten die het voorwerp moet uitmaken van het advies.

4. Bij schrijven van 30 mei jl. vanwege de bevoegde ministers werd het ontwerp van Koninklijk besluit *betreffende de gemeenschappelijke gegevensbank Foreign Terrorist Fighters en tot uitvoering van sommige bepalingen van de afdeling 1bis 'het informatiebeheer' van hoofdstuk IV van de wet op het politieambt* (hierna het ontwerp koninklijk besluit) gevoegd, evenals een nota getiteld 'voorafgaandelijke toelichting bij de gemeenschappelijke databank Foreign Terrorist Fighters' (hierna 'de voorafgaandelijke toelichting'). Deze voorafgaandelijke toelichting volstaat evenwel niet als aangifte voor het COC en Comité I, aangezien er fundamentele informatie aangaande de databank ontbreekt.

5. Het COC en Comité I brengen hiernavolgend in dit dossier toch een voorlopig advies uit aangaande de voorafgaandelijke toelichting, omdat hierdoor nog wijzigingen mogelijk zijn aan het ontwerp van Koninklijk besluit, zie *infra* nrs. 7, 13-15, 17. Zij behouden zich evenwel het recht voor om nog een bijkomend advies te verstrekken na de publicatie van het Koninklijk besluit inzake de FTF-databank, en na mogelijke bijkomende aanvullende aangiftes voor deze databank.

B. TEN GRONDE

6. Hiernavolgend wordt een analyse gemaakt van het document 'voorafgaandelijke toelichting', rekening houdend met de daarin aangehouden indeling.

1. Finaliteit

7. Overeenkomstig de toelichting draagt de FTF-databank bij tot de analyse, de evaluatie en de opvolging van de *Foreign Terrorist Fighters* die zich in één van de situaties bevinden zoals beschreven onder punt 7 van de toelichting. Deze situaties sluiten evenwel ronselaars en propagandisten, en personen met louter binnenlandse terroristische intenties uit, hetgeen bij het C.O.C en Comité I vragen oproept. Immers, het verslag aan de Koning bij het ontwerp Koninklijk besluit stelt op pagina 2 dat '*Dankzij deze gegevensbank maakt een inlichtingenfiche van de personen die betrokken zijn bij het fenomeen van strijders die afreizen naar jihadistische gevechtszones het niet alleen mogelijk de potentiële dreiging te beoordelen die deze personen vertonen, maar voornamelijk er een opvolging van te verzekeren met het oog op het anticiperen en het verhinderen van mogelijke terroristische acties door hen*.' In de vertrouwelijke omzendbrief col 10/2015 van het college van procureurs-generaal bij de hoven van beroep betreffende de gerechtelijke aanpak inzake de *Foreign Terrorist Fighters* is sprake van een categorie 6 'steun en rekrutering'. De opname van deze bijkomende categorie zou een nog grotere operationele bruikbaarheid kunnen genereren van de FTF-databank.

8. Indien het echter de bedoeling is om inderdaad enkel en alleen de 5 categorieën te voorzien waarvan sprake in punt 7 van de toelichting, zullen het C.O.C en het Comité I er in dat geval tijdens hun controletaken over waken dat enkel deze categorieën in de FTF-databank vertegenwoordigd zijn, en dus niet de categorie 6, noch personen met louter binnenlandse terroristische en extremistische[281] intenties, zelfs indien zij opdrachten uit het buitenland zouden ontvangen of uitvoeren, noch radicaliserende vectoren in de samenleving.

2. Wettelijke en reglementaire basis

9. Hier kan worden verwezen naar de opmerkingen onder randnummer 3. In de voorafgaandelijke toelichting is er op heden geen verwijzing naar een publicatie van een Koninklijk besluit opgenomen. Een toekomstige aangifte van een gemeenschappelijke databank dient pas te gebeuren na publicatie van het Koninklijk besluit inzake deze gemeenschappelijke databank. Dit Koninklijk besluit kan derhalve in de aangifte worden opgenomen. Het is voor de controleorganen essentieel dat en de gemeenschappelijke databank en zijn juridische omkadering eenduidig vastliggen alvorens zich definitief uit te spreken over de voorgenomen gemeenschappelijke gegevensbank.

3. Consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer

10. De toelichting maakt 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. Deze persoon is nochtans van groot belang in het kader van de controletaken van het COC en Comité I, aangezien hij of zij overeenkomstig artikel 44/3, § 1/1 WPA belast is met de contacten met het COC en het Comité I. Deze persoon dient derhalve in de aangifte te worden opgenomen. Het is daarnaast ook van belang dat van bij de conceptie en uitrol van de gemeenschappelijke gegevensbank de consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer betrokken wordt en dus in een zo vroeg mogelijk stadium wordt aangeduid. De aanduiding ervan in de aangifte aan de controleorganen laat deze laatste ook toe meteen een zicht te hebben op de graad van onafhankelijkheid die betrokkene moet hebben ten aanzien van de overheden, organen, organismen, diensten, directies of de commissie bedoeld in artikel 44/11/3*ter* WPA.

5. Operationele verantwoordelijke

11. Het Coördinatieorgaan voor de Dreigingsanalyse (hierna OCAD) wordt in de toelichting vermeld als operationele verantwoordelijke. Voor het vergemakkelijken van de controletaken is het aangewezen om in de aangifte de namen op te nemen van de verantwoordelijken bij het OCAD, die door het COC en het Comité I kunnen worden gecontacteerd.

6. Beheerder

12. De federale politie wordt opgegeven als de beheerder. Ook hier kan worden opgemerkt dat in de aangifte minstens de concrete verantwoordelijke dienst bij de federale politie dient te worden vermeld, evenals enkele contactpersonen bij deze dienst.

---

281 Extremisme dat tot terrorisme kan leiden (cf. art. 44/2 § 2 WPA).

7. Personen die het voorwerp uitmaken van een registratie in de databank

13. Hier kan worden verwezen naar de opmerkingen onder de randnummers 7 en 8. Daarenboven stelt de voorafgaandelijke toelichting overeenkomstig artikel 6, 3° van het ontwerp Koninklijk besluit dat van deze personen enkel de niet-geclassificeerde inlichtingen worden verwerkt.

Dit houdt derhalve in dat de Veiligheid van de Staat, de ADIV en het OCAD in de praktijk waarschijnlijk een zeer geringe voeding zullen kunnen doen van de FTF-databank, aangezien veel informatie waarover zij beschikken geclassificeerde informatie uitmaakt. Nochtans voorziet de wet[282] in artikel 44/2, § 2 WPA in een voedingsverplichting voor de verschillende diensten. Artikel 44/11/3*ter* § 5 WPA voorziet in een uitzondering op deze voedingsverplichting voor de inlichtingen- en veiligheidsdiensten indien de leidinggevende oordeelt dat deze voeding de veiligheid van een persoon in gevaar kan brengen, of indien het gaat om vertrouwelijke informatie afkomstig van een buitenlandse dienst. Er werd geen algemene uitzondering ingevoerd voor geclassificeerde informatie. De vraag stelt zich dan ook hoe het ontwerp Koninklijk besluit in artikel 6, 3° kan afwijken van deze voedingsplicht zoals voorzien in de WPA of deze voedingsverplichting op zijn minst toch zeer sterk kan reduceren. Naast de louter juridische vraag stelt zich overigens en vooral ook de operationele vraag of het wel raadzaam is alle geclassificeerde informatie te weren uit de FTF-databank, temeer daar conform de interne richtlijnen van de federale politie, minstens alle leden van de politiediensten die een toegang wensen tot de FTF-databank over een veiligheidsmachtiging van het niveau geheim (zullen) moeten beschikken. De vereiste van een veiligheidsmachtiging "geheim" is overigens ook voorzien in het ontworpen artikel 7 § 2 van het KB.

