RAPPORT D'ACTIVITÉS 2019
ACTIVITEITENVERSLAG 2019

Quis custodiet ipsos custodes ?

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

Rédaction

Comité permanent de Contrôle des services de renseignement et de sécurité, rue de Louvain 48, boîte 4 à 1000 Bruxelles (02 286 29 88).

Déjà parus dans cette série

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Comité permanent R, *Rapport d'activités 2006,* 2007, 147 p.
3) Comité permanent R, *Rapport d'activités 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, 2010, 220 p.
5) Comité permanent R, *Rapport d'activités 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Comité permanent R, *Rapport d'activités 2009,* 2010, 127 p.
8) Comité permanent R, *Rapport d'activités 2010,* 2011, 119 p.
9) Comité permanent R, *Rapport d'activités 2011,* 2012, 134 p.
10) W. Van Laethem et J. Vanderborght, *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, 2013, 565 p.
11) Comité permanent R, *Rapport d'activités 2012*, 2013, 127 p.
12) Comité permanent R, *Rapport d'activités 2013*, 2014, 212 p.
13) Comité permanent R, *Rapport d'activités 2014*, 2015, 141 p.
14) Comité permanent R, *Rapport d'activités 2015*, 2016, 131 p.
15) Comité permanent R, *Rapport d'activités 2016*, 2017, 227 p.
16) Comité permanent R, *Rapport d'activités 2017*, 2018, 152 p.
17) Comité permanent R, *Rapport d'activités 2018*, 2019, 167 p.
18) J. Vanderborght (ed.), *Les méthodes particulières de renseignement : de l'ombre à la lumière*, 2020, 151 p.
19) Comité permanent R, *Rapport d'activités 2019*, 2020, 150 p.

RAPPORT D'ACTIVITÉS 2019

Comité permanent de Contrôle des services de renseignement et de sécurité

Comité permanent de Contrôle des services
de renseignement et de sécurité

INTERSENTIA

Antwerpen – Gent – Cambridge

Le présent *Rapport d'activités 2019* a été approuvé par le Comité permanent de Contrôle des services de renseignement et de sécurité lors de la réunion du 28 octobre 2020.

(*soussignés*)
Serge Lipszyc, président
Pieter-Alexander De Brock, conseiller
Laurent Van Doren, conseiller
Wauter Van Laethem, greffier faisant fonction

Rapport d'activités 2019
Comité permanent de Contrôle des services de renseignement et de sécurité

© 2020 Lefebvre Sarrut Belgium NV
rue Haute 139/6 – 1000 Bruxelles

ISBN 978-94-000-1209-7
D/2020/7849/68
NUR 823

Tous droits réservés. Sous réserve d'exceptions explicitement prévues par la loi, aucun élément de cette publication ne peut être reproduit, stocké dans une base de données automatisée ou publié, de quelque manière que ce soit, sans l'autorisation expresse préalable des éditeurs.

Malgré tout le soin apporté à la composition du texte, ni les auteurs ni l'éditeur ne sauraient être tenus pour responsables des dommages pouvant résulter d'une erreur éventuelle de cette publication.

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

ACC	Autorité de contrôle compétente
AFCN	Agence fédérale de Contrôle nucléaire
AG	Administrateur général (VSSE)
AGA	Administrateur général adjoint (VSSE)
A.M.	Arrêté ministériel
Ann. parl.	Annales parlementaires
ANS	Autorité nationale de sécurité
APD	Autorité de protection des données
A.R.	Arrêté royal
AR C&HS	Arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
AR FTF	Arrêté royal du 21 juillet 2016 relatif à la banque de données commune 'Foreign Terrorist Fighters' et portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police
AR OCAM	Arrêté royal du 28 novembre 2006 portant exécution de la Loi du 10 juillet 2006 relative à l'analyse de la menace
AR PH	Arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandiste de haine et portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police
AR TF	Arrêté royal du 23 avril 2018 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters
BDC	Banque de données commune
BDC PH	Banque de données commune 'Propagandistes de haine'
BDC TF	Banque de données commune 'Terrorist fighters'

BELPIU	*Belgian Passenger Information Unit* (Unité belge d'Information des Passagers)
BISC	*Belgian Intelligence Studies Centre*
BNG	Banque de données nationale générale
BPR	*Business Process Re-engineering*
BSS	*British Security Service* (MI5)
CCB	Centre pour la Cybersécurité Belgique
CCIRM	*Collection Coordination Information Requirement Management* (SGRS)
CEDH	Convention européenne des droits de l'homme
CGRA	Commissariat général aux réfugiés et aux apatrides
CHOD	*Chief of Defence*
CI	*Counterintelligence*
CNCIS	Commission nationale de contrôle des interceptions de sécurité
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNS	Conseil national de sécurité
C.O.C.	Organe de contrôle de l'information policière
Comité permanent P	Comité permanent de Contrôle des services de police
Comité permanent R	Comité permanent de Contrôle des services de renseignement et de sécurité
Commission BIM	Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité
CRABV	Compte Rendu Analytique – *Beknopt Verslag*
CRIV	Compte Rendu Intégral – *Integraal Verslag*
CTG	*Counter Terrorism Group*
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten*
DA	Directeur Analyse
DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
DGCC	Direction générale du Centre de crise
DISCC	*Defense Intelligence and Security Coordination Centre* (SGRS)
Doc. parl.	Documents parlementaires de la Chambre et du Sénat
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
EION	*European Intelligence Oversight Network*
EPV	Extrémistes potentiellement violents

FTF	*Foreign terrorist fighters*
GCHQ	*General Communications Headquarters*
HTF	*Homegrown terrorist fighters*
HUMINT	*Human intelligence*
ICP	*Intelligence collection plan*
ICT	*Information and communications technology*
IMINT	*Image intelligence*
INE	*Intelligence Network Europe*
IOWG	*Intelligence Oversight Working Group*
ISTAR	*Intelligence, surveillance, target acquisition and reconnaissance*
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 APD	Loi du 3 décembre 2017 portant création de l'Autorité de protection des données
Loi MRD	Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité
Loi PNR	Loi du 25 décembre 2016 relative au traitement des données des passagers
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
LPD	Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Loi protection des données)
L.R&S	Loi du 30 novembre 1998 organique des services de renseignement et de sécurité
M.B.	Moniteur belge
MoU	*Memorandum of Understanding*
MRD	Méthodes de recueil des données
NA	Note aux autorités
NOS	*Nato Office of Security*
OCAM	Organe de coordination pour l'analyse de la menace
OE	Office des étrangers
OSINT	*Open sources intelligence*

OTAN	Organisation du Traité de l'Atlantique Nord
PCT	Personnes condamnées pour terrorisme
PDR	Plan Directeur du Renseignement
PH	Propagandistes de haine
PNR	*Passenger Name Record*
POC	*Point of contact*
PSNR	Plan Stratégique National du Renseignement
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
RGPD	Règlement Général sur la Protection des Données
Service VVS	Service Vérifications de Sécurité (VSSE)
SGRS	Service Général du Renseignement et de la Sécurité
SIGINT	*Signal intelligence*
SIS	*Secret Intelligence Service* (MI6)
SOP	*Standard Operating Procedures*
SPF	Service public fédéral
TF	*Terrorist fighters*
TO	Tableau organique
UIP	Unité d'Information des Passagers
VSSE	Sûreté de l'État

PRÉFACE

En septembre 1994, dans son premier rapport annuel, le Comité permanent R relevait le manque de capacité humaine à la Sûreté de l'État et au Service Général du Renseignement (qui deviendra plus tard SGRS).[1] Vingt-six ans plus tard, le constat reste malheureusement toujours d'actualité.

Le Comité constate qu'en Belgique, la communauté du renseignement n'occupe pas la place qui lui reviendrait concrètement. Pourquoi ? En raison, d'une part, du déséquilibre entre les obligations et les attentes qui sont aujourd'hui prescrites à ces deux services et, d'autre part, en raison du sous-effectif structurel qui les affecte. Or, cela ne peut pas être un problème insoluble !

Les rapports annuels du Comité, pas plus que les rapports des Commissions parlementaires, ne peuvent plus constituer un catalogue de rappels ou de recommandations. Et, si certains observateurs en Belgique comme à l'étranger ont notamment déclaré que la Belgique était un État défaillant, les travaux de la Commission parlementaire 'Attentats terroristes' ont clairement démontré que ces déclarations étaient excessives. Selon son président[2], la plupart des opérations ont été – et sont – bien menées, quoique certains rouages aient été – et soient encore – grippés. Les recommandations de la Commission d'enquête visent précisément à les dégripper.

Notre pays est, aujourd'hui, comme la plupart des pays européens, confronté à une diversification des menaces. Il y a assurément le terrorisme, qu'il soit djihadiste ou d'extrême droite. Il y a également le développement inquiétant des activités d'ingérence et d'espionnage menées par des puissances étrangères. Ces menaces exigent que nos services soient aptes à y répondre. Eux qui ont tous comme même objectif de lutter contre les atteintes au fondement démocratique de notre État.

Faut-il se lamenter ? Non, tout n'est pas qu'inquiétude. On peut relever que les rapports successifs du Comité ont permis aux responsables de la Défense d'initier le '*change management*' devenu indispensable au sein du SGRS.

Mais cette amélioration sensible ne suffit pas à distribuer un satisfecit général. En effet, l'enquête portant sur le screening en Belgique au sein des services de renseignement, soulève indubitablement un réel problème. Comment, malgré les recommandations de la Commission d'enquête 'Attentats terroristes', accepter

---

1 COMITÉ PERMANENT R, *Rapport d'activités 1994*, 51.

2 LA CHAMBRE DES REPRÉSENTANTS DE BELGIQUE, *Commission d'enquête Attentats terroristes 22 mars 2016. Résumé des travaux et recommandations*, 2018, 13.

que les nouvelles informations en possession des services de police, de justice et de sécurité ne soient pas intégrées en temps réel, mais bien plus tard, au gré des demandes de renouvellements des habilitations, attestations et avis de sécurité. Ces informations restent inacceptablement en silos hermétiques. Cette constatation est plus que préoccupante. La recommandation de la Commission parlementaire reste lettre morte sur ce point : "*Les informations pertinentes doivent circuler rapidement d'un niveau de pouvoir à l'autre, d'un service public à l'autre. Cette circulation rapide de l'information doit également être effective entre les services belges et leurs homologues internationaux. Cela doit permettre aux services de sécurité de détecter de façon précoce les terroristes potentiels, de se concerter rapidement et de fixer des priorités de façon flexible.*"[3]

Les attentats de Paris et Bruxelles ont eu pour conséquence une avalanche législative. Les deux services de renseignement ainsi que le Comité voient leurs compétences étendues. Pour le Comité, il s'agit assurément d'une garantie dans la protection de la vie privée, des droits du citoyen et du bon fonctionnement des institutions. Mais ces mesures légales sont malheureusement adoptées sans tenir compte de la capacité réelle de mise en œuvre par les institutions. Il nous appartient de rappeler ce principe de réalité et de voir, enfin, les pouvoirs législatifs et exécutifs prendre la réelle mesure de ces évolutions législatives.

Notre rôle apparaît encore plus essentiel aujourd'hui, puisque les nouvelles mesures attribuées nécessitent un contrôle effectif sous peine de ne pas jouer notre rôle de gardien de la démocratie. Il appartient au Comité d'exercer non seulement un contrôle attentif des deux services de renseignement mais, selon une distribution alambiquée des compétences, soit avec le Comité permanent P, soit avec l'Organe de contrôle de l'information policière (C.O.C.), d'examiner le fonctionnement adéquat de l'Organe de coordination pour l'analyse de la menace (OCAM), de ses banques de données et de ses services d'appui.

Le Comité est devenu, depuis 2018, l'autorité de protection des données dans le domaine spécifique du renseignement. Il est donc dorénavant le gardien de la protection des données du citoyen. Dans un monde où les bases de données et métadonnées deviennent la règle, son rôle est accru. Il doit être apte à contrôler tant les *databases* que leur faille de sécurité, tant l'utilisation du cyber que la question de la création d'une banque carrefour de la sécurité.

À côté de ces missions, ne lui revient-il pas naturellement d'être désigné pour contrôler les autres services publics qui font du renseignement en dehors de tout contrôle ou de tout cadre légal ?

Outre ses missions de contrôle des services de renseignement, son rôle et soutien à la juridiction administrative qu'est l'Organe de recours est de la plus haute importance. Il peut ainsi donner les garanties d'être au quotidien un "service public de la Justice" dans le domaine de la sécurité.

---

3 *Ibid*., 38.

Face à ces menaces, ces nouvelles compétences, à ces trop nombreuses recommandations non suivies d'effet, pouvons-nous rester passifs ? Le Comité estime que le contexte général dans lequel œuvrent au quotidien le SGRS et la VSSE exige des engagements fermes en faveur de la sécurité.

Nous dédions le présent rapport d'activités à Wouter De Ridder, qui part aujourd'hui à la retraite, après une vie professionnelle consacrée à notre institution. Notre greffier a œuvré pendant près de 30 ans à faire du Comité un modèle d'organe de contrôle des services de renseignement qui s'est exporté dans le monde entier. Nous tenons à lui adresser nos plus sincères remerciements.

Serge Lipszyc,
Président du Comité permanent de Contrôle
des services de renseignement et de sécurité

26 octobre 2020

CHAPITRE I
LES ENQUÊTES DE CONTRÔLE

Diverses instances et personnes peuvent 'saisir' le Comité permanent R d'une enquête de contrôle : la Commission parlementaire de suivi, les ministres de tutelle, toute personne (morale) qui souhaite introduire une plainte ou faire une dénonciation, etc. Le Comité peut lui aussi prendre l'initiative d'ouvrir une enquête. En 2019, le Comité permanent R a finalisé six enquêtes de contrôle (I.1 à I.6), dont deux ont été ouvertes d'initiative, deux effectuées à la demande de la Commission parlementaire de suivi et, enfin, deux ont été initiées à la suite de plaintes individuelles.[1] Le Comité a par ailleurs initié sept nouvelles enquêtes en 2019. Une description succincte des enquêtes en cours et/ou des enquêtes figure au chapitre I.7. Les recommandations émises à l'issue des enquêtes de contrôle ont été regroupées au Chapitre XI.

Au total, le Comité permanent R a reçu 90 plaintes ou dénonciations en 2019.[2] Après une brève pré-enquête et la vérification de plusieurs données objectives, le Comité a rejeté 82 plaintes ou dénonciations, soit parce qu'elles étaient manifestement non fondées[3] (art. 34 L.Contrôle), soit parce que le Comité n'était pas compétent pour en traiter les griefs. Dans ces derniers cas, les plaignants ont été renvoyés, si possible, vers les instances compétentes (le Comité permanent P, la Police fédérale, le procureur du Roi ou d'autres instances). Six des huit plaintes traitées ont pu être clôturées en 2019.

Outre les enquêtes de contrôle, le Comité permanent R ouvre ce que l'on appelle des 'dossiers d'information'. Ceux-ci doivent permettre de répondre à des questions relatives au fonctionnement des services de renseignement et de l'OCAM.[4] Si ces dossiers font apparaître des indices de dysfonctionnement ou

---

1 En janvier 2019, un protocole a été conclu avec la VSSE, ce service donnant accès à sa banque de données centrale aux membres du Service d'Enquêtes R mandatés individuellement pour des consultations dans le cadre des missions légales du Comité ou de la sécurité de l'exercice des missions.

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

3 Le Comité reçoit encore toute une série de plaintes et dénonciations fantaisistes.

4 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

des aspects du fonctionnement des services de renseignement qui requièrent un examen approfondi, le Comité peut procéder à l'ouverture d'une enquête de contrôle formelle. Si toutefois il apparaît que ce genre d'enquête n'apporterait pas de plus-value au regard des finalités du Comité, aucune suite n'est donnée au dossier d'information. En 2019, des dossiers d'information ont été ouverts notamment sur la concertation sociale au sein des services de renseignement, sur les risques en matière de sécurité et les éventuels dysfonctionnements au SGRS, ou encore sur les activités de la Commission de suivi 'Attentats terroristes'.[5]

I.1. LA RÉALISATION DE SCREENINGS DE SÉCURITÉ PAR LES SERVICES DE RENSEIGNEMENT

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

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

En partant d'une plainte individuelle, le Comité a estimé légitime d'ouvrir une enquête de contrôle plus large sur la manière dont les services de renseignement réalisent les screenings de sécurité.[6, 7]

état d'un incident et le Comité souhaite vérifier comment cet incident a été traité ; les médias signalent un événement et le Comité souhaite déterminer si ces faits sont conformes à la réalité et s'ils relèvent d'une problématique plus générale.

5 Le nom complet est le suivant : 'Commission de suivi 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'.

6 Par screening de sécurité, on entend *"une évaluation imposée par la loi et conforme à celle-ci, effectuée par une autorité administrative sur la base des données (à caractère personnel) dont elle dispose déjà ou qui lui ont été communiquées, par laquelle elle décide si le profil d'une personne (morale) privée présente ou peut présenter un risque d'usage non approprié d'une autorisation déterminée susceptible de mettre en péril certains intérêts fondamentaux (de l'État), de sorte que cette même autorité ou une autre autorité (étrangère) qui en est informée peut décider de l'octroi, du retrait ou de la limitation de cette autorisation."* (traduction libre). Définition empruntée à W. VAN LAETHEM, 'Veiligheidsscreenings', Praktijkseminarie, 22 novembre 2016 (Bruxelles, Politeia).

7 'Enquête de contrôle sur la manière dont la VSSE et la SGRS procèdent aux vérifications de sécurité et à l'évaluation des données nécessaires à l'octroi des attestations de sécurité, en

I.1.1. LE CADRE JURIDIQUE

I.1.1.1. Les missions légales

La Loi du 30 novembre 1998 a décrit de manière stricte les missions et les compétences des deux services de renseignement. Les missions de la VSSE sont reprises à l'article 7 L.R&S, tandis que celles confiées au SGRS figurent à l'article 11 L.R&S. Outre la mission de renseignement (art. 7, 1° et 3°/1 L.R&S) et la réalisation d'enquêtes de sécurité (art. 7, 2° L.R&S), la VSSE peut *'exécuter toutes autres missions qui lui sont confiées par ou en vertu de la loi'* (art. 7, 4° L.R&S). Pour le SGRS, le législateur s'est montré plus strict encore, en ce sens qu'il n'a pas prévu la possibilité d'exécuter des missions *'en vertu de la loi'*. En d'autres termes, cela signifie donc qu'une base légale spécifique est nécessaire pour les screenings qui sont effectués par les services de renseignement ou pour les screenings auxquels les services prêtent leur concours en communiquant des données à d'autres autorités.

À cet égard, il existe de nombreuses dispositions légales qui permettent à la VSSE et/ou au SGRS (dans certaines procédures, le SGRS n'est pas partie prenante), de communiquer les renseignements dont ils disposent à diverses autorités sur la base desquels ces autorités réalisent une évaluation. Il est néanmoins ressorti de l'analyse juridique que toutes ces réglementations diffèrent, tantôt fondamentalement, tantôt superficiellement.

Indépendamment de cela, le Comité a pu constater que les deux services de renseignement ne tenaient compte de ces réglementations que dans une mesure limitée, voire n'en tenaient pas compte (*infra*). Il est en outre apparu que les services ne se sont pas montrés suffisamment critiques quant à la légalité du concours qu'ils prêtent dans le cadre de certains screenings et, le cas échéant, quant aux conditions dans lesquelles ce concours était autorisé. Il s'est également avéré que les services de renseignement se référaient à l'article 19 L.R&S. Le Comité avait néanmoins déjà établi[8] que l'article 19 L.R&S n'offrait pas de base légale pour la communication systématique de données à d'autres autorités en vue d'une évaluation.[9]

---

application des articles 22*bis* à 22*sexies* de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&HS)'. L'enquête a été ouverte en février 2017 et clôturée en mars 2019.

8 COMITÉ PERMANENT R, *Rapport d'activités 2003*, 256-279. Le Comité mettait en garde contre d'éventuels problèmes juridiques si une autorité continuait de fonder ses décisions sur des informations obtenues dans le cadre d'un screening systématique de la VSSE ou du SGRS, en l'absence de base légale spécifique. L'enquête a démontré que ce genre de situation se présente encore.

9 Cette analyse du Comité a d'ailleurs donné lieu à l'adoption de la Loi du 3 mai 2005 qui, dans la Loi Classification du 11 décembre 1998, a élargi le cadre des screenings dans les domaines les plus divers.

I.1.1.2. Adaptation de la législation

Au moment de l'enquête, il n'y avait pas de base légale pour le screening de certaines fonctions et de certains secteurs sensibles (par ex. les fonctionnaires pénitentiaires). Toujours en cours d'enquête, la législation en matière de vérifications de sécurité a été adaptée par la Loi du 23 février 2018[10], avec en corollaire davantage de demandes de vérifications émanant d'une série de nouveaux secteurs (par ex. les transports publics, le secteur de la sécurité privée, etc.). La nouvelle législation prévoit aussi une nouvelle mission pour la VSSE et le SGRS, les services de renseignement devenant responsables des analyses de la menace dans différents secteurs en matière d'espionnage.

I.1.2. LES SCREENINGS DE SÉCURITÉ À LA VSSE

I.1.2.1. Organisation

À la VSSE, les demandes de vérifications de sécurité sont traitées en premier lieu par le Service Vérifications de Sécurité (VVS). D'un point de vue organisationnel, ce service est placé sous la responsabilité de l'Administrateur général adjoint (AGA) de la VSSE. Certains types de screenings sont traités dans un second temps par les services d'analyse. Ces services sont placés sous l'autorité du Directeur de l'Analyse (DA).

Le Comité a pu constater qu'aucune formation spécifique n'est prévue pour le personnel du Service VVS. Il dispose de la même offre de formations que le reste du personnel administratif. Ces formations ont un caractère plutôt générique, et s'ajoutent à la formation de base sur la structure et les missions générales de la VSSE. Selon le Chef du service VVS, aucune lacune n'a cependant été constatée dans le passé en termes de besoins en formation des collaborateurs. La formation spécifique afférente aux missions a lieu *'on the job'*.

La Direction générale de la VSSE considère que la réalisation de screenings est une mission spécifique du service, qu'elle voudrait donc voir traitée exclusivement en interne. La Direction générale avait l'intention de restructurer à court terme la manière dont la mission du service est remplie. Concrètement, tout ce qui concerne les screenings sera centralisé au sein du Service VVS. Au cours de l'enquête, un groupe de travail a initié une réflexion sur l'avenir du Service VVS et sur l'instauration d'un pilier 'Sécurité et Avis' qui regrouperait les Services VVS, VES (enquêtes de sécurité) et VBS (bureau de sécurité). La décision de la Direction générale de la VSSE de centraliser, à l'avenir, le

[10] Loi du 23 février 2018 portant modification de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *M.B.* 1er juin 2018.

traitement de toutes les vérifications de sécurité dans un seul et même service a eu pour autre conséquence de renforcer l'effectif du Service VVS.

I.1.2.2. Données quantitatives

Les chiffres[11] mis à disposition par la Sûreté de l'État montrent une croissance régulière du nombre de vérifications. Un constat particulièrement frappant est l'augmentation du nombre de vérifications dans le cadre des naturalisations et des déclarations de nationalité et la forte croissance du nombre de vérifications effectuées à la demande de l'Office des étrangers (OE) et du Commissariat général aux réfugiés et aux apatrides (CGRA). Les vérifications effectuées dans le cadre de la délivrance de badges d'accès à (certaines zones) des aéroports constituent une autre catégorie de screenings de sécurité importante au niveau quantitatif.