14. Aansluitend bij de vraag of geclassificeerde gegevens of gevoelige politionele informatie al dan niet dienen te worden opgenomen in de gemeenschappelijke databank, willen het COC en het Comité I naar de volgende problematiek verwijzen. De wet en het ontwerp Koninklijk besluit (art. 4) dragen het OCAD op om 'op basis van de in deze gegevensbank geregistreerde gegevens en informatie' te valideren of een persoon als een FTF kan beschouwd worden. Indien essentiële informatie over een persoon niet aan de gemeenschappelijke databank wordt toegevoegd omwille van de classificatie of de gevoeligheid, zal het OCAD die info niet mee kunnen opnemen in zijn beoordeling, terwijl het Coördinatieorgaan wél over die geclassificeerde of gevoelige informatie zal beschikken op basis van de Wet van 10 juli 2006 betreffende de analyse van de dreiging.

---

282 Zie tevens de voorbereidende werken van de wet inzake aanvullende maatregelen ter bestrijding van terrorisme (*Parl. St.* Kamer 2015-2016, DOC 54, 1727/001, 21-22): '*Deze gegevens en informatie die betrekking hebben op de verschillende gegevenscategorieën zijn in principe geen geclassificeerde persoonsgegevens of informatie. Een zo ruim mogelijke verdeling van de gegevens en de informatie moet mogelijk zijn zonder hinderpalen te plaatsen op de verwerking ervan. Evenwel, wanneer het absoluut noodzakelijk is dat dergelijke gegevens in deze gegevensbanken verwerkt worden teneinde te beantwoorden aan de doelstellingen waarvoor ze opgericht werden, dan is de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen van toepassing. Daarom moet elke persoon die bijvoorbeeld een toegang wenst tot deze geclassificeerde gegevens en informatie over de gepaste veiligheidsmachtiging beschikken..*'.

8. Categorieën en types van persoonsgegevens en informatie

15. De identificatiegegevens van de gebruikers van de FTF-databank worden eveneens opgenomen in de databank. Overeenkomstig artikel 7, § 3 van het ontwerp Koninklijk besluit wordt door elke dienst een lijst van de personen met toegang opgesteld die aan de beheerder wordt overhandigd. In afwijking hiervan wordt de lijst van de inlichtingen- en veiligheidsdiensten enkel ter beschikking gehouden van de CBPL. Deze lijsten dienen echter niet enkel aan de beheerder te worden overhandigd, maar tevens aan de controleorganen, zijnde het COC en het Comité I. Daarnaast dient de lijst van de inlichtingen- en veiligheidsdiensten ter beschikking worden gesteld van het Comité I, en niet van de CBPL. De CBPL heeft immers geen specifieke controleopdracht in het kader van deze databank ten aanzien van de inlichtingen– en veiligheidsdiensten. Het is dan ook aanbevolen om het ontwerp van Koninklijk besluit in die zin aan te passen.

9. Betrokken diensten en aard van de toegang

16. Drie types van diensten zullen overeenkomstig de toelichting de databank gebruiken: de basisdiensten, de partnerdiensten en de andere Belgische openbare overheden, andere openbare organen of organismen die door de wet belast zijn met de toepassing van de strafwet of die wettelijke opdrachten van openbare veiligheid hebben. Hierbij vallen een aantal diensten op, waarvan men zich de vraag kan stellen waarom zij toegang dienen te krijgen tot deze FTF-databank.[283] Een dergelijke toegang kan overeenkomstig de voorbereidende werken[284] noodzakelijk zijn op strategisch, tactisch dan wel operationeel vlak. Daarnaast stellen de voorbereidende werken[285] dat dit natuurlijk niet betekent dat al deze actoren zomaar toegang zullen hebben tot de gemeenschappelijke databank, maar dat allen of sommigen ervan, op basis van de doelstelling eigen aan de gemeenschappelijke gegevensbank, hun wettelijke bevoegdheid en in functie van hun behoefte om te kennen, toegang zullen kunnen hebben. Bij de partnerdiensten kan bijvoorbeeld worden gedacht aan het waarom van een toegang voor de Vaste Commissie van de Lokale Politie (dat een louter strategisch beleidsorgaan is). Het basisprincipe van de toegang tot (de informatie in) een dergelijke databank moet de '*need to know*' zijn, en niet de '*nice to know*', zeker als men geen hypotheek wil leggen op de noodzakelijke '*need to share*' door de betrokken diensten. Derhalve dienen alle diensten die hieraan niet voldoen te worden uitgesloten van toegang tot de databank of dient hun toegang beperkt te worden tot bepaalde gegevens. Dit betekent uiteraard niet dat zij deze databank niet zouden kunnen voeden. Er zijn systemen denkbaar waarbij informatie kan worden aangeleverd door een bepaalde dienst, zonder dat deze dienst daarvoor zelf over een toegang tot de FTF-databank dient te beschikken.