Une norme est appliquée en interne pour déterminer le nombre de vérifications pouvant être effectuées. Pour 2017, on se trouvait 12 % au-dessus de cette norme. En cas d'absence d'un ou de plusieurs membre(s) du personnel, le dépassement de cette norme présentait un risque de retard dans le traitement des dossiers. Il n'y avait donc aucune réserve pour pallier les absences.

I.1.2.3. Processus de travail

Dans le cadre de la réalisation des screenings, la VSSE opère, d'une part, comme un service qui fournit des informations à d'autres autorités, et, d'autre part, comme autorité de sécurité.[12]

Toutes les demandes de screening sont traitées en premier lieu par le Service VVS. Le Comité a remarqué qu'à la réception de la liste de noms, la légalité de la demande n'était pas vérifiée, ce qui, dans certains cas, s'impose néanmoins (par ex. pour les questions non systématiques). Toutefois, les collaborateurs du Service VVS procèdent immédiatement à une vérification dans la banque de données de la VSSE. Si une personne n'y figure pas, le collaborateur traitant répond directement à l'autorité compétente/au client. En revanche, un *'hit'*

---

11 Les chiffres fournis par la VSSE dans le cadre de cette enquête ont un caractère indicatif. La méthode de travail utilisée actuellement ne permet pas de générer des statistiques sur le nombre de vérifications positives ou *'hits'*. Cela tient au fait que les données chiffrées ne sont pas systématiquement conservées. Il en résulte une impossibilité de monitorer les résultats du service (à long terme) et de les rectifier lorsque, par exemple, le nombre de *'hits'* change. Ce second aspect influence également l'élaboration de la stratégie, en ce sens qu'en l'absence d'informations sur les résultats, il est difficile de fixer les objectifs (et d'ailleurs aussi les moyens à affecter) ou de définir une répartition fondée de la charge de travail entre le Service VVS et les services d'analyse.

12 La VSSE opère comme autorité de sécurité lorsque du personnel sous contrat (par ex. pour des travaux d'entretien) doit se voir autoriser l'accès à des bâtiments du service et lorsque le service lui-même organise des événements.

positif est présenté au chef de service, qui établit une analyse des informations disponibles et rédige la réponse pour l'autorité requérante/le client.

Dans le cas des screenings pour lesquels l'Autorité nationale de sécurité (ANS) est l'autorité de sécurité compétente (par ex. des vérifications de sécurité devant donner lieu à une attestation de sécurité ou à un avis de sécurité), toutes les informations pertinentes sont discutées collégialement à l'ANS avec tous les services concernés. Ce n'est que dans le cadre des procédures de recours qu'une note complète et contextualisée est établie et envoyée à l'ANS.

Une autre méthode de travail est utilisée pour traiter des questions posées dans le cadre d'une demande de naturalisation et des demandes émanant de l'OE ou du CGRA. Si, dans ces cas-là, il est question d'un *'hit'*, la demande est alors transmise au service d'analyse (géographique) compétent, qui évalue les informations disponibles dans la banque de données et rédige une réponse sous la forme d'une note contextualisée. En 2017, ce sont plusieurs milliers de dossiers qui ont été traités par les services d'analyse.[13] Dans certains cas, il a été décidé qu'une enquête complémentaire menée par les services extérieurs qui sont responsables de la collecte des informations, s'imposait (par ex. lorsque les informations disponibles sur une personne sont incertaines (non confirmées) ou ne sont pas actualisées). Ce genre d'enquête complémentaire ne constituait pas une priorité pour les services de collecte.

Les processus susmentionnés n'étaient décrits ni dans des notes de service, ni dans un vademecum.

Il est ressorti de l'enquête du Comité que le Service VVS réalise des screenings sans indication claire de la base légale (*supra*). Dans certains cas, la finalité de la demande n'est pas précisée : s'agit-il d'un screening de sécurité ou d'un contrôle dans la banque de données de la VSSE ?[14] À cet égard, la VSSE se référait systématiquement à l'article 19 L.R&S. S'il peut être utile et conseillé de consulter les services belges à propos des résidents belges pour lesquels un accès à des installations d'instances internationales établies en Belgique devrait éventuellement être autorisé, un mandat légal est requis à cet effet.[15]

Enfin, le Comité a pu constater que dans le cadre de la réalisation des screenings, la relation avec les services partenaires étrangers était défaillante.

---

13 Au moment de l'enquête, la VSSE n'utilisait aucun critère pour la formulation des réponses dans le cadre des screenings. Chaque service (VVS ou service d'analyse) rédigeait une réponse à sa discrétion.

14 Par exemple, les screenings effectués à la demande du service de sécurité de l'OTAN, le Nato Office of Security (NOS). Il s'agit ici du screening de personnes auxquelles l'accès aux installations est autorisé ou non.

15 De tels screenings ont été rendus possibles par la Loi de février 2018. Avant que des vérifications de sécurité puissent être demandées pour une instance internationale, un accord doit notamment être conclu entre l'autorité administrative compétente et l'instance concernée, et une analyse de la menace, de risque et d'impact doit être effectuée (Loi du 23 février 2018 portant modification de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité).

La charge de travail élevée ne permet pas d'interroger des autorités étrangères. Ceci compromet la position d'information de la VSSE, et des personnes d'origine étrangère risquent de passer à travers les mailles du filet dans le cadre des vérifications de sécurité. Inversement, le Service VVS répond à des questions de services de renseignement étrangers, alors qu'ici non plus, la base légale n'est pas claire.

I.1.2.4. Moyens

La VSSE estime que la responsabilité du service dans le cadre d'un screening pour d'autres autorités de sécurité se limite à vérifier si l'entité (la personne) est connue dans sa propre documentation (banque de données interne).

La VSSE utilise une seule banque de données centralisée. Au cours de l'enquête, il est apparu clairement que les incomplétudes observées par le Service VVS dans cette banque de données de la VSSE n'étaient pas corrigées.[16] Toutefois, lors du développement de cette banque de données, il n'a peu (voire pas) été tenu compte à l'époque de l'existence du Service VVS et de sa mission. Résultat : la structure de la banque de données permet certes au Service VVS de constituer sa propre documentation (par ex. des rapports internes de réunions de concertation avec des partenaires externes) et de l'introduire dans la banque de données, mais ces documents ne sont visibles que par les collaborateurs de ce service.

Quant aux moyens IT, des améliorations devront également être apportées dans la structure de la banque de données en ce qui concerne les screenings. Ces améliorations s'inscrivent toutefois dans la réforme plus générale du service, dont le timing n'était pas encore clairement défini.

Comme suite à l'adaptation de la législation en matière de vérifications de sécurité, il est prévu que 25 % des frais[17] qui incomberaient au requérant pour une attestation de sécurité seront versés au(x) service(s) qui doi(ven)t procéder à la vérification. Ces crédits peuvent être investis dans des outils supplémentaires.

---

16 Il a été dit que le motif de l'ouverture de cette enquête de contrôle, à savoir la plainte d'une personne qui a reçu un avis négatif dans le cadre d'une procédure de naturalisation, est l'utilisation d'informations qui n'ont pas pu être complètement prouvées, ou du moins qui n'étaient pas actualisées. Le fait que des identités incomplètes ou erronées sont souvent reprises dans la banque de données de la VSSE accroît le risque de 'faux' résultats dans le cadre des vérifications de sécurité. Ne pas compléter les informations erronées est contraire aux principes de protection des données à caractère personnel.

17 A.R. du 8 mai 2018 fixant les montants des rétributions dues pour les habilitations de sécurité, pour les attestations de sécurité et les avis de sécurité délivrés par l'Autorité nationale de sécurité et pour les attestations de sécurité délivrées par l'Agence fédérale de Contrôle nucléaire, ainsi que les clés de répartition visées à l'article 22*septies*, alinéas 6 et 8, de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *M.B.* 1er juin 2018.

I.1.2.5. Plan d'amélioration

La VSSE considérait plusieurs possibilités d'amélioration en matière de screenings.

Une des améliorations les plus utiles et nécessaires est la création d'un système *'flagging'*, par lequel toutes les personnes qui sont connues dans la banque de données et qui sont ou ont été screenées sont désignées comme telles. Ceci permettrait aux services d'analyse et aux services extérieurs de reprendre dans une vérification de sécurité d'éventuelles nouvelles informations pertinentes concernant une personne et d'attirer l'attention du Service VVS.

En outre, le service verrait comme une évolution positive le fait qu'un accord soit trouvé avec les clients sur un *template* uniforme à utiliser pour les demandes.

Une autre piste d'amélioration est la création d'un portail IT pour saisir les demandes de vérifications de sécurité.

La VSSE ambitionne par ailleurs une meilleure harmonisation des screenings avec les besoins des 'clients'. Une concertation est d'ailleurs en cours avec les parquets d'Anvers et de Liège afin d'examiner comment mieux définir les renseignements qui sont pertinents dans le cadre des procédures d'acquisition de la nationalité.

Enfin, un vademecum est élaboré en vue de formaliser les procédures internes qu'il conviendra de suivre dans le cadre des screenings.

Le Comité permanent R juge souhaitable de développer ces initiatives pour d'autres bénéficiaires également.[18] Selon la VSSE, l'Autorité nationale de sécurité (ANS) pourrait jouer un rôle essentiel dans le lancement de telles initiatives d'amélioration.

I.1.2.6. Point d'attention particulier

L'enquête a une nouvelle fois montré l'absence de suivi actif et systématique dans le temps de la situation d'une personne pour laquelle un screening a été effectué. Cela comporte des risques, à commencer pour le service qui a demandé le screening et éventuellement pour une personne qui a été recrutée sur la base d'un screening favorable. Par exemple, un badge permettant d'accéder à des terrains d'un aéroport est délivré pour une période de cinq ans, ce qui est relativement long. Au cours de cette période de cinq ans, une nouvelle vérification sera effectuée si et seulement si l'intéressé est amené à exercer une nouvelle fonction.

---

[18] Le Comité permanent R a fait valoir à cet égard que les différentes dispositions réglementaires permettant de procéder à des screenings reprennent des éléments indiquant quelles informations sont pertinentes dans l'évaluation de la fiabilité d'une personne au vu de l'autorisation, de la licence, de la fonction, etc. Une meilleure connaissance de ces dispositions réglementaires est dès lors cruciale pour communiquer les informations correctes aux clients.

Ceci comporte naturellement aussi une dimension processuelle. En effet, au vu de la structure de la banque de données de la VSSE, le Service VVS n'est pas non plus automatiquement tenu au courant de nouvelles informations défavorables concernant une personne qui avait fait l'objet d'une vérification de sécurité dans le passé.[19]

I.1.3. LES SCREENINGS DE SÉCURITÉ AU SGRS

I.1.3.1. Organisation[20]

La Cellule Screenings, créée en 2015[21], est officiellement placée sous la responsabilité hiérarchique du Chef du *Collection Coordination & Information Requirement Management* (CCIRM), qui est responsable, au sein du SGRS, de l'enregistrement et de la diffusion de toutes les informations entrantes et sortantes. Cette cellule n'est composée que de quelques sous-officiers et se trouve dans une situation ambiguë. Les collaborateurs ont en effet comme supérieur administratif le Chef de la Direction S(ecurity) et comme supérieur fonctionnel, le Chef du CCIRM. Ils ne disposent apparemment pas d'un point de contact permanent dans la hiérarchie en cas de questions, de problèmes, ou lorsqu'une décision doit être prise.

La Cellule Screenings est apparue très autonome. Il n'y a en effet aucune supervision de la hiérarchie en termes de fonctionnement, et la Cellule reçoit peu d'instructions (voire aucune) de la hiérarchie. Cette situation ambiguë soulève également des questions sur la responsabilité finale au sein du SGRS et sur le contrôle (de qualité) interne.

En 2018, l'effectif de la cellule précitée était insuffisant pour accomplir les tâches. Entre-temps, l'augmentation continue du nombre de demandes de vérifications a généré un retard dans le traitement. Le tableau organique (TO) prévoyait un renforcement de la Cellule. Ces renforts, qui ne sont pas encore arrivés, n'étaient prévu que pour faire face à la charge de travail actuelle. C'était sans compter la charge de travail toujours plus lourde qui s'annonce.

---

19 Un système de '*flagging*' peut apporter une solution.

20 L'enquête portait sur la période s'étendant de janvier à avril 2018 et ne tenait pas compte de la création du *Defence Intelligence and Security Coordination Centre* (DISCC) au sein de la structure du SGRS. Ce DISCC s'est vu attribuer des compétences élargies. Il est devenu, entre autres, le *single point of entry & exit*, qui enregistre et diffuse à la Direction compétente toutes les informations entrantes et sortantes. Depuis juin 2018, la Cellule Screenings est placée sous la responsabilité administrative et fonctionnelle du Chef du DISCC. Le DISCC regroupe le CCIRM, le CTR (le centre de communication du SGRS) et un secrétariat central.

21 Avant mai 2015, les screenings étaient traités par un seul membre du personnel de la Cellule Banque de données au niveau du SGRS. Cette section fait partie du pilier Appui aux Opérations de la Direction CI.

Comme déjà indiqué, le fonctionnement de ladite cellule au sein du SGRS a plutôt évolué de manière 'organique', sans directives claires de la hiérarchie. Les collaborateurs de la Cellule n'ont jamais reçu de formation spécifique dans le domaine juridique ni pour l'utilisation des moyens techniques disponibles. Ils ont appris le métier 'sur le tas', par la pratique quotidienne.

Enfin, le Comité permanent R a pu constater qu'au SGRS, il n'y a pas d'enregistrement ni de gestion centralisée des (réponses aux) demandes de vérification. Aucun suivi n'est donc possible, ce qui comporte des risques, en premier lieu pour le service qui a demandé le screening et éventuellement pour une personne qui a été recrutée sur la base d'un screening favorable.

I.1.3.2. Données quantitatives

Le Comité permanent R a constaté que le SGRS ne tient pas de statistiques intégrales sur les vérifications de sécurité et les screenings réalisés par le service. Il est donc impossible de se faire une opinion sur les principaux résultats du service, ni sur les besoins du service en termes de moyens pour mener à bien sa mission. Or, l'absence de vue sur les résultats et les moyens nécessaires complique l'élaboration d'une stratégie et d'une planification adéquate.

À l'occasion de cette enquête de contrôle et de la demande de transmission de données chiffrées, la Cellule Screenings du SGRS a pris l'initiative de demander des statistiques au service d'appui J6 (ICT). Il en a résulté une série de chiffres concernant le nombre de recherches effectuées via un programme de recherche dans une banque de données du SGRS, à savoir la banque de données de la Direction CI. Le nombre de recherches effectuées correspondrait *grosso modo* au nombre d'entités à vérifier. Ce chiffre élevé ne s'explique pas au regard des chiffres de la VSSE.

Lors de la création de la Cellule Screenings en 2015, le nombre de demandes à traiter était tout à fait gérable. Mais, depuis fin 2016, il n'a cessé d'augmenter, ce qui a retardé le traitement des demandes et ce qui explique que certains types de screenings doivent être laissés de côté. La Cellule Screenings déterminait elle-même – à sa discrétion – quels screenings étaient prioritaires.

I.1.3.3. Processus de travail

Tous types de screenings

Les demandes de screenings parviennent à la Cellule Screenings par courriel et, à juste titre, via deux canaux : le réseau classifié (via le CCIRM) et le réseau non classifié (envoi direct du 'client').[22]

[22] La Cellule Screenings a déjà proposé (au CCIRM) de simplifier la procédure et de veiller à ce que toutes les demandes lui soient transmises par un seul et même canal, à savoir via le CCIRM.

Le rôle de cette cellule se limite à vérifier si l'entité (la personne) figure ou non dans certaines banques de données du SGRS en premier lieu en effectuant une recherche via un programme de recherche. Si aucune information relative à la personne concernée n'est disponible dans les banques de données consultées du SGRS, le service envoie directement, par courriel, une réponse *'nothing significant to report'* (NSTR) à l'autorité requérante/le client. En cas de *'hit'* positif, il est indiqué dans quelle Direction et dans quelle banque de données les informations relatives à l'entité sont disponibles. Par la suite, la cellule peut encore effectuer une recherche complémentaire dans la banque de données en question. Pour avoir un aperçu du contenu des informations disponibles, la Cellule Screenings s'adresse toutefois au service (d'analyse) compétent qui a introduit les informations dans la banque de données et qui en assure le traitement. Lorsque des informations alarmantes apparaissent dans le cadre de la vérification de sécurité, les services d'analyse les transmettent sous la forme d'une note à l'ANS ou à l'AFCN, selon le cas. Lorsqu'il s'agit d'éléments moins graves, les informations sont envoyées par courriel à la cellule précitée pour une concertation orale avec l'ANS.

Les services d'analyse du SGRS se disent conscients que les informations qui sont communiquées sur une personne peuvent être lourdes de conséquences pour la personne elle-même. Une certaine retenue et le sens de la nuance sont de mise dans le cadre de la communication d'informations. Le service affirme que les informations transmises ne portent en principe que sur la personne qui fait l'objet de la vérification de sécurité. Dans certains cas, des informations pertinentes sont également transmises sur l'entourage immédiat de l'intéressé à des fins de contextualisation. Le Comité n'a pas constaté l'existence de critères uniformes dans les services d'analyse définissant quelles informations sont communiquées et sous quelle forme elles le sont.[23] La transmission ou non de certaines informations dépend de l'évaluation de l'analyste qui traite le dossier.

Une exception : les candidats militaires

La procédure décrite ci-dessus s'applique à tous les types de screenings, à une exception près. Dans le cas d'une vérification effectuée dans le cadre d'un avis de sécurité pour un candidat militaire, le 'client' est un service de la Défense, à savoir la Direction générale Human Resources (DGHR). Dans ce cas, c'est le Service Habilitations de sécurité (Habilitations) de la Direction S du SGRS qui coordonne la formulation de l'avis de sécurité et qui, dans cette optique, interroge également la VSSE et la Police fédérale.

---

[23] Concernant la définition de critères communs, il a été suggéré de mener une réflexion avec les autres services concernés, tels que la VSSE, la Police fédérale et l'OCAM, et ce d'autant que la nouvelle législation de février 2018 prévoyait également que les services devraient établir des analyses de la menace dans le cadre des vérifications de sécurité.

La Cellule Screenings reçoit la demande de vérification de sécurité des candidats militaires – sous la forme d'une liste de noms – directement de la DGHR et via le Service Habilitations. Ce n'est qu'au moment où le Service Habilitations de sécurité donne son feu vert que la Cellule procède aux vérifications dans les banques de données. D'éventuels '*hits*' sont communiqués à ce Service Habilitations. Lorsque le SGRS intervient comme autorité de sécurité, la compétence de décision en la matière était déléguée par le Chef du SGRS au Chef de la Direction S(ecurity).

Hormis pour des faits liés à la possession, l'usage et le commerce de stupéfiants, aucun critère formel n'a été fixé par le SGRS pour déterminer sur quelle base un candidat militaire reçoit un avis positif ou négatif. Dans la pratique, c'est l'éventuelle gravité des faits qui est examinée, et il est tenu compte du fait que l'intéressé était mineur ou majeur au moment des faits. Un critère supplémentaire est le caractère récent des éventuels faits négatifs. Dans le cas d'éléments moins graves, la vérification des informations porte seulement sur les deux à trois dernières années.

En cas d'informations défavorables concernant le candidat militaire, une décision collégiale est prise *in fine* par le Chef de la Direction S et deux autres officiers du Service Habilitations.[24]

Absence de base légale

L'enquête a montré qu'il est souvent demandé à la Cellule Screenings de procéder à des screenings en l'absence d'une base légale claire. Il s'agit, par exemple, de demandes émanant de l'OCAM, du Service DJSoc Terro de la Police fédérale, du Service External Relations Office (ERO) du SGRS même (par ex. concernant les Attachés de défense étrangers accrédités en Belgique), la Cellule de traitement des informations financière (CTIF), le NATO Office of Security (NOS), Europol/Interpol, etc.

À la question de savoir qui au sein du SGRS décide quel type de recherches doit être effectué dans les banques de données par la Cellule Screening, il n'y a pas eu de réponse satisfaisante. La plupart du temps, il s'agit de messages entrants qui sont simplement transmis par le CCIRM à la Cellule Screenings pour y être traités. En d'autres termes, il n'y a aucune vérification de la base légale de la demande d'informations.

Il est apparu que les membres de la Cellule Screenings n'avaient qu'une connaissance très limitée de la base légale de leur travail. La Cellule n'était pas non plus systématiquement tenue informée par la hiérarchie ou par le service

[24] Une décision négative est prise dans environ 5 % des cas. Selon les estimations, il y a aussi 15 % de 'cas douteux', pour lesquels des informations défavorables existent sur le candidat, mais où celui-ci a été autorisé à devenir militaire et où il a été demandé à l'officier de sécurité de sa future unité de garder un œil attentif sur lui pendant les premiers mois de son affectation.

juridique du SGRS des adaptations de la loi ou des nouvelles lois pertinentes pour l'accomplissement de leurs tâches, ni des protocoles d'accord conclus avec des partenaires. Ils devaient eux-mêmes rechercher ce genre d'informations.

Cependant, la Cellule Screenings reçoit systématiquement les décisions de l'Organe de recours, mais elle ne les traite pas. Autrement dit, ces décisions ne font l'objet d'aucune analyse. La Cellule considère que cela ne fait pas partie de sa mission.[25]

En gardant à l'esprit la création du DISCC (voir *infra*), une réflexion a été initiée sur la manière dont la Cellule Screening pourrait mieux fonctionner à l'avenir. Cette réflexion devrait aboutir à l'élaboration de procédures de travail, qui seraient également décrites à un stade ultérieur.

I.1.3.4. Moyens

Les enquêtes de contrôle effectuées dans le passé par le Comité permanent R sur le fonctionnement du SGRS avaient déjà montré que différentes banques de données sont utilisées au sein de ce service. À elle seule, la Direction S(ecurity) utilisait au moins cinq banques de données différentes. Restent les autres directions (I, CI) qui disposaient de leurs propres banques de données. Il en résulte que le travail de la Cellule Screening requérait beaucoup de temps et que les screenings étaient très difficiles à gérer de manière centralisée au sein du SGRS. À cet égard, le Comité a également attiré l'attention sur le point faible qui avait été constaté[26], à savoir un retard dans la saisie des informations pertinentes dans la banque de données du service précité. Ici aussi, certains renseignements pertinents disponibles – et, dans ce cas, les renseignements les plus récents – pouvaient ne pas être retrouvés lors d'un screening, avec toutes les conséquences potentielles pour la personne concernée et pour le service qui avait demandé le screening. Ce n'était pas non plus un gage de fiabilité du service vis-à-vis de ses partenaires.

Outre le problème d'effectif, le manque de moyens techniques performants était considéré par les membres du personnel de la Cellule Screenings comme un obstacle à l'accomplissement de leur mission. La Cellule Screenings devrait pouvoir utiliser un nouveau moteur de recherche, qui permettra d'effectuer des recherches à la fois dans les banques de données et directement dans les documents sauvegardés dans les fichiers de la Direction I. Cela s'inscrit dans l'amélioration de la gestion de l'information en général au SGRS.

Les membres de la Cellule Screenings n'étaient pas au courant d'initiatives qui auraient été prises avec des partenaires externes sur l'utilisation de moyens

---

25 Le fait que les décisions de l'Organe de recours ne parviennent qu'à la Cellule Screenings, qui n'en fait rien ou ne peut rien en faire, a déjà été abordé par la Cellule avec la hiérarchie, sans qu'aucune action n'ait été entreprise à ce jour.

26 'Enquête de contrôle sur le fonctionnement de la Direction Counterintelligence (CI) du SGRS'.

technologiques communs. Quant aux banques de données externes, la cellule précitée n'a accès qu'au Registre national, et encore seul un collaborateur de la Cellule peut y accéder. Elle indique que l'accès à d'autres banques de données externes n'est pas nécessaire.

Un autre problème réside dans le fait que les demandes parviennent à la Cellule Screenings dans toutes sortes de formats (listes Excel, documents pdf, etc.). Autrement dit, il n'y a pas de document standardisé pour les demandes de vérifications de sécurité.

I.2. ANALYSE DU FONCTIONNEMENT DE LA SECTION HUMINT DU SERVICE DE RENSEIGNEMENT MILITAIRE

Le recours à des sources ouvertes (*human intelligence* ou HUMINT) est un moyen essentiel pour les services de renseignement et de sécurité dans le cadre de leur mission de collecte d'informations. La Section HUMINT de la Division Intelligence (Section I/H, en abrégé) a pour mission de créer des réseaux de sources et d'informateurs pour permettre au SGRS de collecter des renseignements sur des phénomènes étrangers.

Le Comité avait déjà traité une plainte spécifique portant sur le fonctionnement de cette section, en particulier sur l'exécution de certaines missions menées à l'étranger.[27] En effet, la Section I/H dispose d'informateurs à l'étranger pour recueillir des informations sur des matières entrant dans la sphère d'intérêt du service de renseignement militaire. Plusieurs dysfonctionnements étaient soulevés dans cette plainte, notamment la description de la mission, la gestion stratégique, les compétences et la qualité du personnel ainsi que le *tradecraft* étaient considérés comme critiques.[28]

Dans le prolongement de cette enquête, le Comité a décidé, fin avril 2018, d'ouvrir une enquête de contrôle sur le fonctionnement de la Section I/H. Le rapport a été finalisé en novembre 2019.

I.2.1. HUMAN INTELLIGENCE

L'article 18 L.R&S stipule que *'les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, avoir recours à des sources humaines*

---

27 La plainte a fait simultanément l'objet d'une enquête de contrôle et d'une enquête judiciaire menée par le Parquet fédéral. Voir COMITÉ PERMANENT R, *Rapport d'activités 2017*, 4-11 ('II.1. Une plainte concernant trois opérations du SGRS').

28 La question de la Section I/H a également été abordée dans l'enquête sur le fonctionnement de la Direction Counterintelligence (I.6). En effet, il était évident qu'en l'absence de directives et d'accords clairs, les deux services risquaient de travailler chacun de leur côté.

pour la collecte de données en rapport avec des événements, des objets, des groupements et des personnes physiques ou morales présentant un intérêt pour l'exercice de leurs missions, conformément aux directives[29] *du Conseil national de sécurité'*. Autrement dit, toute personne qui fournit des informations à un service de renseignement ou de sécurité, peu importe le moyen de communication, et qui ne relève pas non plus du champ d'application d'autres articles de la L.R&S[30], est considérée comme une source humaine. Il s'agit de personnes aux profils très variés, qui peuvent être vues une fois pour un débriefing, sporadiquement, ou encore sur une base très régulière, sur de courtes ou longues périodes, indépendamment de leur position d'information et de la sensibilité des informations qu'elles transmettent. Le recours à de telles sources constitue une méthode ordinaire de recueil de données.[31]

L'OTAN définit à son tour le HUMINT comme *"a category of intelligence derived from information collected and provided by human sources"*[32] et le subdivise en trois catégories.[33] Le HUMINT est qualifié d''ouvert' lorsque la collecte est effectuée via des sources qui ne cachent pas leur véritable rôle. Lorsque la collecte s'effectue via des sources humaines qui cachent leur véritable fonction et leur véritable but, le HUMINT est considéré comme 'discret'. Enfin, la notion de HUMINT 'clandestin' est attribuée à une catégorie d'activités menées en secret, c'est-à-dire en vue de protéger les sources.

I.2.2. ANALYSE DE LA SECTION I/H DU SGRS

I.2.2.1. Organe de collecte avec un déficit en personnel

La Section I/H – qui ne détient pas le monopole sur la gestion des sources humaines au sein du service de renseignement militaire – ne représente qu'une petite partie de l'ensemble de l'effectif de la Direction Intelligence. En plus d'un roulement important du personnel (rotation), le Comité a pu constater, pour les années 2017 et 2018, une perte nette de 25 % du personnel (départs). Le Comité a

29 En mars 2019, le Conseil national de sécurité (CNS) a validé le projet de directive établi conjointement par la VSSE et le SGRS. Cette validation permet de conférer un cadre complet au traitement des sources ouvertes. Ce cadre se décline en quatre niveaux : la Loi organique, le Plan Stratégique National du Renseignement (PSNR), la directive du CNS et les instructions internes.

30 Comme par exemple l'article 14 L.R&S, qui précise que les services peuvent faire appel aux autorités judiciaires, aux fonctionnaires et aux agents des services publics dans le cadre de leur mission de renseignement.

31 En d'autres termes, sur la base des principes de subsidiarité et de proportionnalité, cette méthode doit avoir la priorité sur les méthodes spécifiques ou exceptionnelles (lesdites 'MRD').

32 NATO, *Glossary of terms and definitions (AAP-6)*, ed. 2015.

33 NATO, *Allied Joint Publication (AJP) 2.3. and STANAG 2578*.

souligné les risques de discontinuité et de perte de connaissances engendrés par la rotation et les départs. En janvier 2019, le Comité permanent R a constaté au sein de la Section I/H un déficit en personnel de 22 % par rapport au tableau organique (TO). En d'autres termes, la situation du personnel est précaire.

La Section I/H a néanmoins développé un réseau de centaines de sources ouvertes réparties à travers le monde. Environ la moitié de ces sources fournit des renseignements sur un ou deux pays seulement ; une source livre des renseignements sur cinq pays en moyenne.

I.2.2.2. Orientation depuis différents niveaux

Pour les activités HUMINT à l'étranger, le Plan Stratégique National du Renseignement prévoit que le SGRS, tout comme la VSSE, établit des listes de pays dans lesquels ils sont actifs en matière de HUMINT.[34] Ce plan détermine également la manière dont la gestion de leurs sources doit être communiquée.

La Direction Intelligence du SGRS rédige à son tour tous les trois ans un Plan directeur de renseignement. Ce plan doit orienter le cycle du renseignement et est actualisé chaque année.[35] C'est sur cette base que les actions et les priorités spécifiques de la collecte et de l'analyse sont définies pour les sections, y compris donc pour la Section I/H. En outre, un '*Intel Focus*' reprenant les objectifs opérationnels est rédigé.

Enfin, il est demandé à chaque organe de collecte sur le terrain, y compris la Section I/H, de compléter des plans de collecte (les '*Intelligence Collection Plan*s ou ICP). Les ICP pour la Section I/H contiennent des questions concrètes à l'attention des sources via lesquelles des informations peuvent être recueillies sur diverses menaces. Le Comité a constaté au sein des différents ICP une grande variété de thèmes spécifiques, ce qui n'est pas illogique compte tenu de la diversité des contextes géopolitiques. Par contre, le Comité a relevé que les différents ICP des autres organes de collecte de la Direction Intelligence ne présentent pas une structure similaire et que les périodes sur lesquelles portent ces plans ne sont pas systématiquement précisées. Le Comité a estimé nécessaire de standardiser et de synchroniser les plans de collecte, ainsi que d'éviter les conflits en matière de gestion des sources par les différents services.

Un aperçu des sources a montré que certains objectifs stratégiques définis dans le Plan directeur de renseignement ne sont pas pleinement rencontrés par la Section I/H et que des informations étaient recueillies sur certains pays alors qu'ils ne présentent pas *ab initio* un intérêt stratégique direct et immédiat pour la

---

34 Quatre catégories de pays sont établies sur la base de ces listes : les pays d'intérêt exclusif du SGRS, les pays d'intérêt exclusif de la VSSE, les pays d'intérêt commun et les pays non prioritaires.

35 Le Comité n'a pu constater que peu de modifications entre le 'Plan directeur de renseignement 2013-2014' et le 'Plan directeur de renseignement 2015-2018'. Un certain nombre d'objectifs stratégiques se sont déplacés de l'une à l'autre priorité de renseignement en raison de la modification du contexte géopolitique.

Défense belge. Selon le SGRS, ce constat doit être vu à travers le prisme du fonctionnement global de la Direction Intelligence et du SGRS. Le Section I/H ne fournit qu'une partie de l'information relative à chacun des pays visés. En outre, une information non prioritaire pour les intérêts de la Belgique peut s'avérer d'un intérêt particulier pour un service de renseignement partenaire et, de ce fait, alimenter l'échange international de renseignement. Là où la Belgique a peut-être plus de difficultés à recruter et à gérer des sources pour un pays qui suscite son intérêt, elle peut malgré tout bénéficier de la réciprocité dans les échanges internationaux.[36]

I.2.2.3. La fiabilité de la source et la crédibilité des informations fournies

Le traitement des sources humaines constitue la tâche essentielle de la Section I/H. Il s'agit d'un processus de *spotting*, d'approche et d'évaluation (le recrutement) des sources, ensuite de traitement de leurs renseignements et, enfin, d'archivage des sources. La plupart de ces processus font l'objet de directives internes. En 2018, la nouvelle direction a toutefois décidé d'effectuer une révision globale des directives. Le Comité a pu constater qu'il n'existait pas encore de directive pour certains processus (par ex. l'archivage).

La fiabilité des sources humaines et la crédibilité des informations reçues doivent naturellement faire l'objet d'une évaluation périodique. Le système OTAN de cotation des sources et de l'information qu'elles récoltent est élaboré comme suit :

Reliability of the source		**Credibility of the information**	
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probably true
C	Fairly reliable	3	Possibly true
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged

Dès le début de son enquête, le Comité permanent R a dû constater que la fiabilité d'une part considérable des sources n'était pas établie.[37] Au cours de

[36] Enfin, le recrutement et la gestion d'une source représentent un investissement sur plusieurs années. La source qui n'a qu'un intérêt stratégique limité aujourd'hui peut s'avérer cruciale demain.

[37] La fiabilité de la source n'est établie que sur la base de ses performances antérieures. Elle n'affecte pas la crédibilité de l'information. Ainsi, une source non fiable pourrait très bien fournir une information dont la crédibilité pourrait être évaluée comme étant très haute. En revanche, la crédibilité des sources en général va affecter les choix qui seront opérés dans le cadre du plan de collecte. Un feedback entre l'analyste et le collecteur est nécessaire pour évaluer la source.

l'enquête, la Section I/H a lancé, avec succès, un processus pour rectifier la situation : toutes les sources ont été évaluées et, si nécessaire, réorientées, réactivées ou archivées.

Les informations obtenues via les sources humaines doivent également être évaluées. En deux ans (2017-2018), plusieurs milliers de bulletins d'information ont été produits.[38] Le Comité a pu constater que les services d'analyse ne donnaient pas de feedback formel pour une grande partie de ces bulletins d'information. Ce constat est inquiétant quant à la gestion du cycle de renseignement ; il est en effet essentiel que les services d'analyse puissent orienter utilement les services de collecte afin de tenter d'atteindre les objectifs de renseignement escomptés.

I.2.2.4. La gestion des dossiers des sources

Les dossiers des sources font l'objet d'une gestion administrative 'papier' et d'une gestion électronique. L'enquête a permis de détecter des problèmes de gestion administrative et de prendre des mesures en vue de corriger ces dysfonctionnements. Le Comité a néanmoins dû constater que des pièces étaient encore manquantes dans une série de dossiers (par ex. les documents de 'demande d'approche d'une source', de 'compte rendu de la phase d'approche', ou encore de 'rapport de recrutement').

I.3. LES ÉCHANGES DE DONNÉES À CARACTÈRE PERSONNEL SUR LES *FOREIGN TERRORIST FIGHTERS* AU NIVEAU INTERNATIONAL

I.3.1. CONTEXTUALISATION

En 2016 déjà, à l'occasion d'une réunion internationale à laquelle participaient plusieurs organes de contrôle européens[39], il a été décidé d'initier, dans tous les pays participants, une enquête de contrôle similaire portant sur la coopération internationale entre les différents services de renseignement en matière de lutte

---

38 À cet égard, tant l'analyse du contenu de ces bulletins d'information que l'évaluation de leur pertinence par rapport aux objectifs stratégiques ne font pas l'objet de la présente enquête.

39 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.

contre les *foreign terrorist fighters* (FTF[40]). L'idée était que chaque organe de contrôle étudie cette thématique de son point de vue et en fonction de sa compétence, tout en adoptant la même philosophie et certainement une approche commune.

Le volet belge consistait à avoir la vision la plus précise et complète possible des échanges d'informations bilatéraux ou internationaux, 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.

Sa finalité ultime était d'évaluer les échanges d'informations et, le cas échéant, de formuler des recommandations afin de les optimaliser. L'objectif était d'améliorer la position d'information des services concernés, sans pour autant éroder les droits des citoyens.

L'enquête menée par le Comité a été suspendue en raison d'autres missions urgentes – certainement après les attentats survenus en France et en Belgique – mais aussi en raison de l'interaction avec le projet international. Le Comité permanent R a alors décidé, en janvier 2019, de clôturer l'enquête avec un rapport final succinct et pas, comme c'est généralement le cas dans un rapport circonstancié reprenant des descriptions, des conclusions et des recommandations.

I.3.2. RÉSULTATS DE L'ENQUÊTE

L'enquête a démontré en premier lieu que les échanges internationaux de données sur les *foreign terrorist fighters* entre les services de renseignement se sont non seulement multipliés, certainement depuis 2015, mais ont également changé de nature. Alors qu'avant la problématique FTF, les échanges de données avaient surtout un caractère réactif et bilatéral, les échanges proactifs et multilatéraux n'ont cessé de gagner du terrain. La coopération au sein de ce que l'on appelle le Counter Terrorist Group (CTG)[41] en est un exemple. Ainsi, en 2016, après les attentats de Paris, une plateforme opérationnelle (ouverte officiellement début 2017) et une base de données commune ont été instaurées sous la présidence néerlandaise. Ces outils permettent d'échanger des informations sur des djihadistes (présumés). Cette évolution induisait également l'application du principe du '*need to share*' au niveau international entre les pays concernés. Son intérêt ne peut être sous-estimé, et cette coopération peut constituer la base

40 Tels que définis dans la Résolution 2178 des Nations Unies du 24 septembre 2014 : "*Individuals who travel to a State other than their State of residence or nationality for the purpose of perpetration, planning or preparation of, or participating in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict*".

41 Le CTG, créé après les attentats du 11 septembre 2001, est un groupe spécialisé émanant de l'organe de concertation informel composé essentiellement des pays de l'Union européenne.

d'une coopération générale et structurelle entre les services de renseignements européens.

Par ailleurs, des services de renseignement, militaires pour la plupart, ont créé une plateforme multilatérale afin de coordonner leurs activités et analyses SIGINT.

Il ressort des vérifications ponctuelles de messages échangés qui ont été effectuées par le Comité que ces communications étaient pertinentes, proportionnelles et conformes aux missions légales des services, mais qu'elles ont eu lieu en dehors du cadre des institutions internationales (UE, NU, etc.) ou d'accords officiels juridiquement contraignants (comme par ex. des conventions). Il y a néanmoins lieu de constater que l'exécution de la Directive du Conseil national de sécurité de septembre 2016 portant sur les relations avec les services de renseignement étrangers a pris un retard considérable.[42] Cette directive donne exécution à l'article 20 L.R&S qui régit la coopération avec des services étrangers.

Enfin, il a été souligné que la réglementation était rendue sans cesse plus complexe, en particulier au niveau international, et sur les jugements rendus par des tribunaux internationaux (*soft law*) mais aussi au niveau national. Ainsi, il convient d'examiner quelles méthodes de collecte sont compatibles avec le droit national ou avec les conventions internationales et de suivre rigoureusement les évolutions en matière de protection des données à caractère personnel.

I.4. LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT SUR LE PHYSICIEN NUCLÉAIRE PAKISTANAIS KAHN

Un article de presse[43] est paru à la mi-janvier 2018 sur le programme nucléaire de la Corée du Nord. Le programme d'armement nucléaire pakistanais y était notamment mentionné. L'article citait également (feu) le professeur Martin Brabers (KU Leuven) et Abdul Qadir Khan, un scientifique pakistanais qui a séjourné en Belgique à la fin des années 60 et au début des années 70 et qui est considéré comme le père de la bombe atomique pakistanaise.

---

42 Le 26 septembre 2016, les ministres de la Justice et de la Défense ont soumis au Conseil national de sécurité, dans une note, la 'Directive concernant les relations des services de renseignement belges avec les services de renseignement étrangers', 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.

43 M. RABAEY, *De Morgen*, 13 janvier 2018 ('De Belgische bommen van Kim Jong-un'). Il y est fait amplement référence à Luc BARBÉ (L. BARBÉ, *België en de bom. De rol van België in de proliferatie van kernwapens*, juin 2012), qui plaide en faveur d'une enquête scientifique élargie et indépendante au sein des milieux académiques et de la VSSE sur le secteur nucléaire belge.

Une question s'est notamment posée, à savoir si les services de renseignement belges avaient suivi cette problématique à l'époque. La Commission de suivi de la Chambre des représentants a chargé la Comité d'étudier la problématique. Début juillet, l'enquête a été initiée et intitulée *'enquête de contrôle sur la position d'information des services de renseignement sur un scientifique pakistanais, actif dans le milieu académique belge, et sur ses connaissances en matière de haute technologie acquises sur les armes de destruction massive, qui ont finalement été utilisées pour développer des armes nucléaires au Pakistan*".[44]

I.4.1. LE VOLET BELGE DU DOSSIER KAHN

Abdul Qadir Khan a joué un rôle important dans le développement du programme nucléaire pakistanais. L'intéressé a étudié et travaillé en Europe entre 1961 et 1975, où il a accumulé des connaissances qui ont peut-être été utilisées par la suite pour développer la bombe atomique pakistanaise. Khan a essentiellement séjourné aux Pays-Bas[45], mais il a étudié en Belgique à partir de 1968. En 1972, il a obtenu un doctorat en sciences naturelles à la KU Leuven, et ce, sous le mentorat du Prof. Brabers.[46]

L'enquête de contrôle s'est concentrée sur le volet belge du dossier Khan et sur la question de savoir si, au cours de cette période, les services de renseignement belges se sont intéressés à la présence de Khan en Belgique et à l'éventuelle menace qu'il pouvait représenter en termes de diffusion de la technologie utilisée pour développer des armes de destruction massive.

I.4.2. LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT

En ce qui concerne la VSSE, le suivi de Khan et des personnes ou des entités qui y sont associées a été opéré sous l'angle des menaces de prolifération et d'espionnage. En outre, dans la mesure où la technologie nucléaire devait

---

44 L'enquête a été finalisée début 2019.

45 En 1980, un rapport d'enquête a été établi au sein de la Seconde Chambre néerlandaise sur l'affaire Kahn ('*De Zaak KHAN*, Tweede Kamer 1979–1980, Bijzondere Commissie Ter Beek, Kamerstuknummer 16082'). En 1983, Khan est condamné aux Pays-Bas pour espionnage (pour des faits remontant à 1974 et 1975), mais en 1985, sa peine est annulée en appel.

46 De nombreux ouvrages belges et internationaux ont été consacrés à l'intéressé/aux intéressés (L. BARBÉ, *België en de bom. De rol van België in de proliferatie van kernwapens*, juin 2012 ; F. DOUGLAS et C. COLLINS, *The Nuclear Jihadist* New York, Twelve, 2007 ; C. COLLINS et F. DOUGLAS, *De Khan-code. Spionage, falende inlichtingendiensten en de handel in atoomgeheimen*, Balans, 2011, etc.).

(pouvoir) être utilisée pour la fabrication et la diffusion d'armes nucléaires, le service de renseignement militaire pouvait, au moment où les faits se sont déroulés, s'appuyer sur un socle de compétences suffisant pour suivre cette problématique. Par conséquent, le Comité permanent R peut conclure que dès avant l'élaboration de la Loi de 1998, tant la VSSE que le SGRS étaient compétents pour suivre la problématique.[47]

I.4.2.1. La VSSE

Au cours de la période 1979-1996 (et donc après le départ de Khan), la VSSE a rassemblé environ 100 documents sur Khan et sur le Prof. Brabers, provenant essentiellement de sources ouvertes. En outre, la VSSE a reçu plus de 50 documents de ses correspondants. Elle a établi environ 40 rapports, en plus des 20 notes destinées aux correspondants belges ou étrangers.

À partir de 1996 (et donc après le virage informatique au sein de la VSSE), on a pu constater qu'une vingtaine de rapports d'enquête (OR) avaient été établis.

L'enquête a révélé une nette augmentation des échanges d'informations à compter de 2004. Il s'agissait de rapports d'information établis par les services extérieurs de la VSSE. Il importe de souligner que ces rapports portaient essentiellement sur la problématique de la prolifération au Pakistan, rapports dans lesquels le nom de Khan y était bien entendu abondamment cité. Une vingtaine de notes ont été envoyées aux autorités politiques fédérales et/ou régionales ; plusieurs notes de synthèse étaient destinées à la direction de la VSSE.[48]

La VSSE a signalé que rien n'indiquait que le Prof. Barbers aurait joué un rôle dans le réseau d'affaires de Khan ni n'aurait contribué activement au développement de la bombe atomique pakistanaise. Il n'y a cependant pas eu de suivi actif et régulier des activités et des contacts du Prof. Brabers.

---

47 Dans les travaux préparatoires de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité, et plus précisément lors des discussions relatives aux missions des services de renseignement et à leur rôle dans le cadre du potentiel économique et scientifique, il était fait référence de manière explicite au dossier Khan : *"[…] L'espionnage scientifique et économique est en développement. Il ne s'agit pas cependant d'être au service d'une entreprise, mais il s'agit tout de même de savoir quels sont les éléments qui encadrent l'activité de cette entreprise et surtout par qui elle peut être contrée à l'extérieur (voir stagiaires pakistanais – compétence de Monsieur Khan en matière nucléaire civile* [nous soulignons]). *Bien connaître le potentiel économique et scientifique et aider à le développer peut donc être très utile. Ceci constitue sûrement le volet le plus moderne de la fonction des services de renseignement à l'heure actuelle".* Cf. Projet de loi organique des services de renseignement et de sécurité, *Doc. parl.* Sénat 1997-98, n° 1-758/10, 101.

48 Quelques notes seulement ont été communiquées à des correspondants étrangers au cours des dix dernières années. La VSSE a fait remarquer qu'en ce qui la concerne, c'est cohérent vu la baisse de l'intérêt pour Khan et pour ce qui était son réseau d'affaires (à cette époque).