17. Artikel 7, § 1, laatste alinea van het ontwerp Koninklijk besluit voorziet dat de toegang voor onder meer de justitiehuizen is beperkt tot de persoonsgegevens en de informatie

283 Zie in dezelfde zin, advies n° 57/2015 van de CBPL betreffende het voorontwerp van wet inzake aanvullende maatregelen ter bestrijding van terrorisme van 16 december 2015, in het bijzonder randnummer 77 e.v.

284 *Parl. St.* Kamer 2015-2016, DOC 54, 1727/001, 20 (Memorie van Toelichting bij het wetsontwerp inzake aanvullende maatregelen ter bestrijding van terrorisme).

285 *Parl. St.* Kamer 2015-2016, DOC 54, 1727/001, 15.

van de Foreign Terrorist Fighters voor wie de dienst zijn opdracht van justitiële begeleiding en toezicht moet verzekeren. Hier stelt zich de vraag hoe men dit technisch kan bewerkstelligen zodat wordt vermeden dat vanuit een justitiehuis opzoekingen kunnen worden gedaan op andere personen dan diegenen die zij begeleiden. Een oplossing kan er in bestaan dat de beheerder van de databank over een permanent geupdate lijst beschikt van alle lopende dossiers van de justitiehuizen waaromtrent een justitieel mandaat bestaat in de materie van de FTF.

Alleszins zal nauwlettend moeten toegezien worden op de toegangen tot de FTF-databank door de justitiehuizen en of deze beantwoorden aan een concreet dossier van het justitiehuis. Een mogelijke bijkomende garantie zou erin kunnen bestaan om de toegang per justitiehuis strikt te beperken, bijvoorbeeld tot één of enkele justitie assistent(en) die speciaal belast wordt met de opvolging van FTF-dossiers. Ook zouden er bij de diverse diensten met toegang tot de FTF-databank consulenten voor de veiligheid en de bescherming van de persoonlijke levenssfeer moeten worden aangewezen. Het COC en het Comité I zullen er nauw op toezien dat deze toegangen (het weze via een rechtstreekse toegang dan via een rechtstreekse bevraging) door de partnerdiensten en de andere Belgische openbare overheden, andere openbare organen of organismen die door de wet belast zijn met de toepassing van de strafwet of die wettelijke opdrachten van openbare veiligheid hebben, conform de wettelijke bepalingen zijn en in overeenstemming met de aangifte van de gemeenschappelijke databank. Het verdient daarnaast aanbeveling om dergelijke consulenten bij de diverse diensten expliciet te voorzien in het ontwerp Koninklijk besluit.

18. Aansluitend bij de punten 16 en 17 benadrukken het COC en het Comité I dat er in de aangifte duidelijk dient te worden vermeld welke dienst en welke functie of personen binnen die dienst toegang heeft tot welke concrete categorie van gegevens, en voor welke concrete doeleinden.

19. De diverse diensten staan zelf in voor de interne validering van de door hen aangeleverde gegevens. Teneinde een controle door het COC en het Comité I mogelijk te maken, dienen deze valideringsregels bij de aangifte te worden gevoegd.

20. Voor een effectieve opvolging van hun controleopdracht dient er tenslotte volgens het COC en het Comité I in een mogelijkheid te worden voorzien om na te gaan wat de toestand en inhoud van een bepaalde informatiefiche op een bepaald moment in de tijd was. Een historiek van de inlichtingenfiches moet op verzoek van de controleorganen aangemaakt kunnen worden.