I.4.2.2. Le SGRS

Le SGRS ne disposait d'aucune information spécifique dans ses différentes banques de données sur l'atomiste pakistanais Khan, ni sur le Prof. Brabers, pour les années 60 et 70. Selon le service, la recherche sur le nom de Khan pour cette période-là a généré de nombreux résultats, mais ceux-ci n'ont pas été traités dans sa réponse puisqu'ils ne portaient pas sur la période au cours de laquelle Khan avait travaillé en Europe.

I.4.3. CONCLUSIONS

Le 'volet belge' de l'affaire Kahn se situe dans la période 1968-1972. À ce moment-là, les deux services de renseignement avaient une mission générale, mais pas toujours de manière explicite, concernant la présente thématique.

Une autre question est de savoir si les services belges avaient un motif clair pour suivre Khan. En effet, le séjour de Khan en Belgique a été relativement court. Il n'attirait manifestement pas l'attention et, qui plus est, il n'était pas le seul étudiant pakistanais actif dans le domaine de la technologie nucléaire.[49] Khan a acquis la plupart de ses connaissances aux Pays-Bas (à partir de 1972), lorsqu'après son doctorat, il a travaillé pour un laboratoire de recherche. Il ressort de l'enquête néerlandaise (*supra*) qu'il y a là aussi dérobé des données. Ce n'est qu'en 1979 que la VSSE a appris qu'il était dans les radars d'un service partenaire, alors que cela faisait déjà sept ans qu'il avait quitté la Belgique.

Ce n'est qu'en 1987 que le Professeur néerlandais Brabers, qui enseignait non seulement à l'université de Tilburg mais aussi à la KU Leuven, a attiré l'attention de la VSSE. Pas le moindre fait relatif à une aide à la prolifération ou à l'espionnage n'a jamais été signalé à son égard, ni aucune preuve avancée.

Le Comité permanent R a estimé que vu les informations ou indications disponibles, ni Khan ni le Prof. Brabers n'aurait dû attirer d'emblée l'attention des services de renseignement belges, ou n'aurait dû être considéré comme une cible importante (et encore moins prioritaire). Avec le recul, on pourrait affirmer que quiconque était impliqué dans une recherche dans le domaine nucléaire méritait assurément d'être suivi par les services de renseignement. Comme l'a signalé la VSSE, cette problématique attirait davantage l'attention depuis les années 80.

En guise d'évaluation finale, le Comité permanent R a considéré que le suivi non prioritaire par les services de renseignement belges, tant de Khan lors de son séjour en Belgique que du Prof. Brabers, n'était pas dénué de fondement, compte tenu du cadre temporel et des données connues à l'époque.

---

[49] En outre, le domaine dans lequel il menait ses recherches (la métallurgie) n'était pas directement lié à la recherche dans le domaine nucléaire.

I.5. CARLES PUIGDEMONT ET LES ÉVENTUELLES ACTIVITÉS MENÉES PAR DES SERVICES DE RENSEIGNEMENT ÉTRANGERS EN BELGIQUE

I.5.1. CONTEXTUALISATION

Le 27 octobre 2017, Carles Puigdemont, ancien président du gouvernement régional de Catalogne et vecteur de la déclaration d'indépendance adoptée par le Parlement catalan, a été destitué de ses fonctions par les institutions espagnoles. Il s'est alors réfugié en Belgique. Début novembre 2017, il a fait l'objet d'un mandat d'arrêt européen délivré par les autorités judiciaires espagnoles.

Le 9 février 2018, M. Puigdemont a déposé plainte auprès des autorités belges pour violation de la vie privée. En effet, quelques jours auparavant, une balise de géolocalisation avait été retrouvée sous le véhicule.[50] Après avoir détecté ce dispositif, les conseillers de M. Puigdemont avaient alerté la zone de police locale de Waterloo. Selon des sources ouvertes, préalablement à la découverte des balises de géolocalisation, les chauffeurs de M. Puigdemont s'étaient sentis observés. Des filatures réalisées avec des véhicules munis de plaques d'immatriculation allemandes avaient été détectées.

Lors de sa réunion du 12 juin 2018, la Commission parlementaire de suivi a demandé au Comité permanent R d'ouvrir une enquête de contrôle sur la position d'information et la réaction des services de renseignement belges face aux activités éventuelles de services de renseignement et de sécurité étrangers sur le territoire belge lors du séjour de M. Puigdemont en Belgique.

I.5.2. ASPECTS JURIDIQUES

En application des articles 7, 1° et 8, alinéa 1er, 1°, g) L.R&S, la VSSE a notamment pour mission de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté extérieure de l'État et les relations internationales, activité résultant, par exemple, de l'espionnage (recueil ou livraison d'informations non accessibles au public […]) ou l'ingérence (tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins).

Par ailleurs, en application des articles 7, 1° et 8, alinéa 1er, 2°, a) et b) L.R&S, la VSSE a notamment la mission de rechercher, d'analyser et de traiter le

50 Voir sources ouvertes : Y.N. avec Belga, *La Libre Belgique*, 28 mars 2018 ('Carles Puigdemont porte plainte en Belgique : sa voiture était pistée avec des balises de traçage'). Il y est notamment mentionné que : '*les responsables de la sécurité de l'ancien président catalan ont inspecté son véhicule et détecté un dispositif de suivi installé sous sa voiture*'.

renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'État et le pérennité de l'ordre démocratique et constitutionnel, activité résultant par exemple d'une atteinte aux droits de l'homme et les libertés fondamentales ou une atteinte à la sécurité et à la sauvegarde physique et morale des personnes et la sécurité et la sauvegarde des biens.

En outre, en application des articles 7, 3°/1 et 11, § 1 er, 5° L.R&S, la VSSE a pour mission, depuis janvier 2016, de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge. La même mission a également été confiée au SGRS en 2016 (art. 11, § 1er, 5° L.R&S). Il s'agit d'une compétence générale, dont l'exercice n'est pas conditionné par l'existence d'une menace.

Afin de régler la répartition des tâches visant à rechercher, analyser et traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge, l'article 20, § 4 L.R&S prévoit que la VSSE et le SGRS concluent un accord de coopération sur la base de directives du Conseil national de sécurité (CNS). À ce propos, le Comité permanent R n'a connaissance ni d'une directive du CNS, ni d'un protocole d'accord pris en application de cette disposition (ni d'ailleurs d'un tel projet).[51]

En ce qui concerne la communication avec des services de renseignement et de sécurité étrangers, l'article 19 L.R&S précise que "*les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11*". À cet égard, les travaux préparatoires[52] relatifs à l'article 19 L.R&S évoquent la possibilité de communiquer des renseignements à des services de renseignement et de sécurité étrangers.

Dans le même contexte, l'article 20, § 1er L.R&S dispose, en outre, que les services de renseignement belges doivent veiller à assurer une collaboration avec les services de renseignement et de sécurité étrangers.

Conformément à l'article 20, alinéa 3 de la même loi, les conditions de cette communication doivent être définies par une directive du Conseil national de sécurité. Le 26 septembre 2016, les ministres de la Justice et de la Défense ont soumis une telle note au Conseil national de sécurité.

Pour compléter le cadre juridique, tout en précisant que ces dispositions n'étaient pas encore en vigueur en octobre 2017, il convient de citer les articles 92 à 94 de la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Ces articles prévoient

---

51 Le Plan stratégique du renseignement adopté en 2018 par le Conseil national de sécurité n'aborde cette question spécifique que de manière succincte (dans un tableau). Cette mission relève de la compétence des deux services.

52 *Doc. parl.*, Chambre, 1995-1996, n°49-638/1, 19.

des dispositions particulières en vue du traitement de données à caractère personnel par les services de renseignement et de sécurité, notamment le transfert de données vers des pays non membres de l'Union européenne ou vers des organisations internationales.

I.5.3. CONSTATATIONS

Quant à la compétence des services de renseignement et de sécurité belges

La répartition des tâches entre la VSSE et le SGRS en ce qui concerne la surveillance des activités des services de renseignement et de sécurité étrangers sur le territoire belge ne figure pas dans le Plan National Stratégique du Renseignement, approuvé par le Conseil national de sécurité. De plus, aucun accord de coopération n'a été conclu entre les deux services en exécution de l'article 20, § 4, L.R&S.

Alors que la VSSE prétendait ne pas être compétente, le Comité a fait remarquer que la VSSE et le SGRS ont pour mission, depuis janvier 2016, de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge. Le Comité permanent R était d'avis que l'analyse juridique de la VSSE nécessitait une révision en ce sens et que les dispositions de l'article 20, § 4, L.R&S devaient être respectées.

En ce qui concerne le SGRS, le Comité permanent R a interrogé le service sur sa position d'information concernant Carles Puigdemont. Le service avait-il entrepris des actions dans le cadre du séjour de l'intéressé en Belgique et/ou avait-il prêté son concours à une opération du service partenaire étranger A ? Le SGRS a répondu qu'il ne disposait d'aucune information à propos de M. Puigdemont, qu'il n'avait pas collaboré avec le service partenaire étranger A dans le cadre de son séjour en Belgique et que, dans la mesure où M. Puigdemont ne représentait pas une menace pour les intérêts de la Belgique ou de l'OTAN, il n'avait mené aucune activité à son encontre. Dans le cas d'espèce, et vu sa sphère de compétence spécifique liée à une menace d'ordre "militaire", le SGRS n'avait, quant à lui, et à juste titre, aucune raison de s'intéresser au dossier de M. Puigdemont.

Quant à l'évaluation du risque lié à l'exercice éventuel d'activités de renseignement et d'ingérence d'un ou de plusieurs service(s) de renseignement ou de sécurité étranger(s)

À la lumière des finalités de l'enquête, le Comité permanent R a conclu que la VSSE n'a, à tort, ni recherché, ni analysé, ni traité des informations relatives à l'exercice d'activités sur le territoire belge d'un service de renseignement ou de sécurité étranger dans le cadre de la présence en Belgique de Carles Puigdemont entre 2017 et la finalisation de l'enquête de contrôle.

La VSSE a néanmoins été saisie d'une demande d'assistance technique en vue de l'analyse des balises de localisation.

Le risque ayant été qualifié d'improbable et le niveau de la menace ayant été évalué à 1 par l'OCAM, M. Puigdemont n'a pas fait l'objet d'opérations ni de la part du SGRS, ni de la part de la VSSE. À ce propos, le Comité permanent R a constaté qu'au travers de l'ensemble des dossiers d'évaluation de la menace réalisés par l'OCAM dans le cadre de la présence de M. Puigdemont, aucun risque lié à l'exercice éventuel d'activités de renseignement et d'ingérence d'un ou de plusieurs service(s) de renseignement ou de sécurité étranger(s) n'apparaissait. Ce risque ne relève pas de la sphère de compétence de l'OCAM, mais il appartenait au Comité permanent R de vérifier la présence ou l'absence de mentions liées à ce risque.

Interrogée sur sa propre méthodologie d'évaluation de ladite menace ou du défaut de menace, la VSSE a implémenté, depuis que ce dossier existe, la méthodologie *'leadfase investigative model'* permettant de décider de l'ouverture d'un dossier et des mesures à prendre après une évaluation du risque, de la crédibilité, des possibilités d'action et de la proportionnalité. Cette méthodologie fera l'objet d'un suivi par le Comité permanent R auprès de la VSSE et sera ensuite proposée au SGRS.

En conclusion, le Comité permanent R a estimé, sur ce point, que la présence d'une personnalité de ce type sur le territoire belge nécessitait une analyse et une évaluation formelle spécifique par les services de la VSSE, à la lumière des menaces spécifiques dont elle a la charge, et non à la seule lumière des menaces évaluées par l'OCAM, dont les évaluations ne répondent pas aux mêmes finalités.

Quant à l'échange d'informations

La VSSE a communiqué des données à caractère personnel, qui provenaient, il est vrai, de sources ouvertes et/ou non confidentielles, à un service de renseignement étranger européen qualifié de partenaire "fiable".[53]

En effet, des demandes d'information ont été adressées par le service partenaire étranger A à la VSSE et portaient sur le lieu de résidence de M. Puigdemont. Des réponses ont été apportées par la VSSE, sur la base de sources ouvertes ou d'informations policières non classifiées. La VSSE n'a pas interrogé le service partenaire A sur le fondement de ses demandes et n'a pas mis en balance, d'une part, l'intérêt du service, et d'autre part, les intérêts des intéressés (par ex. le droit fondamental au respect de la vie privée et la liberté d'association). Pour le Comité permanent R, ce cas démontre l'importance de définir des règles claires en matière d'échange d'informations entre les services de renseignement belges et étrangers.

[53] Bien que la directive du Conseil national de sécurité date de septembre 2016, la VSSE a déjà établi une analyse le 25 novembre 2015 (en tenant compte des principes contenus dans le projet de directive que le service avait lui-même rédigé) concernant sa relation avec le service partenaire étranger A. Ce service a été qualifié de partenaire fiable. Le SGRS n'avait pas encore implémenté cette directive.

Par ailleurs, le Comité a déploré que le ministre compétent n'ait pas été informé de la demande du service partenaire étranger A.

Quant aux modalités formelles de concertation entre les services de renseignement belges et les services de renseignement ou de sécurité étrangers

Le Comité permanent R a constaté qu'aucune modalité formelle de concertation n'a été établie entre les services de renseignement belges et un ou plusieurs service(s) de renseignement ou de sécurité étranger(s) concernant Carles Puigdemont. Des contacts informels ont été initiés par le service partenaire étranger A, mais la VSSE n'y a pas donné suite. Le Comité permanent R s'est abstenu de tout commentaire sur ce point.

Quant à la réaction de la VSSE à l'égard du service partenaire étranger A et du service de police étranger

Le Comité permanent R a relevé qu'à un moment donné, l'Administrateur général a décidé de geler la collaboration bilatérale avec le service partenaire étranger A, qui avait formulé certains griefs à son encontre. Les relations entre la VSSE et le service partenaire étranger A se sont normalisées peu après, après l'entretien entre les deux dirigeants des services. Il ne ressortait pas du dossier que ministre compétent avait été informé du gel temporaire de cette relation.

Après la découverte des balises, l'information policière selon laquelle un service de police étranger était en charge du dossier de M. Puigdemont et que ce service posait des questions à la police belge quant aux déplacements de l'intéressé, n'a pas été considérée, à tort, par la VSSE comme pouvant constituer une menace d'activités de services de renseignement ou de sécurité étrangers sur le territoire belge. Le Comité a également estimé que l'information selon laquelle un service de police étranger était en charge du dossier de Carles Puigdemont méritait une analyse formelle et une évaluation spécifique par les services au sein de la VSSE.

I.6. LE FONCTIONNEMENT DE LA DIRECTION COUNTERINTELLIGENCE (CI) DU SGRS : SUIVI DES RECOMMANDATIONS

I.6.1. CONTEXTUALISATION ET OBJET DE L'ENQUÊTE

En exécution de l'article 32 L.Contrôle, le ministre de la Défense a demandé au Comité permanent R, fin décembre 2016, d'effectuer une enquête sur la fonctionnement de la Direction Counterintelligence (CI), l'une des quatre anciennes directions du SGRS. C'est le courrier envoyé par une part importante

du personnel de CI qui est à l'origine de cette demande. Les signataires y exprimaient leurs préoccupations quant au fonctionnement du service et quant aux conditions dans lesquelles le personnel devait remplir ses missions légales.

Le Comité permanent R a ouvert son enquête de contrôle[54] en janvier 2017 et l'a finalisée en février 2018.[55] L'enquête donnait une vue sur la gravité, la complexité et la diversité des dysfonctionnements au sein de la Direction CI. Le Comité avait posé comme postulat que la sécurité nationale requiert un service de renseignement militaire fort et fiable. Aussi, le Comité était convaincu de l'intérêt, pour la Direction CI, d'être organisée et gérée de manière à répondre aux standards d'un service public efficace et efficient. L'enquête a montré que le service audité ne répondait pas à ces standards.

L'enquête sur le fonctionnement de la Direction CI a donné lieu à des recommandations détaillées.[56] En ce qui concerne le calendrier de mise en œuvre, un degré de priorité a été attribué : 'très haut' (à réaliser pour la fin 2018), 'haut' (à réaliser pour fin juin 2019) et 'moyen' (à réaliser pour fin décembre 2019).

Fin janvier 2019, le Comité permanent R a ouvert une enquête de suivi afin de vérifier dans quelle mesure l'ensemble des recommandations formulées dans l'audit susmentionné ont été mises en œuvre. Fin février 2019, la Commission parlementaire de suivi a invité le Comité permanent R à un échange de vues. Celui-ci a eu lieu en préparation des auditions[57], à huis clos, avec le Chef du SGRS, le Chef de la Défense et l'ancien ministre de la Défense, compte tenu de la persistance des problèmes constatés au sein du service de renseignement militaire.

I.6.2. LANCEMENT D'UN *BUSINESS PROCESS RE-ENGINEERING* (BPR)

En réaction à l'audit de la Direction CI, le Chef du SGRS a décidé de lancer, début juin 2018, un *Business Process Re-engineering* (BPR).[58] Cette technique de

---

54 Le Comité avait déjà réalisé un audit similaire. Voir : COMITÉ PERMANENT R, *Rapport d'activités 2011*, 7-14 ('II.1. Un audit au sein du service de renseignement militaire') et 104-107 ('IX.2.1. Recommandations relatives à l'audit effectué au sein du SGRS').

55 COMITÉ PERMANENT R, *Rapport d'activités 2018*, 2-18 ('I.1. Le fonctionnement de la Direction Counterintelligence (CI) du SGRS').

56 COMITÉ PERMANENT R, *Rapport d'activités 2018*, 132-136 ('XII.2.1. Diverses recommandations émises à l'égard du SGRS dans le cadre de l'enquête de contrôle sur la Direction Counterintelligence').

57 Commission spéciale chargée de l'accompagnement parlementaire des Comités permanents P et R, Échange de vues avec le lieutenant-général Claude Van de Voorde, Chef du SGRS, le général Marc Compernol, Chef de la Défense, et le Vice-Premier ministre et ministre des Affaires étrangères et européennes, et de la Défense, chargé de Beliris et des institutions culturelles fédérales, sur la situation de la Direction Counterintelligence (CI) du SGRS, 18 mars 2019 (réunion à huis clos).

58 Une 'core team' a été constituée afin de mettre ce BPR sur les rails. Elle se composait du Deputy Assistant Chief of Staff, des Conseillers civils et militaires du Commandement du

management devait permettre de restructurer de fond en comble les processus de l'organisation. En plus d'exercer un effet sur la structure de l'organisation, une telle méthodologie vise aussi à modifier le style de management et la culture de l'organisation. En outre, inscrire la réflexion sur les réponses aux recommandations portant sur le fonctionnement de CI dans un exercice plus large sur le fonctionnement de l'ensemble du SGRS relevait d'un choix stratégique. En effet, le Commandement du SGRS voulait tenir compte également des conclusions de la Commission d'enquête parlementaire 'Attentats'. Un choix valable, selon le Comité, même si le processus de réformes de la Direction CI serait rendu plus compliqué.

Fin octobre 2018, un conflit a cependant éclaté entre le Commandement du SGRS et le dirigeant de la Direction CI. Étant donné que les propositions élaborées depuis juin 2018 suite aux recommandations du rapport d'audit CI de 2018 n'ont pas pu être intégrées dans ce BPR, les deux plans d'amélioration ont été désynchronisés (octobre 2018 – janvier 2019). Début février 2019, le Commandement de CI a changé de mains, ce qui a permis une reconnexion au trajet BPR.

I.6.3. ÉTAT DES LIEUX DE LA MISE EN OEUVRE DES RECOMMANDATIONS DE L'AUDIT DE 2018

Le Comité a examiné – notamment par des recherches documentaires et des entretiens – la mesure dans laquelle des progrès significatifs ont été réalisés dans la mise en œuvre des recommandations. L'enquête a montré que début mars 2019, des progrès significatifs ont été réalisés dans un tiers des recommandations assorties d'une très haute priorité ; pour la moitié des recommandations, des progrès étaient visibles mais insuffisants pour rétablir complètement l'opérationnalité. Enfin, quelques recommandations n'ont enregistré aucun progrès.

Le Comité a pu constater ce qui suit :

- Le rôle de la Direction CI dans la lutte contre le terrorisme a été clarifié : s'il s'agit de terrorisme à caractère 'civil', c'est la VSSE qui dirige les opérations. Dans le cadre d'un protocole, CI a transféré le personnel et les sources vers une plateforme commune CounterTerro hébergée à la VSSE. Au SGRS, un coordinateur 'horizontal' CounterTerro (issue de CI) a été désigné. Il a été intégré dans le DISCC, ce qui doit améliorer la coopération au sein même du SGRS ;
- Au niveau de l'infrastructure, une issue a été trouvée à la situation très pénible dans laquelle se trouvait la Direction CI : elle a pu déménager en

SGRS, de deux représentants des services d'appui J1 à J8, et des dirigeants des cinq (anciennes) Directions (CI, I, S, Cy, ERO, DISCC) du SGRS.

mars 2019 vers un nouveau bâtiment, entièrement rénové et équipé avec tous les dispositifs de sécurité ;
– Une meilleure coordination a été établie entre la Direction CI et 'J6', qui est responsable de l'ICT au SGRS. Un point de contact a été clairement désigné, et un inventaire a été réalisé en vue de définir les besoins en matière d'ICT.
– En termes de mission et de vision, le travail conceptuel a été réalisé, mais l'ensemble devait encore être validé et *in fine* formalisé. Ce n'est qu'une fois que les objectifs auront été clairement définis qu'il sera possible d'établir les *intelligence requirements* et les *intelligence collection plans* à tous les niveaux ;
– Des propositions ont été soumises concernant l'organigramme et la définition des besoins en moyens (en personnel). Ces propositions doivent encore être validées et formalisées, ce qui était prévu pour le second trimestre 2019 ;
– En ce qui concerne la collaboration entre l'analyse et la collecte, certaines étapes ont également été franchies. Il ne peut plus être question d'une situation où, pour certaines matières, il y avait bien des collecteurs mais pas d'analystes (et inversement).

Il est cependant important de souligner que pour certaines recommandations, il est apparu que la Direction CI n'était peu, voire pas, en mesure de faire progresser la situation (et le SGRS non plus dans certains cas) ; la solution devait surtout venir d'autres échelons (par ex. la réalisation d'une spécialisation 'renseignement').

Le Comité permanent R a décidé de continuer à suivre avec attention la mise en œuvre des recommandations.

I.7. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ EFFECTUÉS EN 2019 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2019

I.7.1. LES SERVICES D'APPUI DE L'OCAM

L'Organe de coordination pour l'analyse de la menace (OCAM) a été institué par la Loi du 10 juillet 2006 relative à l'analyse de la menace. Cet organe a été créé dans le but de donner aux autorités politiques, administratives et judiciaires la vision la plus précise possible de la menace terroriste ou extrémiste en et contre la Belgique, et de leur permettre de réagir de manière adéquate. Le *core business* de l'OCAM consiste à réaliser des évaluations ponctuelles ou stratégiques. Cette tâche incombe à des analystes et à des experts, détachés de ce que l'on appelle les 'services d'appui' (art. 2, 2. L.OCAM). Les services d'appui constituent la source

d'informations la plus importante pour l'organe de coordination. Il s'agit de services très variés, de culture et de taille différentes.