10. Modaliteiten met betrekking tot de verwerking van de gegevens

21. Het interne valideringssysteem wordt overeenkomstig punt 10.4 van de toelichting door elke basisdienst en door elke partnerdienst meegedeeld aan de operationeel verantwoordelijke, die het zal doorgeven aan de beheerder en de consulent voor de veiligheid en bescherming van de persoonlijke levenssfeer. Zoals hierboven reeds aangehaald onder randnummer 19, dienen deze interne valideringsregels tevens te worden

overgemaakt aan het COC en het Comité I, zodat deze hun controletaken kunnen uitoefenen. Het intern valideringssysteem dient er immers voor te zorgen dat de persoonsgegevens en informatie die de betrokken diensten in het systeem inbrengen passend, ter zake dienend en niet overmatig zijn in het licht van de doeleinden bepaald in artikel 44/2, § 2 WPA en van de doeleinden voorzien in artikel 44/11/3*bis* § 2 WPA.

22. Voor wat betreft de overzending van persoonsgegevens en andere informatie uit een gemeenschappelijke gegevensbank aan buitenlandse inlichtingendiensten en organen die belast zijn met de analyse van de dreiging, bepaalt art. 44/11/3*quinquies*, derde lid, WPA dat de Koning hierover nadere regels uitwerkt. Artikel 15 § 3 van het ontwerp Koninklijk besluit stelt in deze alleen dat deze mededeling moet gebeuren in overeenstemming met art. 20 § 3 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en artikel 8, 3° van de wet van 10 juli 2006 betreffende de analyse van de dreiging.

23. Art. 20 § 3 Wet 30 november 1998 bepaalt op zijn beurt dat de voorwaarden voor de samenwerking met buitenlandse inlichtingendiensten nader moeten bepaald worden door de Nationale Veiligheidsraad (voorheen het Ministerieel Comité voor Inlichtingen en Veiligheid). Het COC en het Comité I zijn echter niet in kennis gesteld van eventuele richtlijnen ter zake van de Nationale Veiligheidsraad. Het is voor een controleorgaan evident onmogelijk om de naleving van eventuele richtlijnen na te gaan als die laatsten aan die controleorganen onthouden worden. Eén en ander verzwakt meteen ook het parlementair toezicht. De controleorganen verwijzen in dit verband naar de talloze aanbevelingen die het Comité I de afgelopen jaren formuleerde om dringend uitvoering te geven aan deze bepaling.[286] Het ontwerp Koninklijk besluit moet bijgevolg zelf de regels bepalen waaronder gegevens met het buitenland kunnen gedeeld worden en mag niet zonder meer verwijzen naar een gelijkaardige wettelijke verplichting aangezien die nog geen uitvoering kreeg.[287] Hierbij dient men onder meer oog te hebben voor de problematiek van buitenlandse 'zwarte lijsten' waarop Belgen kunnen terechtkomen ingevolge uitgewisselde gegevens.[288]

---

286 VAST COMITE I, *Activiteitenverslag 2006*, 4 en 132; *Activiteitenverslag 2013*, 4 en 111; *Activiteitenverslag 2014*, 112-113 en Activiteitenverslag 2015, tbc (Toezichtonderzoek betreffende de informatiepositie van de twee inlichtingendiensten over de rekrutering, de zending, het verblijf en den terugkeer van jongeren (van Belgische en andere nationaliteiten die in België verblijven) die vertrekken of vertrokken zijn naar Syrië of Irak en aangaande de uitwisseling van inlichtingen met diverse overheden).

287 Ook louter juridisch is het overigens zeer twijfelachtig of het ontworpen artikel 15 § 3 een correcte uitvoering is van de in artikel 44/11/3*quinquies*, laatste lid WPA voorziene delegatie aan de Koning.

288 Zie 'Toezichtonderzoek betreffende de klacht van een in België verblijvende Tunesische onderdaan die meent door de inlichtingendiensten gevolgd te worden' (*Activiteitenverslag 2015, tbc*). Het Vast Comité I beveelt daarin de diensten aan om bij verzoeken om informatie vanwege buitenlandse diensten of 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 binnenlands als buitenlands, met oog voor de mogelijke gevolgen voor betrokkenen. Daarenboven is het aanbevolen dat er getracht wordt een evenwicht te bereiken tussen enerzijds de collectieve en multilaterale veiligheidsvereisten en anderzijds de rechten van de burgers die op dergelijke lijsten voorkomen.

24. Wat betreft artikel 8, 3°, Wet van 10 juli 2006 geldt overigens dezelfde opmerking: de door de Nationale Veiligheidsraad uit te werken nadere regels inzake de uitwisseling van gegevens met homologe diensten ontbreken.

OM DEZE REDENEN,
Het COC en het Comité I,

Verlenen een voorlopig en gunstig advies onder voorbehoud van de opmerkingen in de randnummers 3-5, 7, 10-12, 15-20 en 22-24.

Advies goedgekeurd op de gezamenlijke plenaire vergadering van het Controleorgaan op de Politionele Informatie en het Vast Comité van Toezicht op de Inlichtingendiensten van 20 juni 2016

Voor het COC,
De Voorzitter,

Philippe ARNOULD

Voor het Vast Comité I,
De Voorzitter,

Guy RAPAILLE

GEZAMENLIJK ADVIES NR. 02/2016 VAN 1 DECEMBER 2016 BETREFFENDE DE VOORAFGAANDE AANGIFTE VAN DE GEMEENSCHAPPELIJKE DATABANK '*FOREIGN TERRORIST FIGHTERS*'

Het Controleorgaan op de politionele informatie (hierna COC) en het Vast Comité van toezicht op de inlichtingen– en veiligheidsdiensten (hierna Vast Comité I);

Gelet op de wet van 5 augustus 1992 op het politieambt (hierna WPA), inzonderheid artikel 44/11/3*bis*, § 3;

Gelet op het verzoek om advies van de Minister van Binnenlandse Zaken en de Minister van Justitie ontvangen op 03/11/2016;

Brengen op 1 december 2016 het volgend advies uit:

A. VOORWERP VAN DE AANVRAAG EN PROCEDURELE ASPECTEN

1. Op 3 november jl. hebben de ministers van Justitie en Binnenlandse Zaken een vraag tot advies overgemaakt aan het COC en het Vast Comité I overeenkomstig artikel 44/11/3*bis*, § 3 WPA aangaande de voorafgaande aangifte van de gemeenschappelijke databank 'Foreign Terrorist Fighters' (hierna FTF-databank). Het COC en Vast Comité I dienen vervolgens overeenkomstig voormeld artikel binnen de dertig dagen een gezamenlijk advies uit te brengen. Bij voormeld schrijven vanwege de bevoegde ministers werd de 'user guide' en de 'handleiding dynamische databank FTF' als bijlage gevoegd.

2. Het COC en Vast Comité I hebben reeds op 20 juni 2016 een voorlopig gezamenlijk advies uitgebracht aangaande een voorafgaande aangifte van de gemeenschappelijke FTF-databank, waarbij zij zich het recht voorbehielden om nog een bijkomend advies te verstrekken na de publicatie van het Koninklijk besluit inzake de FTF-databank, en na mogelijke bijkomende aanvullende aangiftes voor deze databank. Zij brengen hiernavolgend dan ook bijkomend advies uit over de huidige 'voorafgaandelijke aangifte'.

B. TEN GRONDE

3. Hiernavolgend wordt een analyse gemaakt van het document 'voorafgaandelijke aangifte', rekening houdend met de daarin aangehouden indeling. Enkel de relevante punten worden besproken. Voorafgaandelijk wordt nog meegegeven dat het voor het Vast Comité I en het COC niet duidelijk is wat wordt bedoeld met "*vonnis is nog lopende*" onder de rubriek 8, b) "gerechtelijke gegevens", temeer het bestaan van een lopend vooronderzoek opgenomen is in de rubriek 8, d) en elke veroordeling/vrijspraak eveneens opgenomen is in de rubriek 8, b). Mogelijks wordt een buitenvervolging of een verwijzingsbeschikking bedoeld door een onderzoeksgerecht?