En 2010, le Comité permanent R avait effectué une enquête, conjointement au Comité permanent P, sur les flux d'informations entre l'OCAM et les services d'appui, en mettant l'accent sur les deux services de renseignement et sur la Police fédérale et les Polices locales.[59]

Lors de la réunion plénière commune de décembre 2017, les Comités permanents R et P ont décidé d'ouvrir une enquête de contrôle commune sur les 'autres' services d'appui, à savoir l'Office des étrangers (SPF Intérieur), le SPF Mobilité, le SPF Affaires étrangères ainsi que l'Administration des Douanes et Accises (SPF Finances). Les Comités souhaitaient ainsi établir un *status quaestionis* du flux d'informations entre l'OCAM et les autres services d'appui, et ce en menant toute une série d'auditions.

Différents devoirs d'enquête ont été effectués au cours de l'année 2019. À la fin de l'année, les Comités ont mis la dernière main au rapport. La Commission parlementaire de suivi, qui a pris acte du rapport en 2020, a d'emblée demandé l'ouverture d'une enquête de suivi ainsi qu'un élargissement de la portée de l'enquête, en prenant en considération les services d'appui qui sont venus s'ajouter en 2018 (la Direction générale du Centre de crise (SPF Intérieur), la Direction générale des Établissements pénitentiaires (SPF Justice), la Direction générale de la Législation et des Libertés et Droits fondamentaux (SPF Justice) et l'Administration générale de la Trésorerie (SPF Finances).[60]

I.7.2. L'APPLICATION DE NOUVELLES MÉTHODES (PARTICULIÈRES) DE RENSEIGNEMENT

Avec l'entrée en vigueur en 2010 de la Loi relative aux méthodes de recueil des données par les services de renseignement et de sécurité (Loi MRD), les possibilités de recueil d'informations du SGRS et de la VSSE ont été considérablement élargies. Depuis lors, les services peuvent recourir à des méthodes ordinaires, spécifiques et exceptionnelles, qui devraient refléter le degré d'intrusion des mesures.[61] Les modifications de loi intervenues entre-temps ont modifié la portée de plusieurs méthodes (lisez : élargi). Ainsi, certaines

---

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

60 A.R. du 17 août 2018 exécutant l'article 2, premier alinéa, 2°, g) de la loi du 10 juillet 2006 relative à l'analyse de la menace, *M.B.* 12 septembre 2018.

61 La logique et la gradation des méthodes est néanmoins sous pression. Voir à ce propos : W. VAN LAETHEM, 'Enkele reflecties over tien jaar BIM-controle door het Vast Comité I', dans J. VANDERBORGHT, (ed.), *Les méthodes particulières de renseignement : de l'ombre à la lumière*, Antwerpen, Intersentia, 2020, 70 et suiv.

méthodes 'particulières' sont devenues 'ordinaires' et de nouvelles méthodes ordinaires ont été ajoutées.

Récemment, le Comité a reçu une série de possibilités de contrôle supplémentaires en ce qui concerne certaines méthodes 'ordinaires', même s'il est vrai que ce contrôle est réglementé différemment pour pratiquement chaque méthode. Il s'agit notamment du contrôle de l'identification de l'utilisateur de télécommunications (art. 16/2 L.R&S), de l'accès à des données PNR (art. 16/3 L.R&S), de l'accès aux images des caméras utilisées par les services police (art. 16/4 L.R&S), ou encore du contrôle préalable aux interceptions, aux intrusions dans un système informatique et la prise d'images animées (art. 44/3 L.R&S).

Le Comité a décidé d'étudier cette thématique dans son enquête initiée en 2019 et intitulée : *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R'*. L'enquête a été finalisée au second semestre de 2020.

I.7.3. LE BREXIT ET LES RELATIONS ENTRE LES SERVICES DE RENSEIGNEMENT BELGES ET BRITANNIQUES

Le 23 juin 2016, un référendum a été organisé au Royaume-Uni sur une sortie de l'Union européenne. Une petite minorité a voté en faveur du retrait. Des négociations, qui ont traîné en longueur, ont démarré peu de temps après. Le Royaume-Uni a finalement quitté l'Union européenne le 31 janvier 2020.

Ce processus, communément appelé 'Brexit', a soulevé des questions sur les conséquences éventuelles du retrait britannique de l'Union européenne au niveau de la coopération entre les deux services de renseignement belges (et d'autres services européens) et les trois services de renseignement (civils) britanniques, à savoir le *British Security Service* (BSS, également connu sous le sigle MI5), le *Secret Intelligence Service* (SIS, également connu sous le sigle MI6) et le *Government Communications Headquarters* (GCHQ).

En mai 2019, le Comité permanent R a ouvert une enquête de contrôle concernant les effets du Brexit sur la coopération entre les services de renseignement belges (VSSE et SGRS) et les services de renseignement britanniques. Le Comité souhaitait en particulier vérifier si le Brexit risquait de mettre en péril cette coopération. Il était également question de la manière dont les services de renseignement belges s'y sont préparés.

Au moment où l'enquête de contrôle a été effectuée (octobre – novembre 2019), il n'y avait encore – en raison de la situation politique conflictuelle et incertaine – aucune certitude sur le timing ni sur les circonstances précises du

retrait.[62] Le Comité s'est penché sur la base légale de la coopération internationale, a examiné plusieurs hypothèses sur l'impact du Brexit ainsi que l'évaluation des services de renseignement belges sur les conséquences du Brexit. Le rapport a été finalisé au premier trimestre de 2020.

I.7.4. L'ÉVENTUELLE INGÉRENCE DE SERVICES/ D'ÉTATS ÉTRANGERS DANS LE PROCESSUS ÉLECTORAL BELGE

Bien que les résultats de l'enquête menée à ce propos aux États-Unis n'ont pas été complètement rendus publics, il existait de fortes présomptions que des services/ États étrangers (plus particulièrement la Russie) avaient usé de cybermoyens pour tenter d'influencer les élections présidentielles américaines de 2016. Ce cas de figure est en principe envisageable en Europe, et donc en Belgique.

Les élections du 26 mai 2019 ont placé cette problématique au centre de l'actualité.[63] L'organisation d'élections ouvertes, régulières est au cœur de la démocratie. Il incombe à la VSSE d'identifier certaines menaces visant les institutions belges et d'en informer les autorités compétentes. Dans le cas présent, il s'agirait d'une éventuelle 'ingérence' (article 8, L. R&S, alinéa 2, g), c'est-à-dire "*la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs et clandestins*". L'ingérence peut revêtir différentes formes : la désinformation, la publicité ciblée via les médias sociaux, mais aussi purement et simplement des cyberattaques. Pour le SGRS également, il existe des critères de rattachement en la matière, et ce même si sa compétence est de prime abord moins évidente.

Par conséquent, le Comité a décidé, début 2019, d'ouvrir une enquête de contrôle[64] sur la manière dont les services de renseignement belges ont réagi (collecte de renseignements, avertissements, coopération internationale,

---

62 Différents scénarios ont longtemps été envisagés : un Brexit sur la base de l'accord négocié en octobre 2019 entre l'Union européenne et le gouvernement britannique, un Brexit sur la base d'un accord devant encore être modifié, un Brexit sans accord (ou 'no deal'), voire une annulation du Brexit après d'éventuelles nouvelles élections (ou un nouveau référendum) au Royaume-Uni.

63 À la mi-octobre 2018, une conférence de haut niveau a été organisée sur la thématique par le *European Political Strategy Center* à la veille des élections européennes de mai 2019, sous le patronage de l'Union européenne ('Election Interference in the Digital age : building resilience to cyber-enabled Threats'). Voir https ://eceuropa.eu/epsc/events/election-interference-digital-age-building-resilience-cyber-enabled-threats-en.

64 Le titre complet est le suivant : 'Enquête de contrôle sur la manière dont les services de renseignement belges suivent les risques liés à une éventuelle ingérence d'acteurs étrangers dans le processus électoral belge, sur la manière dont ils tentent de contrer les menaces potentielles et sur la manière dont ils font rapport aux autorités, en particulier en ce qui concerne le risque de cyber-ingérence ou de cyber-attaques'.

possibles entraves[65], etc.) à l'ingérence éventuelle par des services/des États étrangers dans le processus électoral belge. Les questions d'enquête étaient les suivantes :

- Comment la menace peut-elle être caractérisée (quelles formes prend-elle et quels instruments sont utilisés ?) ? Quels sont les précédents récents ?
- Quel est le contexte juridique (tant de l'intervention des services belges que d'éventuels aspects juridiques internationaux) ?
- Qui sont les différents acteurs en Belgique concernés par cette problématique (services de renseignement, OCAM, Centre pour la Cybersécurité, etc.) et comment les compétences sont-elles réparties ?

Le rapport d'enquête a été approuvé début 2020.

I.7.5. LE SUIVI DE L'EXTRÊME DROITE PAR LES SERVICES DE RENSEIGNEMENT BELGES

Il ressort de nombreuses sources que les groupes et mouvements extrémistes de droite se sont fortement implantés en Europe et qu'ils ne cessent d'y étendre leur influence. Une série d'attentats, d'attaques et d'actes de violence (planifiés) attribués à des extrémistes de droite ont été perpétrés ces dernières années. La Belgique n'a pas été épargnée. Aussi, le Comité permanent R a décidé, en mai 2019, d'ouvrir une enquête de contrôle sur la manière dont les services de renseignement suivent aujourd'hui la menace qui émane du phénomène de l'extrême droite en Belgique et sur la manière dont ils font rapport aux autorités. Le Comité permanent R souhaite savoir si et comment les services de renseignement remplissent leur mission légale en matière de suivi de l'extrémisme, et en particulier l'extrémisme de droite en Belgique, et comment ils procèdent. Les questions d'enquête ont été formulées comme suit :

- Comment les services de renseignement définissent-ils le phénomène de l'extrême droite ? La VSSE et le SGRS utilisent-ils une définition pour cerner l'extrême droite ? Les services de renseignement et de sécurité utilisent-ils une définition commune dans le cadre du Plan Radicalisme ? Ces définitions s'inscrivent-elles dans le contexte juridique ?
- Quel est le contexte juridique ? Quelles sont les instructions des ministres compétents ou du Conseil national de sécurité ou d'autres instances ?

---

65 La VSSE considère également l'entrave ('*disruption*') comme faisant partie de sa mission. L'entrave signifie qu'un service de renseignement non seulement mène discrètement des opérations de renseignement, mais éventuellement aussi qu'il tente activement de contrer les menaces détections par toutes sortes de moyens (par ex. en les rendant publiques ; cf. la réaction de l'AIVD néerlandais après qu'il est apparu que le GRU russe a tenté de pirater une institution internationale à La Haye).

- Les services de renseignement peuvent-ils situer le phénomène dans un contexte et le quantifier ? Quelle forme et quelle place l'extrême droite prend-elle en Belgique ?
- Comment les services suivent-ils le phénomène ? Comment détermine-t-on quels groupements et quelles situations font l'objet d'un suivi actif ? Comment les services sont-ils organisés pour effectuer ce suivi ? Quelles priorités sont établies ? Quels moyens sont mis en œuvre (personnel, méthodes, etc.) et quelles méthodes sont utilisées (méthodes ordinaires, méthodes particulières de renseignement) Quelles évaluations ont été faites (analyse) et comment en a-t-on fait rapport aux autorités ? Quel est leur feedback ?

Différents actes d'enquête ont été posés courant 2019. L'enquête se poursuit en 2020.

I.7.6. LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION DANS LE PROCESSUS DE RENSEIGNEMENT

Les Technologies de l'Information et de la Communication (ICT ou TIC) jouent un rôle de plus en plus important dans les processus du renseignement, aussi bien dans la collecte et l'analyse des informations de base que dans la diffusion des renseignements. Les informations peuvent provenir des sources humaines (HUMINT), des informations de partenaires ou des sources digitales, telles que, notamment, les '*open sources*' ou sources ouvertes (OSINT), les écoutes (SIGINT) ou les prises d'images (GEOINT). La croissance constante des flux de données nécessite des systèmes adéquats, prêts à absorber ces flux et permettant une analyse correcte, rapide et efficace. L'environnement informatique doit donc être un outil stable et orienté vers l'avenir, et ce afin de donner du support aux différents acteurs intervenant dans le cycle du renseignement. Cet environnement, aussi bien matériel que logiciel, doit se conformer aux standards en la matière, aux bonnes pratiques IT, tout en prenant en compte les nouvelles et futures évolutions technologiques[66], telles que le '*big data*'.[67]

---

66 Les organes de contrôle ont également un rôle important à jouer à cet égard. Voir à ce propos : K. VIETH et T. WETZLING, *Data-driven Intelligence Oversight. Recommendations for a System Update*, StiftungNeueVerantwortung, novembre 2019, 63 p.

67 Le '*big data*' se réfère à la science de collecter et d'analyser de grands volumes de données dans le but de découvrir certains '*patterns*' intéressants sur la base d'une classification ('*clustering*') et d'analyses statistiques permettant ainsi de fournir une aide à la décision. Ces données sont généralement caractérisées par une variété, une vélocité et un volume importants.

Dans des enquêtes antérieures, le Comité permanent R a constaté que les services de renseignement étaient confrontés à des défis majeurs dans ce domaine. En ce qui concerne le SGRS, il est déjà apparu par le passé que l'ICT est un point délicat. Le Comité a constaté que les activités de renseignement n'étaient pas (ou plus) suffisamment soutenues par l'ICT. Les conditions d'une bonne gestion de l'information n'étaient pas (plus) pleinement remplies.[68, 69]

En mai 2019, le Comité permanent R a informé le Président de la Chambre des représentants de l'ouverture de l'enquête intitulée *'Enquête de contrôle sur les moyens informatiques utilisés par les services de renseignement belges pour la collecte, le traitement, l'analyse et la communication de l'information dans le cadre du cycle du renseignement'*. La portée de l'enquête a été balisée dès le départ. L'enquête se concentre sur les moyens informatiques spécifiquement utilisés pour appuyer les éléments du cycle du renseignement. Ce sont ces systèmes qui sont utilisés, par exemple, pour effectuer la collecte, ou des outils d'analyse spécifiques et des banques de données.[70] Le Comité permanent R n'a donc pas examiné les facilités bureautiques (génériques/standard) utilisées par les services (par exemple, Windows, Word, Excel, etc.) pour autant qu'elles ne sont pas spécifiques aux services de renseignement. Le Comité n'a pas non plus examiné en détail le matériel informatique (hardware) mis à la disposition des services, à moins qu'il ne soit spécifique aux services de renseignement. L'enquête vise à identifier les risques auxquels sont confrontés les services et, par le biais de recommandations, à réduire ces risques.

Un premier module (SGRS) a été finalisé à la mi-2020. Les résultats de l'enquête concernant la VSSE sont attendus pour début 2021.

I.7.7. LE SUIVI PAR LA VSSE DES CONDAMNÉS POUR TERRORISME QUI ONT ÉTÉ LIBÉRÉS

En Belgique, ce sont environ 400 personnes qui ont été condamnées pour infractions terroristes depuis 2015.[71] Certaines d'entre elles ont été condamnées

68 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 7-14 ('II.1. Un audit au sein du service de renseignement militaire') ; *Rapport d'activités 2018*, 2-18 2-18 ('I.1. Le fonctionnement de la Direction Counterintelligence (CI) du SGRS').

69 Le rapport de la Commission d'enquête parlementaire en réponse aux attaques de Zaventem et de Maelbeek recommandait de renforcer la gestion de l'information des services afin notamment de garder la surinformation ('infobesitas') sous contrôle. Voir 'Commission d'enquête sur les attentats terroristes du 22 mars 2016. *Doc. parl.* Chambre, 2016-2017, n°54-1752/008, 15 juin 2017, p. 53 et 180 et suiv.

70 Au SGRS, on appelle ces systèmes *'weaponsystems'* – par analogie avec, par exemple, des systèmes intégrés aux plateformes de défense à la Défense (par ex., les logiciels pour les systèmes radar ou pour le *'battle management'*).

71 Questions jointes du ministre de la Justice sur 'la libération de terroristes' (*C.R.I.*, Chambre 2019-20, 4 juin 2020, COM043, 16, Q. n°550000781P et 550000786P).

par défaut et n'ont donc pas pu être incarcérées. Plusieurs de ces individus condamnés ont entre-temps purgé leur peine ou, sur décision du tribunal de l'application des peines, ont été libérés sous conditions (pour l'exécution de la fin de leur peine).

Grâce à un système informatique (SIDIS Suite)[72] de l'administration pénitentiaire, plusieurs instances (VSSE, Police fédérale, etc.) sont informées de chaque libération d'un détenu radicalisé. À la mi-2019, le Comité a décidé d'ouvrir une enquête de contrôle sur *'le suivi par les services de renseignement et de sécurité belges, d'une part des inculpés en Belgique pour infractions terroristes perpétrées en Belgique ou ailleurs et bénéficiant d'une modalité visée par la loi du 20 juillet 1990 et d'autre part, des condamnés en Belgique pour infractions terroristes qui sortent de prisons belges, soit dans le cadre d'une des modalités visées dans le cadre de la loi du 17 mai 2006, soit qui sont libérés définitivement (art. 71 de ladite loi)'*.

I.7.8. LE RISQUE D'INFILTRATION AU SEIN DES DEUX SERVICES DE RENSEIGNEMENT

Ces dernières années, le monde du renseignement, au niveau international, a été secoué par une série de cas d'infiltration (et '*insider threat*'). En 2019, le Comité a pris l'initiative de lancer une enquête de contrôle sur la manière dont les deux services de renseignement gèrent le risque d'infiltration : quels risques ont été identifiés ? Quelles mesures ont été prises pour les maîtriser et pour réagir si ces risques venaient à se concrétiser ?

Plusieurs réunions de travail ont été organisées avec le SGRS et la VSSE sur la thématique 'cartographie et évaluation du risque d'infiltration au sein des services de renseignement'. À cet égard, le processus de gestion du risque, telle que reprise dans la norme ISO 31000, a constitué une base de départ.[73]

---

72 La banque de données SIDIS Suite traite les données de personnes auxquelles une peine privative de liberté, une mesure privative de liberté (détention provisoire) ou un internement a été imposé et qui, pour cette raison, séjournent en prison, dans une institution ou dans une section de défense sociale (internement), ou encore dans un centre d'internement pour mineurs. SIDIS Suite permet l'échange d'informations et les flux de données nécessaires entre ces autorités.

73 www.iso.org :fr/iso-31000-risk-management.html.

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

Ce chapitre reprend les chiffres détaillés de la mise en œuvre par la Sûreté de l'État (VSSE) et par le Service Général du Renseignement et de la Sécurité (SGRS) des méthodes spécifiques et exceptionnelles (les 'méthodes particulières') et de certaines méthodes ordinaires, pour lesquelles le Comité s'est vu confier une mission spécifique. De plus, il est fait rapport sur la manière dont le Comité assure sa mission de contrôle juridictionnelle sur ces méthodes. Outre une série de chiffres sur le nombre de décisions et la manière dont le Comité a été saisi, la substance des décisions finales du Comité permanent R est reprise. La jurisprudence a été expurgée des données opérationnelles ; seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue juridique.

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

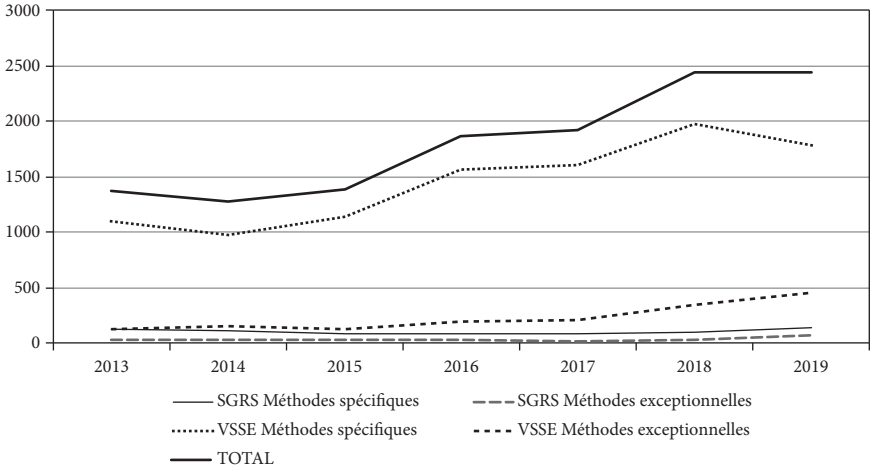
Entre le 1er janvier et le 31 décembre 2019, 2444 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 2230 par la VSSE (1781 spécifiques et 449 exceptionnelles) et 214 par le SGRS (138 spécifiques et 76 exceptionnelles).

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

	SGRS		VSSE		TOTAL
	Méthodes spécifiques	**Méthodes exceptionnelles**	**Méthodes spécifiques**	**Méthodes exceptionnelles**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445
2019	138	76	1781	449	2444

Schématiquement :

Aperçu du nombre de MRD mises en oeuvre au fil des ans (2013-2019)



Après une augmentation constante du nombre de MRD mises en œuvre ces dernières années, on remarque pour la première fois une stagnation : le nombre total de méthodes utilisées est resté stable en 2019 par rapport à 2018. Il convient néanmoins de noter que plusieurs targets (tels que des personnes, des organisations, des lieux, des objets, des moyens de communication, etc.) peuvent être visés dans une même autorisation.

La VSSE se taille la part du lion, avec 91,2 % des méthodes mises en œuvre.

Une ventilation de ces chiffres permet toutefois de constater une hausse notable des méthodes mises en œuvre par SGRS, tant des méthodes spécifiques (de 102 à 138) que des méthodes exceptionnelles (de 28 à 76, soit plus du double). À la VSSE, ce sont les méthodes exceptionnelles qui ont connu une croissance marquée (de 344 à 449). La stagnation observée malgré toutes ces augmentations s'explique par une forte diminution du nombre de méthodes spécifiques mises

en œuvre (de 1971 à 1781) pour l'année 2019. Le Comité se limite ici à reprendre les chiffres bruts et s'abstient de tout commentaire. Le Comité a l'intention d'interroger les services à cet égard afin de pouvoir interpréter ces chiffres en connaissance de cause.

En ce qui concerne les méthodes ordinaires qui consistent à adresser une réquisition à des opérateurs afin d'identifier certains moyens de communication, on note, contrairement à ces dernières années, une diminution d'environ 12 % (60 réquisitions de moins au SGRS par rapport à 2018, contre 800 réquisitions de moins du côté de la VSSE).

	Réquisitions par le SGRS	**Réquisitions par la VSSE**
2016	216	2203
2017	257	4327
2018	502	6482
2019	442	5674

Le Comité avait déjà indiqué[74] que *"[il] ne [pouvait] nier qu'un nombre beaucoup plus élevé d'identifications ont été effectuées depuis l'introduction de la procédure assouplie visée à l'article 16/2 L.R&S"*. Le nombre de réquisitions en 2019, bien qu'en baisse, demeure assez important. Dans l'exercice de sa compétence de contrôle générale, le Comité en a examiné les motifs ; les résultats ont été repris dans l'enquête de contrôle ouverte en 2019 et intitulée *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R'* (cf. I.7.2).

II.1.1. MÉTHODES UTILISÉES PAR LE SGRS

II.1.1.1. Les méthodes ordinaires

Identification de l'utilisateur de télécommunications

L'identification de l'utilisateur de télécommunications (par ex. d'un numéro de GSM ou d'une adresse IP) ou d'un moyen de communication utilisé est considérée 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.[75]

74 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 43.