Inzake punt 1. Consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer

4. De voorafgaande aangifte maakt 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. Deze persoon is nochtans van groot belang in het kader van de controletaken van het COC en Vast Comité I, aangezien hij of zij overeenkomstig artikel 44/3, § 1/1 WPA belast is met de contacten met het COC en het Vast Comité I. Deze persoon dient derhalve in de aangifte te worden opgenomen. Het is daarnaast ook van belang dat van bij de conceptie en uitrol van de gemeenschappelijke gegevensbank de consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer betrokken wordt en dus in een zo vroeg mogelijk stadium wordt aangeduid. De aanduiding ervan in de aangifte aan de controleorganen laat deze laatste ook toe meteen een zicht te hebben op de graad van onafhankelijkheid die betrokkene moet hebben ten aanzien van de overheden, organen, organismen, diensten, directies of de commissie bedoeld in artikel 44/11/3*ter* WPA. Het belang van deze figuur werd nog benadrukt in art. 5 van het 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 (hierna afgekort "KB FTF") en in het Verslag aan de Koning bij dat artikel.

5. Daarentegen worden bij de diverse diensten (OCAD, geïntegreerde politie, VSSE, ADIV, DG penitentiaire inrichtingen, openbaar ministerie, CFI en de dienst vreemdelingenzaken) met toegang tot de gemeenschappelijke FTF-databank in de aanstelling van een consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer voorzien, zoals voorgesteld in het gezamenlijk advies 01/2016 in randnummer 17, laatste zin. Het COC en het Vast Comité I herinneren eraan dat zij op de hoogte dienen te worden gesteld van de aanstelling van andere bijkomende consulenten voor nieuwe diensten die toegang zouden bekomen.

Inzake punt 9. Betrokken diensten en aard van de toegang

6. Drie types van diensten zullen overeenkomstig de toelichting bij de aangifte de databank gebruiken: de basisdiensten, de partnerdiensten en de andere Belgische openbare overheden, andere openbare organen of organismen die door de wet belast zijn met de toepassing van de strafwet of die wettelijke opdrachten van openbare veiligheid hebben. Het COC en het Vast Comité I herhalen dat het basisprincipe van de toegang tot (de informatie in) een dergelijke databank de '*need to know*' moet zijn, en niet de '*nice to know*', zeker als men geen hypotheek wil leggen op de noodzakelijke '*need to share*' door de betrokken diensten. Derhalve dienen alle diensten die hieraan niet voldoen te worden uitgesloten van toegang tot de databank of dient hun toegang beperkt te worden tot bepaalde gegevens. Dit betekent uiteraard niet dat zij deze databank niet zouden kunnen voeden. Er zijn systemen denkbaar waarbij informatie kan worden aangeleverd door een bepaalde dienst, zonder dat deze dienst daarvoor zelf over een (al dan niet volledige) toegang tot de FTF-databank dient te beschikken. Het

COC en het Vast Comité I verwijzen hieromtrent tevens naar het gezamenlijk advies 01/2016 van 20 juni 2016, randnummer 17 met betrekking tot de justitiehuizen.

7. In voormeld gezamenlijk advies 01/2016 hadden het COC en het Vast Comité I tevens aangestipt dat er in de aangifte duidelijk diende te worden vermeld welke dienst en welke functie of personen binnen die dienst toegang heeft tot welke concrete categorie van gegevens, en voor welke concrete doeleinden tot de gemeenschappelijke databank. Onder punt 9.2 van de voorafgaande aangifte wordt een opsomming weergegeven voor de toegangen per betrokken dienst, zowel de rechtstreekse toegang als de rechtstreekse bevraging. De concrete doeleinden worden hierbij echter vaak vergeten; het verdient dan ook aanbeveling voor de betrokken diensten om deze ter beschikking te houden van het COC en het Vast Comité I, elk via hun respectieve consulenten voor de veiligheid en bescherming van de persoonlijke levenssfeer. Voor wat betreft de directe toegang door de justitiehuizen en het Vlaams Agentschap Jongerenwelzijn tenslotte, noteren het COC en het Vast Comité I dat de praktische modaliteiten hiervan nog zullen worden gedefinieerd in een aanvullende aangifte.