75 Auparavant, il s'agissait d'une méthode spécifique. La modification a eu lieu via l'introduction d'un nouvel article 16/2 dans la Loi du 30 novembre 1998. Lorsque l'identification a lieu à l'aide d'un moyen technique (et donc pas via une réquisition à un opérateur), la collecte reste une méthode spécifique (art. 18/7 § 1er L.R&S).

La réglementation prévoit une obligation pour la VSSE et le SGRS de tenir un registre de toutes les identifications requises et de toutes les identifications obtenues par accès direct. Conformément à cette même réglementation, le Comité doit recevoir, sur une base mensuelle, une liste des identifications requises et de chaque accès. Dans la pratique, le Comité ne reçoit chaque mois que le nombre de réquisitions.[76] Cette thématique a également fait l'objet d'une enquête de contrôle ouverte en 2019 (*supra*).

Identification du détenteur d'une carte prépayée

La VSSE et le SGRS doivent – comme dans le cadre de l'identification de l'utilisateur de télécommunications ou d'un moyen de communication utilisé – tenir un registre de toutes les identifications requises et de toutes les identifications obtenues d'une autre méthode ordinaire introduite en 2016. L'article 16/2 L.R&S mentionne en effet ce qui suit : '*§ 2. Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée visée dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.*' Comme en 2018, les deux services de renseignement n'ont pas fait usage de cette méthode.

Accès aux données PNR

Début 2017[77], une loi a introduit la possibilité pour les services de renseignement d'avoir accès aux informations détenues par l'Unité d'information des passagers, et ce par le biais de recherches ciblées (art. 16/3 L.R&S et art. 27 Loi PNR du 25 décembre 2016). Le Comité est informé de l'utilisation de cette méthode et peut l'interdire le cas échéant.[78]

La réglementation PNR permet également de réaliser ce que l'on appelle une 'évaluation préalable', qui consiste à vérifier automatiquement la correspondance entre les données PNR et les listes ou fichiers de noms des services de renseignement et à envoyer des informations sur la base de *hits* validés (art. 24 Loi PNR).

---

76 La situation a été régularisée courant 2020.

77 Loi du 25 décembre 2016 (*M.B.* 25 janvier 2017).

78 Contrairement à ce qui s'applique aux méthodes reprises à l'article 16/2 L.R&S, il n'était pas prévu qu'un rapport doive être rédigé à l'intention du Parlement. L'article 35 § 2 L. Contrôle n'a, en effet, pas été adapté. Suivant la suggestion émise par la Commission de suivi, le Comité a décidé de reprendre ces chiffres dans son rapport annuel et de ne pas attendre une éventuelle modification de la loi.

Utilisation d'images enregistrées par les caméras des services de police

La Loi du 30 novembre 1998 organique des services de renseignement et de sécurité a été adaptée par la Loi du 21 mars 2018 (*M.B.* 16 avril 2018) pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services de police. Une nouvelle méthode ordinaire d'observation a été introduite à cet effet (art. 16/4 L.R&S).[79] En l'absence d'arrêté d'exécution, cette disposition n'est pas encore entrée en vigueur.[80]

Les chiffres

Méthodes ordinaires (SGRS)	**Nombre d'autorisations**
Identification de l'utilisateur de télécommunications	442
Identification du détenteur d'une carte prépayée	0
Recherches ciblées de données PNR	38
Transmission de données PNR sur la base de *hits*	Non communiqué
Utilisation d'images enregistrées par les caméras des services de police	Pas en vigueur

II.1.1.2. Les méthodes spécifiques

Le tableau ci-dessous reprend les chiffres relatifs à l'application des méthodes spécifiques par le SGRS. On en distingue sept.

Méthodes spécifiques (SGRS)	**Nombre d'autorisations**
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)[81]	12
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	0
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	0

79 Cette même loi a étendu la possibilité d'observation spécifique et exceptionnelle existante (articles 18/4 § 3 et 18/11 § 3 L.R&S).

80 Début 2019, le Conseil des ministres a approuvé un projet d'arrêté royal en la matière, qui a été soumis à l'avis du Comité permanent R. Cet avis 002/CPR-ACC/2019 du 9 avril 2019 peut être consulté sur le site internet du Comité (www.comiteri.be).

81 La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/4 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées, n'a pas encore été opérationnalisée.

Méthodes spécifiques (SGRS)	Nombre d'autorisations
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée, et requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 L.R&S)	0
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	63
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	63
TOTAL	**138**

II.1.1.3. Les méthodes exceptionnelles

Dans le cadre de ses missions visées aux articles 11, § 1er, 1° à 3° en 5°, et § 2 L.R&S, le SGRS peut mettre en œuvre différentes méthodes exceptionnelles :

Méthodes exceptionnelles (SGRS)	Nombre d'autorisations
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)[82]	3
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	3
Recourir à une personne morale visée à l'article 13/3, § 1er L.R&S afin de collecter des données	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	2
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	20
S'introduire dans un système informatique (article 18/16 L.R&S)	8
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	40
TOTAL	**76**

[82] La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/4 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées, n'a pas encore été opérationnalisée.

II.1.1.4. Les missions et les menaces justifiant le recours aux méthodes ordinaires et particulières[83]

Le SGRS est autorisé à employer les méthodes spécifiques et exceptionnelles dans le cadre de quatre missions et tenant compte de différentes natures de menaces.

1. **La mission de renseignement (art. 11, 1° L.R&S)**
   Le recueil, l'analyse et le traitement du renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir. Le recueil, l'analyse et le traitement du renseignement relatif à toute activité qui menace ou pourrait menacer les intérêts suivants :
   - l'intégrité du territoire national ou la survie de tout ou partie de la population ;
   - les plans de défense militaires ;
   - le potentiel économique et scientifique en rapport avec la défense ;
   - l'accomplissement des missions des Forces armées ;
   - la sécurité des ressortissants belges à l'étranger.
2. **Veiller au maintien de la sécurité militaire (art. 11, 2° L.R&S)**
   - la sécurité militaire du personnel relevant du ministre de la Défense nationale ;
   - les installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires ;
   - dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense nationale gère, neutraliser l'attaque et en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés.
3. **La protection de secrets (art. 11, 3° L.R&S)**
   - La protection du secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que gère le ministre de la Défense nationale.
4. **La recherche, l'analyse et le traitement du renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge (art. 11, 5°, L.R&S).**

---

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

Ces méthodes ne peuvent donc pas être utilisées dans le cadre d'enquêtes de sécurité ou d'autres missions assignées au SGRS par des lois particulières (par ex. effectuer des vérifications de sécurité pour des candidats militaires). Toutefois, depuis l'entrée en vigueur de la Loi du 30 mars 2017, la mise en œuvre de méthodes particulières n'est plus limitée au territoire belge (art. 18/1, 2° L.R&S). La pratique a montré que plusieurs menaces peuvent figurer dans une même autorisation.

Deux tiers des méthodes spécifiques et exceptionnelles sont utilisées par le SGRS dans le cadre de la mission de recherche, d'analyse et de traitement du renseignement relatif aux activités des services de renseignements étrangers sur le territoire belge (art. 11, 5° L.R&S). On ne peut cependant pas en déduire que, depuis 2017, le SGRS suit un 'nouveau genre' de menace. En effet, le suivi de services étrangers était auparavant plus vite associé à la mission de renseignement dans le contexte de la lutte contre l'espionnage.

NATURE DE LA MENACE	NOMBRE EN 2019
Espionnage	165
Terrorisme (et processus de radicalisation)	6
Extrémisme	5
Ingérence	38
Organisations criminelles	–
Autre	–
Total	214

Contrairement à la mise en œuvre de méthodes particulières, le Comité ne dispose pas de données chiffrées relatives à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question dans le présent chapitre. Dans son précédent rapport d'activités, le Comité recommandait aux services de consigner ces données et de les tenir à disposition.[84] Étant donné que ce n'est pas encore le cas, le Comité réitère sa recommandation.

II.1.2. LES MÉTHODES UTILISÉES PAR LA VSSE

II.1.2.1. Les méthodes ordinaires

Méthodes ordinaires (VSSE)	Nombre d'autorisations
Identification de l'utilisateur de télécommunications	5674
Identification du détenteur d'une carte prépayée	0
Recherches ciblées de données PNR	27
Transmission de données PNR sur la base de *hits*	Non communiqué
Utilisation d'images enregistrées par les caméras des services de police	Pas en vigueur

84 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 43.

Pour rappel, le Comité va procéder à un examen approfondi de la manière dont cette méthode est mise en œuvre dans son enquête de contrôle initiée en 2019.

II.1.2.2. Les méthodes spécifiques

Méthodes spécifiques (VSSE)	**Nombre d'autorisations**
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)	311
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	0
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	48
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée, et requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 L.R&S)	50
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	700
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	672
TOTAL	**1781**

II.1.2.3. Les méthodes exceptionnelles

Méthodes exceptionnelles (VSSE)	**Nombre d'autorisations**
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)[85]	26
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	13
Recourir à une personne morale visée à l'article 13/3, § 1er L.R&S afin de collecter des données	0

85 La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/4 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées, n'a pas encore été opérationnalisée.

Méthodes exceptionnelles (VSSE)	Nombre d'autorisations
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	12
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	95
S'introduire dans un système informatique (article 18/16 L.R&S)	48
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	255
TOTAL	**449**

II.1.2.4. Les menaces et les intérêts justifiant le recours aux méthodes particulières

Le tableau suivant reprend les menaces (potentielles) dans le cadre desquelles la VSSE a accordé des autorisations spécifiques et exceptionnelles. Une méthode peut naturellement viser plusieurs menaces. La VSSE peut utiliser les méthodes spécifiques dans le cadre de toutes les menaces qui entrent dans ses compétences (art. 8 L.R&S). La loi définit les diverses notions comme suit :

1. L'espionnage : le recueil ou la livraison d'informations non accessibles au public, et le fait d'entretenir des intelligences de nature à les préparer ou à les faciliter ;
2. Le terrorisme : le recours à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d'atteindre ses objectifs par la terreur, l'intimidation ou les menaces ;
   Processus de radicalisation : un processus influençant un individu ou un groupe d'individus de telle sorte que cet individu ou ce groupe d'individus soit mentalement préparé ou disposé à commettre des actes terroristes ;
3. L'extrémisme : les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit ;
4. La prolifération : le trafic ou les transactions relatives aux matériaux, produits, biens ou know-how pouvant contribuer à la production ou au développement de systèmes d'armement non conventionnels ou très avancés. Sont notamment visés dans ce cadre le développement de programmes d'armement nucléaire, chimique et biologique, les systèmes de transmission qui s'y rapportent, ainsi que les personnes, structures ou pays qui y sont impliqués ;
5. Les organisations sectaires nuisibles, c'est-à-dire tout groupement à vocation philosophique ou religieuse, ou se prétendant tel, qui, dans son organisation ou sa pratique, se livre à des activités illégales dommageables, nuit aux individus ou à la société ou porte atteinte à la dignité humaine ;

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

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

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

NATURE DE LA MENACE	NOMBRE EN 2019
Espionnage	777
Terrorisme (et processus de radicalisation)	1118
Extrémisme	291
Prolifération	2
Organisations sectaires nuisibles	0
Ingérence	87
Organisations criminelles	0
Suivi des activités des services étrangers en Belgique	(inclus dans les chiffres ci-dessus)
TOTAL	**2230**

Les chiffres repris ci-dessus montrent que le terrorisme, pour ce qui est de la mise en œuvre de MRD, demeure la priorité absolue de la VSSE en 2019.

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

1. La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, c'est-à-dire :
   a) la sécurité des institutions de l'État et la sauvegarde de la continuité du fonctionnement régulier de l'État de droit, des institutions démocratiques, des principes élémentaires propres à tout État de droit, ainsi que des droits de l'homme et des libertés fondamentales ;

b) la sécurité et la sauvegarde physique et morale des personnes et la sécurité et la sauvegarde des biens.
2. La sûreté extérieure de l'État et les relations internationales : la sauvegarde de l'intégrité du territoire national, de la souveraineté et de l'indépendance de l'État, des intérêts des pays avec lesquels la Belgique poursuit des objectifs communs, ainsi que des relations internationales et autres que la Belgique entretient avec des États étrangers et des institutions internationales ou supranationales.
3. La sauvegarde des éléments essentiels du potentiel économique et scientifique.

A l'instar du SGRS, la VSSE combine plusieurs intérêts. On peut néanmoins mentionner que la 'sauvegarde des éléments essentiels du potentiel économique et scientifique' n'apparaissait pas dans les chiffres comme étant un intérêt.

Pour rappel (voir II.1.1.4.), le Comité ne dispose pas des chiffres relatifs à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question dans le présent chapitre.

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

II.2.1. CONTRÔLE DE CERTAINES MÉTHODES ORDINAIRES

Le contrôle de certaines méthodes ordinaires est réglementé de manière différente pour chacune d'entre elles.

En ce qui concerne l'identification de l'utilisateur de télécommunications (ou l'identification de l'utilisateur d'une carte prépayée), la loi n'a pas instauré de contrôle spécifique. À l'article 16/2 § 4 L.R&S, il est seulement stipulé que la liste des identifications requises et de tous les accès directs doit être communiquée chaque mois au Comité. Comme déjà indiqué, le Comité reçoit uniquement le nombre de réquisitions. Il a toutefois proposé de contrôler annuellement une sélection de réquisitions.[86] Ce contrôle a débuté en 2020. Le Comité a décidé de reprendre cette thématique dans l'enquête qu'il a initiée en 2019 et qui est intitulée '*enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R.*'

86 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 25 note de bas de page 41.

En ce qui concerne l'accès aux données PNR, qui sont détenues par l'Unité d'information des passagers, l'article 16/3 L.R&S dispose que c'est le dirigeant du service qui doit décider de tout accès, et ce '*de façon dûment motivée*'. Le Comité doit en être informé *et* '*interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales*'. Le Comité n'a prononcé aucune interdiction de ce genre en 2019.

Enfin, le Comité s'est vu attribuer des modalités de contrôle particulières dans le cadre de la possibilité pour les services de renseignement d'avoir accès à des informations provenant d'images enregistrées par des caméras utilisées par les services de police (article 16/4 L.R&S) : un contrôle *a priori*[87] et un contrôle *a posteriori*.[88] Étant donné que les services de renseignement n'ont pas encore pu employer cette méthode, le Comité n'a pas dû intervenir.

II.2.2. CONTRÔLE DES MÉTHODES PARTICULIÈRES

II.2.2.1. Les chiffres

Cette section reprend les activités du Comité permanent R relatives aux méthodes de renseignement spécifiques et exceptionnelles. L'attention se focalise ici sur les décisions juridictionnelles prises en la matière, et non sur les données opérationnelles. Il convient toutefois de souligner au préalable que le Comité soumet *toutes* les autorisations de mise en œuvre de méthodes particulières à une enquête *prima facie*, et ce en vue de décider d'une éventuelle saisine. Par ailleurs, un membre du Service d'Enquêtes participe à une réunion de quinzaine, au cours de laquelle la VSSE informe la Commission BIM sur l'exécution des méthodes exceptionnelles. Un rapport en est fait à l'intention du Comité, ce qui lui permet d'avoir une meilleure vue sur ces méthodes.[89]

---

87 '*Les critères d'évaluation visés à l'alinéa 1er, 2°, sont préalablement présentés au Comité permanent R.*'

88 *'La décision du dirigeant du service ou de son délégué et sa motivation sont transmises au Comité permanent R dans les meilleurs délais. La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, une liste des accès ponctuels est communiquée une fois par mois au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales'* et *'Chaque liste avec laquelle la corrélation visée à l'alinéa 1er, 1°, est réalisée, est communiquée dans les meilleurs délais au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les circonstances qui ne respectent pas les conditions légales.*'

89 En 2017, le Comité a recommandé au SGRS d'organiser lui aussi de telles réunions de quinzaine. Il s'agit en effet d'une obligation légale (art. 18/10 § 1er, alinéa 3, L.R&S et art. 9 A.R. du 12 octobre 2010). Depuis fin janvier 2018, en raison du nombre restreint de méthodes

L'article 43/4 L.R&S stipule que le Comité permanent R peut être saisi de cinq manières :
1. D'initiative ;
2. À la demande de la Commission de la protection de la vie privée/Autorité de protection des données ;
3. Par le dépôt d'une plainte d'un citoyen ;
4. De plein droit, chaque fois que la Commission BIM a suspendu une méthode spécifique ou exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données ;
5. De plein droit, quand le ministre compétent a donné son autorisation sur base de l'article 18/10, § 3 L.R&S.

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

TYPE DE SAISINE	2013	2014	2015	2016	2017	2018	2019
1. D'initiative	16	12	16	3	1	1	4
2. Commission Vie Privée/ Autorité de protection des données	0	0	0	0	0	0	0
3. Plainte	0	0	0	1	0	0	0
4. Suspension par la Commission BIM	5	5	11	19	15	10	12
5. Autorisation du ministre	2	1	0	0	0	0	0
6. Auteur d'avis préjudiciel	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**

Le nombre de décisions prises par le Comité a continué à diminuer, et ce malgré la hausse significative (+ 27 %) du nombre de méthodes particulières de renseignement mises en œuvre. En outre, toutes les saisines, à une exception près, résultent d'une suspension décidée par la Commission BIM.

Une fois saisi, le Comité peut prendre plusieurs types de décisions et de décisions intermédiaires.
1. Constater la nullité de la plainte pour cause de vice de forme ou absence d'un intérêt personnel et légitime (art. 43/4, alinéa 1er, L.R&S) ;
2. Ne pas donner suite à une plainte qui est manifestement non fondée (art. 43/4, alinéa 1er, L.R&S) ;

particulières de renseignement mises en œuvre, une réunion est organisée sur une base mensuelle et, en principe, un rapport est établi sur une base bimensuelle.

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

NATURE DE LA DÉCISION	2014	2015	2016	2017	2018	2019
Décisions préalables à la saisine						
1. Plainte frappée de nullité	0	0	0	0	0	0
2. Plainte manifestement non fondée	0	0	0	0	0	0
Décisions intermédiaires						
3. Suspension de la méthode	3	2	1	0	0	0
4. Information complémentaire de la Commission BIM	0	0	0	0	0	0
5. Information complémentaire du service de renseignement	1	1	4	0	0	0
6. Mission d'enquête confiée au Service d'Enquêtes R	54	48	60	35	52	52
7. Audition membres de la Commission BIM	0	2	0	0	0	0
8. Audition membres des services de renseignement	0	2	0	0	0	1
9. Décision relative au secret de l'instruction	0	0	0	0	0	0
10. Informations sensibles lors de l'audition	0	0	0	0	0	0
Décisions finales						
11. Cessation de la méthode	3	3	6	9	4	11
12. Cessation partielle de la méthode	10	13	4	6	6	4
13. Levée (partielle) de l'interdiction de la Commission BIM	0	4	11	0	0	0
14. Non compétent	0	0	0	0	0	0
15. Autorisation légale/Non- cessation de la méthode/Non-fondement[51]	4	6	2	1	1	0
Avis préjudiciels						
16. Avis préjudiciel	0	0	0	0	0	0

II.2.2.2. La jurisprudence

La substance des décisions finales prises par le Comité permanent R en 2019 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.

Les décisions ont été regroupées en quatre rubriques :

- Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode ;
- La proportionnalité et la subsidiarité ;
- La légalité d'une méthode concernant les techniques employées, des données recueillies, la durée de la mesure et la nature de la menace ;
- La légalité de l'exécution d'une méthode légale.

Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode

Réquisitions adressées à des fournisseurs de services de communications

Le dossier 2019/8254 portait sur une demande adressée par un service de renseignement à une plateforme de médias sociaux en vue de prendre connaissance du contenu de deux profils. En l'absence de réponse, le service a adressé une réquisition à un service de renseignement étranger afin de lui demander de questionner cette plateforme. Il ne faisait aucun doute que la démarche du service s'inscrivait dans le cadre d'une menace imminente, mais aucune décision MRD n'a été rédigée vu que le service considérait cette démarche comme une méthode ordinaire. Tant la Commission BIM, qui avait eu connaissance de la réquisition via un autre dossier, que le Comité permanent R estimaient pour leur part qu'il s'agissait d'une méthode exceptionnelle. Compte tenu de l'importance de ce jugement, l'essence de la décision est reproduite *in extenso* : *'Overwegende dat de wet van 13 juni 2005 betreffende de elektronische communicaties en meer in het bijzonder de artikelen 9 en 122 tot 127 de procedures vastlegt waarin de politiediensten en de inlichtingen- en veiligheidsdiensten toegang hebben tot elektronische communicaties. Dat het Koninklijk Besluit van 12 oktober 2010, en meer in het bijzonder artikel 5, de modaliteiten vastlegt inzake de verzoeken betreffende elektronische communicaties door de inlichtingen-en veiligheidsdiensten. Overwegende dat het Arrest van het Hof van Cassatie van 1 december 2015 (zaak Yahoo, P.13.2082.N) bevestigt dat een maatregel die bestaat in de verplichting om gevorderde gegevens te verstrekken wordt genomen op het Belgisch grondgebied ten aanzien van elke operator of verstrekker die zijn economische activiteiten actief op consumenten in België richt. Overwegende dat overigens artikel 3, 11/1 in die zin werd gewijzigd, waarbij het begrip 'verstrekker van communicatiedienst' nader werd gedefinieerd. Overwegende dat […] in die optiek aan de Belgische wet is onderworpen en op basis van de Belgische wet door de [betrokken inlichtingendienst] kan worden aangesproken. Overwegende dat de [betrokken inlichtingendienst] bij haar vordering […] bij […], herhaald via haar vordering […] bij de [buitenlandse inlichtingendienst], dienvolgens de Belgische wet diende na te leven. Overwegende dat in voorliggend geval art. 18/17 W.I&V diende te worden nageleefd. Dat inderdaad voornoemd artikel 18/17 van toepassing is en niet art. 18/16 W. I&V, nu art. 18/17 W.I&V spreekt van "communicaties onderscheppen" en "er kennis van te nemen", terwijl art. 18/16 integendeel spreekt van het "toegang krijgen tot een informaticasysteem" (…) Overwegende dat het Vast Comité I overigens benadrukt dat, anders dan de [betrokken inlichtingendienst] voorhoudt in haar brief van […] aan de BIM-commissie, de bevraging bij de [buitenlandse inlichtingendienst] niet kan gezien worden als een gewone methode. Dat integendeel deze bevraging moet worden gezien als een*

tweede poging (na de vordering aan […]) om alsnog de inhoud van communicatie te bekomen.'[90]

Motivation insuffisante

Dans le cadre d'une méthode spécifique qui a été suspendue par la Commission BIM, le Comité a demandé un complément d'informations au service de renseignement. Celui-ci n'a répondu que manière sommaire, invoquant notamment la règle du tiers service. Il a cependant ajouté qu'il acceptait la suspension décidée par la Commission BIM. La Comité a jugé '*dat onder deze omstandigheden de beoogde methode dient te worden gestaakt en dat alle door de methode bekomen inlichtingen dienen te verdwijnen*'[91] (dossier 2019/8418).