8. De diverse diensten staan zelf in voor de interne validering van de door hen aangeleverde gegevens. Teneinde een controle door het COC en het Vast Comité I mogelijk te maken, dienen deze valideringsregels bij de aangifte te worden gevoegd. Deze werden opgenomen onder punt 10.4 van de voorafgaande aangifte, en worden hiernavolgend besproken onder randnummer 10.

9. Voor een effectieve opvolging van hun controleopdracht diende er tenslotte volgens het COC en het Vast Comité I in een mogelijkheid te worden voorzien om na te gaan wat de toestand en inhoud van een bepaalde informatiefiche op een bepaald moment in de tijd was. Een historiek van de inlichtingenfiches moet op verzoek van de controleorganen aangemaakt kunnen worden. Hierop wordt niet ingegaan door de voorafgaande aangifte. Het COC en het Vast Comité I dringen erop aan om alsnog in deze mogelijkheid te voorzien, dan wel toe te lichten waarom dit niet mogelijk zou zijn. Het bijhouden van een historiek is alvast voor controledoeleinden essentieel. Zoniet is het steeds bijzonder problematisch om te kunnen achterhalen wie, wat wist of behoorde te weten, op welk moment. Maar ook voor onderzoeksdoeleinden lijkt het bijhouden ervan minstens zeer nuttig. Er moet trouwens op gewezen worden dat het waken over de traceerbaarheid één van de opdrachten is van de beheerder van de FTF-databank, met name de federale politie (art. 3, 2e streepje KB FTF van 21.07.2016 en het verslag aan de Koning bij voormeld artikel). Terecht vermeldt voormeld verslag bij artikel 6 ook nog "*Tot slot worden tevens de persoonsgegevens of – wat de leden van de inlichtingen- en veiligheidsdiensten betreft – de identificatiecodes van de gebruikers geregistreerd (oplijsting, logging) in de gegevensbank F.T.F. Dit is niet alleen interessant op operationeel vlak (weten wie een bepaald gegeven toegevoegd heeft, maakt het mogelijk de samenwerking tussen de verschillende partners te versterken) maar ook op het vlak van de beveiliging (wie heeft gewijzigd, uitgewist, wanneer, …)*".

Inzake punt 10. Modaliteiten met betrekking tot de verwerking van de gegevens

10. Het interne valideringssysteem, verplichtend voorzien in art. 8 § 1, 1e lid van het FTF KB (en dat overeenkomstig art. 8 § 1, 2e lid KB FTF aan het Vast Comité I en het C.O.C moet worden overgemaakt) wordt overeenkomstig punt 10.4 opgelijst voor de diverse diensten: OCAD, Federale politie, ADIV, VSSE, CFI en DVZ, weze het in veel gevallen te summier of zelfs helemaal onbestaande (zoals voor DVZ). Het intern valideringssysteem dient er immers voor te zorgen dat de persoonsgegevens en informatie die de betrokken diensten in het systeem inbrengen passend, ter zake dienend en niet overmatig zijn in het licht van de doeleinden bepaald in artikel 44/2, § 2 WPA en van de doeleinden voorzien in artikel 44/11/3*bis* § 2 WPA. Het COC en het Vast Comité I roepen de betrokken diensten dan ook op om voor het opstellen van hun intern valideringssysteem hiermee rekening te houden, zodat men (middels een document) kan aantonen (aan onder meer het Vast Comité I en het COC) dat de persoonsgegevens en informatie die de betrokken diensten in het systeem inbrengen passend, ter zake dienend en niet overmatig zijn in het licht van de doeleinden bepaald in artikel 44/2, § 2 WPA en van de doeleinden voorzien in artikel 44/11/3*bis* § 2 WPA.

OM DEZE REDENEN,
Het COC en het Vast Comité I,

Verlenen een gunstig advies onder voorbehoud van de opmerkingen in de randnummers 4, 6-7 en 9-10.

Advies goedgekeurd door het Controleorgaan op de Politionele Informatie en het Vast Comité van Toezicht op de Inlichtingendiensten op 1 december 2016.

Voor het Controleorgaan	Voor het Vast Comité I
De Voorzitter van het COC,	De Voorzitter van het Vast Comité I,
(get.) Philippe ARNOULD	(get.) Guy RAPAILLE