Dans un autre dossier, il était également question d'une absence de motivation solide de la décision. Dans le dossier 2019/8768, le service de renseignement souhaitait recevoir des données relatives à des communications téléphoniques d'une personne déterminée pour une période de douze mois précédant la date de la décision du dirigeant du service. Le Comité a toutefois jugé que la motivation énoncée dans la décision MRD ne permettait pas '*te beslissen of de in toepassing gebrachte BIM voldoet aan de door de wet gestelde vereisten, inzake bevoegdheid van de dienst en proportionaliteit van de methode*'.[92]

---

90 *'Considérant que la loi du 13 juin 2005 relative aux communications électroniques, et plus particulièrement les articles 9 et 122 à 127, fixe les procédures par lesquelles les services de police ainsi que les services de renseignement et de sécurité ont accès aux communications électroniques. Que l'Arrêté royal du 12 octobre 2010, et plus particulièrement l'article 5, fixe les modalités des demandes relatives aux communications électroniques par les services de renseignement et de sécurité. Considérant que l'Arrêt de la Cour de Cassation du 1er décembre 2015 (affaire Yahoo, P.13.2082.N) confirme qu'une mesure consistant en l'obligation de fournir des données réclamées est prise sur le territoire belge à l'égard de tout opérateur ou fournisseur qui concentre activement ses activités économiques sur les consommateurs en Belgique. Considérant que l'article 3, 11/1 a en outre été modifié dans le sens où la définition de la notion de 'fournisseur d'un service de communication' a été précisée. Considérant que, dans cette optique, […] est soumis à la loi belge et que [le service de renseignement concerné] peut faire appel à lui sur la base de la loi belge. Considérant que [le service de renseignement concerné] dans sa réquisition […], réitérée dans la réquisition […] [au service de renseignement étranger], était dès lors tenu de respecter la législation belge. Considérant qu'en l'espèce, l'art. 18/17 L.R&S devait être respecté. Qu'en effet, c'est l'article 18/17 précité qui s'applique et non l'art. 18/16 L.R&S, puisque l'art. 18/17 L.R&S parle d' "intercepter des communications" et "en prendre connaissance", alors que l'art. 18/16 parle au contraire d' "accéder à un système informatique" (…) Considérant que le Comité permanent R souligne au demeurant que contrairement à ce que soutient [le service de renseignement concerné] dans sa lettre du […] à la Commission BIM, la demande adressée [au service de renseignement étranger] ne peut pas être considérée comme une méthode ordinaire. Qu'au contraire, cette demande doit être considérée comme une seconde tentative (après la réquisition adressée à […]) en vue d'obtenir le contenu de la communication.'* (traduction libre).

91 *'Que dans ces circonstances, la méthode envisagée doit être abandonnée et toutes les informations obtenues par la méthode doivent être supprimées.'* (traduction libre).

92 '*décider si la MRD mise en œuvre répond aux exigences légales en termes de compétence du service et de proportionnalité de la méthode.*' (traduction libre).

En outre, il s'est notamment avéré que :

- *'in de BIM-beslissing nergens sprake is van de twee wettelijk op te volgen dreigingen waarnaar wordt verwezen' ;*
- '*de werkelijke activiteit die door de dienst als een op te volgen dreiging wordt beschouwd en waarvoor een specifieke methode wordt aangevraagd, niet duidelijk of eenduidig omschreven is, evenmin onderbouwd is met feitelijke elementen en op bepaalde vlakken de bevoegdheid van een inlichtingendienst te buiten gaat. Dat onvoldoende wordt aangetoond of en hoe de voorziene methode een reële bijdrage kan leveren aan bepaalde van de in de beslissing vooropgesteld finaliteiten*' ;
- *'het Comité er op wijst dat 'pacifisme' op zich geen op te volgen dreiging kan uitmaken. Het is immers niet meer dan een wereldbeschouwing die duurzame vrede nastreeft en in die optiek volkomen legitiem is in een democratische samenleving' ;*
- '*de definitie van extremisme strikt genomen niet van toepassing is op de ADIV aangezien ze is opgenomen in de artikelen 7 en 8 W.I&V die alleen van toepassing zijn op de Veiligheid van de Staat. Echter, aangezien de toepassing van de methode zoals omschreven in artikel 18/8 W.I&V een verwijzing naar een van de dreigingen uit de artikelen 7 en 8 W.I&V vereist om de maximale duur van de methode te rechtvaardigen, is deze definitie in deze ook van toepassing op de ADIV' ;*
- *'uit de feiten zoals die in de BIM-beslissing zijn hernomen, evenmin blijkt dat de betrokkene of een (extremistische) dreiging vormt' ; 'het Vast Comité I op artikel 2 § 1 tweede lid IW.I&V wijst : 'Bij het vervullen van hun opdrachten zorgen die diensten voor de naleving van, en dragen bij tot de bescherming van de individuele rechten en vrijheden alsook tot de democratische ontwikkeling van de maatschappij.' Het Comité benadrukt in dit kader het belang van de vrijheid van vereniging en de vrijheid van meningsuiting als fundamentele waarden van onze Westerse maatschappij. Het wijst er op dat een inmenging van de overheid in deze rechten en vrijheden alleen kan in uitzonderlijke omstandigheden. Dat deze omstandigheden allerminst blijken uit voorliggend dossier. In die optiek zijn de gehanteerde bewoordingen, de gemaakte redeneringen waarbij men vanuit zeer onzekere feiten nog meer onzekere hypothese opbouwt (als A waar zou zijn – maar hiervoor zijn omzeggens geen aanwijzingen – dan is B eventueel mogelijk…) en de niet-onderbouwde verdachtmakingen en doemscenario's (de term terrorisme wordt zelfs gebruikt), onaanvaardbaar.'*
- *'de BIM-beslissing tot slot op sommige plaatsen melding maakt van de of een finaliteit van de methode terwijl deze finaliteit niet aantoonbaar kan gerealiseerd worden via de geviseerde methoden.'*[93]

[93] – *'dans la décision MRD, il n'est nulle part question des deux menaces légales auxquelles il est fait référence' ;*

Le Comité s'est saisi et a posé plusieurs autres questions au service de renseignement concerné. Le Comité a pris une décision à ce sujet en 2020.

Différence entre la période figurant dans le projet d'autorisation et celle figurant dans l'autorisation finale

La Commission BIM a rendu son avis conforme sur un projet d'autorisation portant sur une méthode exceptionnelle pour '*une période de deux semaines, à partir de mon autorisation*.' Cependant, il n'était pas fait mention d'une période de deux mois dans l'autorisation finale. La Commission BIM a alors suspendu l'autorisation pour la période qui excédait les deux semaines à compter de l'autorisation du dirigeant du service. Le Comité permanent R s'est rallié à cette décision de suspension (dossier 2019/8421).

Avertissement tardif de la Commission BIM

Dans deux dossiers, un service de renseignement souhaitait prolonger une méthode en cours (dossiers 2019/8788 et 2019/8968). Cependant, la Commission BIM n'a été informée de la prolongation que quelques jours après le terme de la décision initiale. La nouvelle méthode n'était donc pas couverte par une décision

---

– *'l'activité réelle qui est considérée par le service comme une menace à suivre et pour laquelle une méthode spécifique est demandée, n'est pas décrite de manière claire ou univoque et n'est pas étayée par des éléments factuels et, à certains égards, sort du champ de compétence d'un service de renseignement. Qu'il n'est pas suffisamment démontré si et comment la méthode prévue peut apporter une réelle contribution à certaines finalités énoncées dans la décision' ;*
– *'le Comité souligne que le 'pacifisme' ne peut en soi constituer une menace à suivre. En effet, ce n'est rien d'autre qu'une vision du monde qui aspire à une paix durable et qui, de ce point de vue, est parfaitement légitime dans une société démocratique'* ;
– *'la définition de l'extrémisme stricto sensu ne s'applique pas au SGRS puisqu'elle est reprise aux articles 7 et 8 L.R&S qui s'appliquent uniquement à la Sûreté de l'État. Toutefois, vu que l'application de la méthode telle que décrite à l'article 18/8 L.R&S exige une référence à l'une des menaces visées aux articles 7 et 8 L.R&S pour justifier une durée maximale de la méthode, cette définition est, dans le cas présent, également d'application pour le SGRS' ;*
– *'d'après les faits tels que repris dans la décision MRD, il n'apparaît pas non plus que l'intéressé représente une menace (extrémiste)' ; 'le Comité permanent R rappelle l'article 2 § 1er, alinéa 2 L.R&S : 'Dans l'exercice de leurs missions, ces services veillent au respect et contribuent à la protection des droits et libertés individuels, ainsi qu'au développement démocratique de la société.' Dans ce contexte, le Comité souligne l'importance de la liberté d'association et de la liberté d'expression en tant que valeurs fondamentales de notre société occidentale. Il fait remarquer qu'une ingérence des autorités dans ces droits et libertés ne se justifie que dans des circonstances exceptionnelles. Que ces circonstances ne ressortent nullement du présent dossier. Dans cette optique, le libellé utilisé, le raisonnement développé, à savoir qu'une hypothèse encore plus incertaine est échafaudée à partir de faits très incertains (si A était vrai – mais il n'y a pour ainsi dire aucune indication en ce sens – alors B est éventuellement possible…) et les soupçons et scénarios catastrophes non étayés (le terme terrorisme est même employé), est inacceptable.' ;*
– *'enfin, à certains endroits, la décision MRD mentionne la ou une finalité de la méthode, alors que cette finalité ne peut être concrétisée par le biais des méthodes visées.'* (traduction libre).

valable dans cet intervalle. En effet, '*pas vanaf het moment van betekening de verlenging van de methode kon worden opgestart*'.[94] Dans le dossier 2019/8788, le service de renseignement avait '*in quarantaine […] gehouden*'[95] ces données recueillies illégalement. Le Comité a toutefois souligné que '*het feit dat de gegevens "in quarantaine worden gehouden" en niet beschikbaar zijn voor exploitatie niets verandert aan de wettelijke bepalingen ter zake. Overwegende dat de BIM-Commissie dan ook een exploitatieverbod uitsprak krachtens artikel 18/3 § 6 W.I&V.*'[96]

La proportionnalité et la subsidiarité[97]

Un service de renseignement souhaitait procéder à la prise de connaissance de données d'appel et de localisation de moyens de communication de trois targets (dossier 2019/8150). Pour un de ces targets, il n'y avait pas le moindre problème : '*Attendu qu'en ce qui concerne le "target" principal dans le dossier, la décision du dirigeant du service est suffisamment motivée et la mesure est proportionnelle à la menace*'. Mais ce n'était pas le cas pour les deux autres personnes. Il s'est avéré que des membres de la famille du premier target n'étaient pas domiciliés à la même adresse. De plus, il n'est en aucune manière apparu que ces personnes seraient impliquées dans les activités du membre de leur famille, ni que le target aurait utilisé les moyens de communication des deux autres personnes. '*Attendu que le simple fait qu'un lien familial existe entre ces personnes n'est en soi pas suffisant pour justifier une intrusion dans la vie privée*'. Par conséquent, la méthode était illégale à ce niveau.

Quand un service de renseignement a voulu observer pendant deux mois un lieu qui allait abriter une réunion extrémiste un jour précis, la Commission BIM et ensuite le Comité permanent R sont intervenus : '*Attendu que la décision de méthode écifique est disproportionnée en ce qu'elle ne mentionne pas en quoi l'observation peut être réalisée pendant deux mois, alors que la menace avancée porte sur un événement à date fixe, sur un seul jour*'. En ce qui concerne le jour même de la réunion, la mesure prise n'était pas disproportionnée : '*Attendu que la décision est motivée par la nécessité d'identifier des personnes issues [d'un milieu extrémiste] et participant à un meeting, dont le lieu et la date sont précisés, et au cours duquel des orateurs [extrémistes] prendront la parole ; que ces*

94 '*la prolongation de la méthode ne pouvait démarrer qu'à partir de la notification.*' (traduction libre).

95 '*gardé en quarantaine*' (traduction libre).

96 '*le fait que les données soient "gardées en quarantaine" et ne soient pas disponibles pour être exploitées ne change rien aux dispositions légales en la matière. Considérant que la Commission BIM a donc prononcé une interdiction d'exploitation en vertu de l'article 18/3 § 6 L.R&S.*' (traduction libre).

97 Il y avait un dossier (mais qui n'a pas donné lieu à une décision juridictionnelle) dans lequel l'accent a été mis sur le principe de subsidiarité.

informations ne peuvent être recueillies par méthode ordinaire ; que l'utilisation de moyens techniques est justifiée par la difficulté d'observer les lieux visés' (dossier 2019/8224). En conclusion, la méthode n'était légale que le jour de la réunion.

Dans le cadre d'un contrôle d'une méthode spécifique, la Commission BIM a demandé davantage d'informations sur la menace d'espionnage qui était mentionnée et sur le lien présumé entre le target et cette éventuelle menace (dossiers 2019/8377 et 2019/8401). Lorsque le service a répondu ne pas disposer des informations demandées, la Commission BIM a suspendu la méthode. En outre, à la demande du Comité permanent R '*om bepaalde aspecten van de specifieke methode nader te motiveren aangezien de wijze waarop de beslissing was gemotiveerd, niet toeliet te bevestigen dat de methode beantwoordde aan de wettelijke vereisten van legaliteit, proportionaliteit en subsidiariteit*'[98], le service concerné a répété essentiellement ce qui figurait dans l'autorisation d'origine. Le service a lui-même reconnu que les quelques données supplémentaires '*de ontoereikende proportionaliteit niet corrigeren*'[99] et qu'il acceptait certainement la suspension décidée par la Commission BIM. Le Comité a dès lors décidé que la méthode n'avait été pas autorisée de manière légale.

La légalité d'une méthode concernant les techniques employées, des données recueillies, la durée de la mesure et la nature de la menace

Objet imprécis

Le service de renseignement concerné souhaitait observer plusieurs targets d'origine étrangère dans '*des lieux non accessibles au public qui ne sont pas soustraits à la vue*', sans pénétrer dans ces lieux (art. 18/4 § 2 L.R&S). Le service avait l'intention d'utiliser des moyens techniques. Dans ce dossier, il était question de caméras (mobiles) et de *closed-circuit television* (CCTV), alors que dans la décision du dirigeant du service, il était fait mention du placement d'une balise. Il est en outre apparu que le véhicule d'un seul target était connu. La Commission BIM a demandé davantage d'explications au service concerné. De la réponse obtenue, il était encore impossible de déterminer clairement sur quels véhicules des balises seraient placées. Par conséquent, l'ordre a été donné de faire cesser le placement de balises sous les véhicules des autres targets (dossier 2019/8109).

Une méthode exceptionnelle au lieu d'une méthode spécifique

Un service de renseignement a requis, par le biais d'une méthode spécifique, le concours d'un opérateur en vue d'obtenir les données de trafic d'une personne

98 '*de motiver davantage certains aspects de la méthode spécifique, car la manière dont la décision était motivée ne permettait pas de confirmer que la méthode était conforme aux exigences légales de légalité, de proportionnalité et de subsidiarité.*' (traduction libre).

99 '*ne corrigent pas l'insuffisance de la proportionnalité*' (traduction libre).

déterminée. Le Comité permanent R a toutefois observé que l'opérateur ne pouvait demander ces données via ses propres fichiers, mais bien via un fichier qui était localisé chez l'intéressé : '*Considérant que les données […] ne sont disponibles que par le biais d'une intrusion dans le système informatique où elles sont stockées, à savoir [chez] la personne faisant l'objet des méthodes de recueil de données. Considérant qu'une telle intrusion constitue une méthode exceptionnelle de recueil des données prévue à l'article 18/16 L.R&S.*' Par conséquent, les données ont été détruites (dossier 2019/8446).

Immunités diplomatiques

La méthode visée dans le dossier 2019/8483 consistait à écouter des communications pendant deux mois à compter de la date de l'autorisation du dirigeant du service (et après l'avis conforme de la Commission BIM). Il est cependant apparu que la méthode portait sur des numéros de téléphone qui étaient enregistrés au nom d'une mission permanente auprès d'une instance internationale établie en Belgique.

La protection offerte par la Convention de Vienne du 18 avril 1961 sur les relations diplomatiques ne s'appliquait pas dans le cas présent. Cette convention porte en effet sur les missions diplomatiques bilatérales traditionnelles. Mais l'instance internationale est soumise à sa propre réglementation, qui oblige la Belgique à respecter les immunités diplomatiques habituelles. Il est fait référence ici aux immunités et privilèges repris dans la Convention de Vienne.

Le service de renseignement estimait ne pas devoir en tenir compte puisque les numéros auxquels il voulait appliquer la mesure seraient utilisés exclusivement par le target. Une première analyse a toutefois montré que les numéros étaient partagés avec d'autres personnes que le target. '*Overwegende dienvolgens dat de omstandigheden en het feitelijk relaas zoals medegedeeld via het ontwerp van machtiging aan de BIM-Commissie […] op die manier niet overeenstemt met de realiteit.*'[100] Le service a lui-même constaté que les conditions dont il était question dans l'avis conforme n'étaient plus remplies et a décidé de mettre un terme à la méthode. Le Comité a dès lors établi '*dat aldus de beoogde methode dient te worden gestaakt en dat alle door de methode bekomen inlichtingen dienen te verdwijnen.*'[101]

Calcul de la période 'préalable à la décision'

Un service de renseignement a décidé de procéder au repérage de moyens de communication électroniques et à la localisation de communications

100 *'Considérant, par conséquent, que de cette manière les circonstances et le récit factuel tels que communiqués par le biais du projet d'autorisation à la Commission BIM […] ne correspondent pas à la réalité.'* (traduction libre).

101 *'que la méthode envisagée doit donc être abandonnée et que toutes les informations obtenues grâce à cette méthode doivent être supprimées.'* (traduction libre).

électroniques pour une période de douze mois précédant la décision (dossier 2019/8794). Cette décision a été prise le 29 du mois X. Le Comité a établi que '*de "periode voorafgaand aan de beslissing" zich in casu noodzakelijkerwijs dient te situeren tussen 28 X 2018 en 29 X 2019.*'[102] Le service a toutefois demandé des données pour la période du 20 X 2018 au 19 X 2019. '*Dat aldus moet worden vastgesteld dat gedurende de periode 20 X 2018 tot en met 27 X 2018 verkeerdelijk gegevens werden opgevraagd, wat niet conform is met artikel 18/8 § 2 W. I&V.*'[103]

Cette problématique s'est également présentée dans le dossier 2019/9024. '*Qu'en l'espèce, les méthodes de repérage et de localisation de communications électroniques décidées concernent une menace potentielle liée au domaine du terrorisme ; Attendu que dans le cadre d'une menace potentielle de terrorisme, et en vertu de l'article précité, le dirigeant d'un service peut uniquement requérir le repérage et la localisation de données liées à des communications électroniques pour une période de 12 mois préalables à la décision ; Que le terme préalable doit être compris comme instituant la date de la décision comme un point de départ non inclus dans le calcul du délai légal visé ; Que la décision dont question étant datée du 18 X 2019, la récolte des données ne pouvait donc pas excéder une période de 12 mois précédant le jour de la décision ; Qu'en l'espèce la période maximale de récolte rétroactive de données pouvait donc uniquement s'étendre [jusqu'au] 17 X 2018.*'

La légalité de l'exécution d'une méthode légale

Mise en œuvre d'une méthode spécifique avant d'en informer la Commission BIM

Dans le dossier 2019/9097, le service de renseignement avait informé la Commission BIM le lendemain de l'envoi de sa réquisition à un opérateur. Cette '*mise en œuvre […] ne respecte pas les prescrits de l'article 18/3, § 1er de la L.R&S ; Qu'en conséquence, le réquisitoire adressé à l'opérateur en date du 4 X 2019 à 16h49 et les résultats obtenus sur la base de celui-ci doivent être considérées comme obtenu illégalement.*'

II.3. CONCLUSIONS

Le Comité permanent R formule les conclusions générales suivantes :

– En 2019, 2444 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de

[102] *qu'en l'espèce, la "période précédant la décision" doit nécessairement se situer entre le 28 X 2018 et le 29 X 2019.*' (traduction libre).

[103] *'Que force est donc de constater qu'entre la période du 20 X 2018 au 27 X 2018 inclus, des données ont été demandées par erreur, ce qui n'est pas conforme à l'article 18/8 § 2 L.R&S.*' (traduction libre).

renseignement : 2230 par la VSSE (1781 spécifiques et 449 exceptionnelles) et 214 par le SGRS (138 spécifiques et 76 exceptionnelles). Après une augmentation constante du nombre de MRD mises en œuvre ces dernières années, on remarque pour la première fois une stagnation.

- La VSSE continue de se tailler la part du lion, avec 91,2 % des méthodes mises en œuvre.
- Une ventilation des chiffres globaux permet de constater une hausse notable des méthodes mises en œuvre par le SGRS, tant des méthodes spécifiques (de 102 à 138) que des méthodes exceptionnelles (de 28 à 76, soit plus du double). À la VSSE, ce sont les méthodes exceptionnelles qui ont connu une croissance marquée (de 344 à 449). La stagnation observée malgré toutes ces augmentations s'explique par une forte diminution du nombre de méthodes spécifiques mises en œuvre (de 1971 à 1781) par la VSSE.
- En ce qui concerne les méthodes ordinaires qui consistent à adresser une réquisition à des opérateurs afin d'identifier certains moyens de communication, on note, contrairement à ces dernières années, une diminution d'environ 12 %.
- Dans le contexte de la mise en œuvre des méthodes particulières de renseignement, le SGRS s'est, comme toujours, davantage concentré sur l'espionnage, suivi de l'ingérence. La VSSE a, quant à elle, focalisé son attention sur le terrorisme (et le processus de radicalisation), suivi par l'espionnage.
- Le Comité a été saisi dans seize dossiers, à savoir quatre saisines d'initiative et douze saisines de plein droit, après la suspension décidée par la Commission BIM pour illégalité (art. 43/4 L.R&S). Les illégalités concernaient notamment une motivation insuffisante, un avertissement tardif de la Commission BIM, un objet imprécis, ou encore une période de collecte trop longue.

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

III.1. LES COMPÉTENCES DU SGRS ET LA MISSION DE CONTRÔLE DU COMITÉ PERMANENT R[104]

Dès 2017, la compétence du SGRS dans le cadre des interceptions de sécurité a été élargie.[105] Les interceptions pouvaient alors porter sur des communications *'émises ou reçues à l'étranger'*. Cette possibilité vaut pour presque toutes les missions du SGRS. Il est d'ailleurs intéressant d'observer que les descriptions des missions ont, elles aussi, été élargies. Le législateur a en même temps introduit deux autres méthodes, à savoir l'intrusion dans un système informatique' (art.44/1 L.R&S) et la prise d'images animées' (art.44/2 L.R&S). Par ailleurs, la manière dont le Comité peut contrôler ces méthodes a été modifiée.

Le contrôle *préalable* aux interceptions, prises d'images fixes ou animées s'effectue sur la base d'une liste établie annuellement.[106] Cela signifie qu'en plus du plan d'interception annuel, le SGRS doit également élaborer un plan d'intrusions et d'images.[107]

Le SGRS doit envoyer ces listes au ministre de la Défense au mois de décembre pour autorisation. Le ministre prend une décision endéans les dix

---

104 Voir articles 44 à 44/5 inclus L.R&S.

105 À propos des modifications de loi successives relatives à la compétence d'interception, voir COMITÉ PERMANENT R, *Rapport d'activités 2018*, 63 et suiv.

106 Ceci n'implique pas que le Comité permanent R a la compétence d'approuver ou non la liste approuvée par le ministre.

107 Dans ces plans, le SGRS dresse une liste *'d'organisations et d'institutions qui feront l'objet d'interceptions de leurs communications, d'intrusions dans leurs systèmes informatiques ou de prises d'images fixes ou animées dans le courant de l'année à venir. Ces listes justifieront pour chaque organisation ou institution la raison pour laquelle elle fera l'objet d'une interception, intrusion ou prise d'images fixes ou animées en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°, et mentionneront la durée prévue'* (art. 44/3 L.R&S).

jours ouvrables et doit la communiquer au SGRS[108], qui transmet à son tour les listes pourvues de l'autorisation ministérielle au Comité permanent R.[109]

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

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

Que peut faire le Comité permanent R en cas d'irrégularité ? L'article 44/4 L.R&S stipule que, '*le Comité permanent de contrôle des services de renseignement, sans préjudice des autres compétences attribuées à ce Comité par la loi du 18 juillet 1991, a le droit de faire cesser des interceptions, intrusions ou prises d'images en cours lorsqu'il apparaît que celles-ci ne respectent pas les dispositions légales ou l'autorisation [ministérielle]. Il ordonne l'interdiction d'exploiter les données recueillies illégalement et leur destruction, selon les modalités à fixer par le Roi.*' Malgré la recommandation pressante du Comité[110], un tel arrêté d'interception n'a toujours pas été pris.[111] Aussi, le Comité recommande une nouvelle fois de le faire au plus vite.[112]

---

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

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

110 COMITÉ PERMANENT R, *Rapport d'activités 2018*, 131.

111 Le Comité doit de toute manière motiver sa décision de manière circonstanciée et la communiquer au ministre et au SGRS.

112 Un arrêté royal doit également être pris en ce qui concerne les modalités relatives au concours des opérateurs d'un réseau ou des fournisseurs de services de communications électroniques (art. 44/5 L.R&S).

III.2. LES CONTRÔLES EFFECTUÉS EN 2019

III.2.1. LE CONTRÔLE PRÉALABLE À L'INTERCEPTION, L'INTRUSION OU LA PRISE D'IMAGES

Le Comité permanent R avait formulé une série de remarques importantes concernant les 'Plans d'interception'. Les principales remarques portaient sur les différences en termes de priorité entre, d'une part, le Plan Directeur du Renseignement[113] et, d'autre part, les interceptions SIGINT prévues et le caractère trop général de la description des organisations et institutions qui feraient l'objet d'interceptions. Dans le 'plan d'interception 2019', qui a été transmis au Comité fin janvier 2019, le SGRS a décrit en détail les organisations susceptibles de faire l'objet d'interceptions. Le Comité n'a dû formuler que quelques remarques çà et là.

En revanche, les plans de prises d'images et d'intrusions étaient une fois encore plutôt sommaires. Ils ont été discutés lors d'une réunion de travail entre le Comité permanent R et le SGRS en mars 2019. Le Comité a décidé de reprendre cette thématique dans l'enquête de contrôle qu'il a initiée en 2019 et intitulée *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R'.*

III.2.2. LE CONTRÔLE PENDANT L'INTERCEPTION, L'INTRUSION OU LA PRISE D'IMAGES

En 2019, le Comité n'a pas visité les installations d'où sont effectuées les interceptions ; ces visites ont été reportées au second semestre de 2020. Elles étaient pourtant planifiées dans le cadre de l'enquête de contrôle précitée. Ce report s'explique de plusieurs manières. Tout d'abord, les premiers modules de l'enquête de contrôle, à savoir l'étude des articles 16/2 et 16/3 L.R&S, ont pris plus de temps et de moyens que prévu. Ensuite, le Comité a été confronté à d'autres priorités et, pour certains aspects, ce contrôle s'est avéré techniquement impossible (par ex. les prises d'images).

[113] Il s'agit d'un plan établi par l'ancienne Direction I reprenant les pays à suivre et leur degré de priorité.

III.2.3. LE CONTRÔLE APRÈS L'EXÉCUTION DE LA MÉTHODE

Le Comité a reçu onze '*listes mensuelles*[114] *des pays ou des organisations ou institutions ayant effectivement fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images durant le mois écoulé*' et qui justifient '*la raison pour laquelle l'écoute, l'intrusion ou la prise d'images a été effectuée en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°*'.

En ce qui concerne les intrusions, le Comité a dû rappeler à plusieurs reprises le SGRS à ses obligations et préciser que le Comité doit recevoir un rapport chaque mois, même en l'absence d'intrusions. En octobre 2019, le Comité a reçu un courrier du SGRS signalant qu'aucune intrusion n'avait eu lieu cette année-là. À la suite de cette lettre, le Comité a également reçu la liste mensuelle des intrusions. Le Comité a reçu trois listes en tout. Le contrôle des listes mensuelles d'intrusions et de prises d'images a été repris dans le cadre de l'enquête de contrôle précitée.

114 Il manquait la liste de novembre 2019 concernant les interceptions et prises d'images.

CHAPITRE IV
MISSIONS PARTICULIÈRES

Au fil du temps, le Comité permanent R s'est vu confier plusieurs missions spécifiques qui ne trouvent pas leur origine dans une disposition légale, mais qui répondent à un besoin concret. Ces missions complémentaires ont été attribuées au Comité en étroite concertation avec celui-ci.

IV.1. CONTRÔLE DES ACTIVITÉS DU BATAILLON ISTAR

Le Comité permanent R avait déjà donné son avis sur les activités de renseignement menées par le Bataillon ISTAR *(Intelligence Surveillance Target Acquisition and Reconnaissance)* dans le cadre d'opérations à l'étranger. Le Comité avait souligné à cet égard que, compte tenu de l'augmentation du nombre de missions à l'étranger, la création du bataillon correspondait à un besoin sans cesse croissant de capacités *battlefield intelligence*. Mais il rappelait que la Loi organique du 30 novembre 1998 ne reconnaît que deux services de renseignement (art. 2 L.R&S). Il avait signalé au Parlement, au ministre de la Défense et au CHOD que ce bataillon développait, ne serait-ce qu'en partie, des activités de renseignement.

En l'absence de solutions légales ou structurelles à court terme, une solution provisoire a été trouvée fin avril 2018. Il s'agit en l'occurrence d'un protocole d'accord entre le SGRS et le CHOD[115] qui définit les attributions et les compétences du Bataillon ISTAR en matière de HUMINT et de capacité d'analyse. En outre, l'organisation d'un contrôle technique et juridique a été élaboré. Par contrôle

[115] Protocole d'Accord du 24 mai 2018 entre le CHOD et le SGRS concernant la capacité HUMINT et la capacité d'analyse du Bn ISTAR. La Commission d'enquête parlementaire 'Attentats' a insisté sur ce point : *'Bien que la commission d'enquête estime que les missions du Bataillon ISTAR sont importantes pour la sécurité de nos militaires, elle considère que les relations entre celui-ci et le SGRS devraient être réglées formellement par le biais d'un protocole de coopération décrivant clairement de quelle façon et à quelles conditions le Bataillon ISTAR pourrait contribuer à renforcer la position d'informations du SGRS. Il s'indiquerait également dans ce cadre de charger le Comité permanent R du contrôle de cette mission de soutien au Bataillon ISTAR.'*. Voir *doc. parl.*, Chambre, 2016-17, n° 54-1752/008, 306.

technique, il y a lieu d'entendre le contrôle sur la bonne application des directives en matière d'analyse et de directives HUMINT ainsi qu'un contrôle sur les accords particuliers entre le CHOD et le SGRS. Par contrôle juridique, il y a lieu d'entendre le contrôle de la bonne application du protocole. Ces missions relèvent du SGRS.

Le Bataillon ISTAR transmet d'initiative au SGRS les règlements et directives internes. Le contrôle s'effectue moyennant des visites aux installations du Bataillon ISTAR et aux zones où il exerce ses opérations et activités. L'analyse des documents et des auditions viennent compléter ce contrôle.

Le Comité permanent R a été désigné dans le protocole pour exercer un contrôle – ne serait-ce qu'indirect – sur les activités du bataillon. Pour ce faire, le SGRS transmet au ministre de la Défense, au chef de la Défense et au Comité permanent R un rapport trimestriel sur toute mission d'enquête.

En 2019, le Comité a effectivement reçu quatre rapports de contrôle, qui ont montré que le bataillon ISTAR déployait peu d'activités entrant dans le champ d'application du protocole d'accord susmentionné. Selon le SGRS, les activités de renseignement développées par le bataillon ISTAR répondaient aux réglementations et directives.

L'analyse de ces rapports fera l'objet d'une enquête ultérieure. Compte tenu du fait qu'ISTAR développe peu d'activités HUMINT, le Comité n'en a pas fait une priorité.

IV.2. CONTRÔLE DES FONDS SPÉCIAUX

La Cour des comptes contrôle la légalité, la légitimité et l'efficacité de toutes les dépenses, y compris, en principe, de toutes les dépenses des services de renseignement. Cependant, vu le caractère sensible de la matière, une partie du budget de la VSSE et du SGRS (à savoir les 'fonds spéciaux' avec des dépenses destinées, par exemple, aux opérations et aux informateurs) n'est pas examinée par la Cour des comptes. Pour la VSSE, le contrôle de ces dépenses est effectué par le directeur de la Cellule politique générale du ministre la Justice. Mi-2018, la Cour des comptes a exprimé son intention de réaliser un contrôle périodique de ces fonds à partir de la clôture des comptes de 2018. En 2020, le Comité a reçu une copie du contrôle de l'exercice comptable 2018 effectué par la Cour des Comptes en 2019.[116]

Le contrôle des fonds spéciaux du SGRS est réalisé par un représentant du Cabinet du ministre de la Défense, et ce quatre fois par an. Depuis 2010, ce contrôle se déroule en présence du président du Comité permanent R, un souhait exprimé par l'ancien ministre de la Défense de ne plus effectuer lui-même le

116 COUR DES COMPTES, *Sûreté de l'État. Contrôle 2019 des fonds spéciaux. Rapport adressé au ministre de la Justice*, 20 mai 2020.

contrôle tel qu'instauré en 1962. En février 2019, le président a effectivement assisté à un de ces contrôles. Toutefois, un courrier a été adressé au Vice-Premier ministre et ministre des Affaires étrangères, des Affaires européennes et de la Défense, l'informant que le Comité n'assumerait plus cette mission. En effet, *"nous estimons que le contrôle actuel basé sur un échantillonnage limité ne correspond pas aux exigences d'un contrôle réellement effectif et pourrait, en outre, engager tant la responsabilité ministérielle que celle du Comité permanent R*". Il était par ailleurs suggéré que conformément au contrôle des fonds de la VSSE, une mission soit assignée à la Cour des Comptes. En février 2020, la Cour des Comptes a appuyé cette initiative et a informé le ministre des Affaires étrangères et de la Défense de sa disponibilité à effectuer un contrôle formel des comptes. Et la Cour d'ajouter qu'elle pourrait recourir à une assistance technique, telle que proposée par le Comité permanent R.[117] Le Comité pourrait ainsi *"exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds"*. En 2019, il a été décidé de démarrer une enquête de suivi en 2020 sur la gestion, l'utilisation et le contrôle des fonds spéciaux.[118]

IV.3. CONTRÔLE DU SUIVI DE MANDATAIRES POLITIQUES

Lors de débats (parlementaires), une question a déjà été posée à maintes reprises, à savoir si et dans quelle mesure les services de renseignement belges suivaient (ou étaient autorisés à suivre) des mandataires politiques, et quelles règles devaient être observées à cet égard.[119]

Depuis début janvier 2018, une nouvelle note de service classifiée 'confidentiel' du 13 décembre 2017 est d'application au sein de la VSSE.[120] Ce service envoie deux types de rapports au ministre de la Justice et au Premier ministre, avec copie au Comité permanent R. Il s'agit, d'une part, de rapports

---

117 *"Ce contrôle sera périodique et comportera, outre un examen des processus et un contrôle de caisse, un contrôle formel réalisé par sondage et portant sur l'existence des pièces justificatives conformes aux instructions et approuvées par les fonctionnaires compétents. Le contrôle ne portera pas sur le bien-fondé ou la bonne gestion des opérations sous-jacentes et sera mis en œuvre, dans le respect des missions du SGRS, par des auditeurs disposant de l'habilitation de sécurité requise"*.

118 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 12-15 ('II.2. La gestion, l'utilisation et le contrôle des fonds spéciaux').

119 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 19-31 (II.2. 'Dossiers réservés à la Sûreté de l'État'). Ce n'était d'ailleurs pas la première fois que le Comité enquêtait sur les activités des services de renseignement à l'égard de mandataires politiques (COMITÉ PERMANENT R, *Rapport d'activités 1998*, 60 et suiv. ; *Rapport d'activités 1999*, 13 et suiv.). Voir également *Rapport d'activités 2013*, 37 et suiv. ('II.4. Le suivi de mandataires politiques par les services de renseignement').

120 La note de service a été actualisée en juin 2020 en vue d'améliorer les rapports destinés à la direction sur les activités disruptives.

ponctuels sur des mandataires politiques qui contribuent à l'apparition d'une menace et, d'autre part, d'un aperçu trimestriel de l'ensemble des documents dans lesquels des mandataires politiques sont mentionnés.[121] Le ministre de la Justice avait précédemment marqué son accord sur le '*principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991*'.[122]

En exécution des principes figurant dans la note de service susmentionnée, le Comité permanent R a effectivement été le destinataire de deux types de rapports en 2019. En raison de la tenue des élections communales en 2018 et des élections régionales, fédérales et européennes en 2019, une attention accrue sur les mandataires politiques a pu être constatée. En effet, dans la période qui précède et qui suit directement les scrutins, la VSSE s'octroie un rôle dans le bon déroulement de ces scrutins, du moins en ce qui concerne les menaces que la loi lui impose de surveiller (par ex. l'ingérence). En outre, un projet commun a été mis au point avec le service de renseignement militaire spécifiquement autour d'éventuelles menaces russes en ligne (cyber, désinformation) visant les élections de mai 2019. Par la suite, des concertations régulières ont été organisées avec le Centre pour la Cybersécurité Belgique (CCB) et la Direction générale du Centre de crise (DGCC).[123]

Malgré ses demandes répétées, le Comité n'a reçu, en 2019, aucune information du SGRS, que le Comité avait pourtant exhorté, comme la VSSE d'ailleurs, à adopter une directive uniforme, assortie de règles claires et univoques quant au recueil, au traitement, à la consultation, au stockage et à l'archivage des informations relatives aux mandataires politiques. Le SGRS ne dispose pas d'une procédure spécifique (SOP) pour traiter cette thématique, pas plus qu'il n'a défini de procédure pour informer le Comité permanent R.

Étant donné qu'il n'est mentionné nulle part ce que le Comité permanent R est censé faire des informations précitées, il a pris l'initiative d'élaborer une méthodologie autour de la 'problématique du suivi des mandataires politiques par les services de renseignement et le rôle du Comité permanent R'. Cette méthodologie a été approuvée par la Commission parlementaire de suivi en 2020.

---

121 Les mandataires politiques visés sont les ministres des différents gouvernements, le Commissaire belge siégeant à la Commission européenne et les membres des différents parlements et assemblées, y compris les membres belges du Parlement européen. Les autres élus ou mandataires désignés ne sont pas concernés. (par ex. les échevins au niveau communal ou les gouverneurs au niveau provincial).

122 Voir le courrier du ministre de la Justice daté du 26 juillet 2018 et adressé au Comité permanent R sur 'le recueil d'informations par un service de renseignement concernant une personne exerçant un mandat politique'.

123 Courant 2019, le Comité permanent R a ouvert une enquête de contrôle, intitulée 'Enquête de contrôle sur la manière dont les services de renseignement belges suivent les risques liés à une éventuelle ingérence d'acteurs étrangers dans le processus électoral belge, sur la manière dont ils tentent de contrer les menaces potentielles et sur la manière dont ils font rapport aux autorités, en particulier en ce qui concerne le risque de cyber-ingérence ou de cyber-attaques' (cf. I.7.4).

IV.4. DAG HAMMARSKJÖLD ET LES ARCHIVES DU RENSEIGNEMENT BELGE

Dans la nuit du 17 au 18 septembre 1961, l'ancien secrétaire général des Nations Unies, Dag Hammarskjöld, a perdu la vie dans un accident d'avion lors d'une mission de paix au Congo. Malgré les soupçons d'attentat, l'origine du crash aérien n'a jamais été déterminée.

L'ancien Secrétaire général des Nations Unies Ban Ki-Moon a ouvert une enquête sous la direction de la 'Personnalité éminente', Mohamed Chande Othman.[124] Il était demandé aux États membres qui détenaient des informations pertinentes sur ce dossier de désigner une personne indépendante pour (faire) examiner leurs archives et de transmettre les résultats aux Nations Unies. Le 16 avril 2018, les ministres de la Justice et de la Défense ont désigné Guy Rapaille[125], qui présidait alors le Comité permanent R, et le Professeur Kris Quanten, lieutenant-colonel et professeur à l'École royale militaire comme '*independent and high-ranking officials*', pour assister les Nations Unies dans l'enquête sur la mort du secrétaire général. Fin septembre 2018, ils ont adressé leur rapport aux Nations Unies. Début novembre 2018, le Juge Othman a transmis à l'Assemblée générale des Nations Unies un premier rapport intermédiaire ; le rapport final a suivi en 2019.[126, 127]

Fin janvier 2019, le juge Othman a demandé à la Belgique d'étendre la portée de l'enquête. Cette demande résultait de certaines informations apparues dans les enquêtes menées dans d'autres pays.[128] Il a été demandé plus particulièrement de vérifier de quelles informations les services de renseignement belges disposaient sur la présence et/ou les activités du personnel du renseignement et de la Défense d'un autre pays au Katanga en septembre 1961. En juin 2019, les Nations Unies ont transmis un rapport à ce propos.[129] Avec le lieutenant-colonel Quanten de l'École royale militaire, le Comité est arrivé à la conclusion que "*the*

---

124 UNITED NATIONS, General Assembly, *71/260 Investigation into the conditions and circumstances resulting in the tragic death of Dag Hammerskjöld and of the members of the party accompanying him*, Resolution adapted on 23 December 2016, 31 January 2017, A/RES/71/260 (en A/C.5/72/19).

125 Guy Rapaille étant parti à la retraite, les ministres de la Justice et des Affaires étrangères ont demandé au Comité permanent R, mi-mars 2019, de désigner un de ses membres pour poursuivre l'enquête. Le Comité a décidé de confier cette mission au président, Serge Lipszyc.

126 La thématique a de nouveau fait l'objet d'un film (*Cold Case Hammerskjöld* van M. BRÜGGER) et de diverses publications (H. MELBER, *Dag Hammerskjöld, the United Nations and the decolonisation of Africa*, Hurst Publishers, Londres, 2019 ; M. PICARD, *Ils ont tué Monsieur H. Congo 1961. Le complot des mercenaires français contre l'ONU*, Seuil, 2019).

127 Voir www.hammarskjoldinquiry.info/pdf/ham_263_UN_Final_Report_complete.pdf.

128 Dans ce cadre, les *Independent Appointees* français, suédois et allemands ont demandé un échange mutuel des rapports intérimaires.

129 BELGIAN STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE, Review investigation of the information available to the intelligence services regarding the death of Dag Hammarskjôld. Final Report, June 2019, 29.

research carried out […] within the framework of this investigation, did not reveal any information that sheds new light on the precise circumstances that led to the death of Mr. Dag Hammarskjöld and his company in September 1961 ».[130] Début 2020, de nouveaux renseignements ont encore permis d'apporter des précisions.

130 "*les recherches effectuées […] dans le cadre de cette enquête ne révèlent aucun élément apportant un nouvel éclairage sur les circonstances précises ayant mené au décès de M. Dag Hammarskjöld et de ses accompagnants en septembre 1961.* » (traduction libre).

CHAPITRE V
LE COMITÉ PERMANENT R EN SA QUALITÉ D'AUTORITÉ DE CONTRÔLE COMPÉTENTE DANS LE CADRE DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

V.1. INTRODUCTION

Le Règlement Général sur la Protection des Données 2016/679 (RGPD)[131] et la Directive 2016/680 (Directive)[132] règlent la manière dont les acteurs publics et privés doivent opérer lorsqu'ils collectent, sauvegardent, conservent et communiquent des données à caractère personnel. Les deux instruments européens ont donné lieu à quelques modifications de loi substantielles au niveau national : en décembre 2017, l'Autorité de protection des données (APD)[133] – qui a succédé à la Commission Vie privée – a été créée et en juillet 2019, une nouvelle Loi relative à la protection des données (LPD) a été votée.[134] Cette loi modifie à son tour la Loi Contrôle du 18 juillet 1991. Le Comité permanent R a en effet été désigné comme autorité de contrôle compétente pour les traitements de données à caractère personnel qui relèvent de la 'sécurité nationale'.

Le rôle du Comité en la matière est décrit dans la Loi portant création de l'Autorité de protection des données (Loi APD), dans la Loi relative à la

131 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD), Journal Officiel de l'Union européenne, 2 mai 2016.

132 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes, de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la Décision-cadre 2008/977/JAI du Conseil, Journal Officiel de l'Union européenne, 4 mai 2016, n° 119/89.

133 Loi du 3 décembre 2017 portant création de l'Autorité de protection des données (Loi APD), *M.B.* 10 janvier 2018.

134 Dénomination complète : Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD), *M.B.* 5 septembre 2018.

protection des données (LPD) et dans la Loi organique du contrôle des services de police et de renseignement et de l'Organe de contrôle pour l'analyse de la menace (L.Contrôle).[135]

En 2019, le Comité a développé diverses activités pour pouvoir assumer cette mission et ces obligations supplémentaires. Dès 2018, un Data Protection Officer (DPO) a été désigné pour tous les traitements effectués par le Comité qui ne relèvent pas de la 'sécurité nationale' (par ex., les traitements dans le cadre de la gestion du personnel et de la logistique). En outre, différentes réunions ont été organisées avec les trois autres autorités de contrôle compétentes (*infra* V.2.). Les Comités permanents R et P se sont mis d'accord pour élaborer une proposition de modification de la Loi Contrôle. En effet, diverses dispositions ne sont pas adaptées à la nouvelle compétence des deux Comités. Enfin, le Comité a élaboré plusieurs processus de travail internes pour la fonction d'avis et l'examen des plaintes introduites par des citoyens.

Dans les sections suivantes, il est fait rapport sur ce rôle assumé par le Comité. Sont successivement abordés la collaboration entre les différentes autorités de contrôle compétentes, le contrôle des traitements de données à caractère personnel par BELPIU, les avis juridiques rendus ainsi le traitement de plaintes individuelles, et ce dans le cadre de l'article 35 § 3 L.Contrôle, qui stipule que le Comité permanent R '*fait rapport annuellement à la Chambre des représentants sur les avis rendus en sa qualité d'autorité de protection des données, sur les enquêtes effectuées et mesures prises en cette même qualité ainsi que sur sa collaboration avec les autres autorités de protection des données*'.

V.2. LA COLLABORATION ENTRE LES AUTORITÉS DE CONTRÔLE COMPÉTENTES

La Belgique compte quatre autorités de contrôle compétentes au niveau fédéral. Outre le Comité permanent R, il y a l'Autorité de protection des données (APD) dotée d'une compétence générale et résiduaire, l'Organe de contrôle de l'information policière (C.O.C.), qui contrôle essentiellement les traitements s'inscrivant dans le cadre du Titre 2 de la Loi relative à la protection des données, et le Comité permanent P qui, avec le Comité permanent R, exerce un contrôle sur les traitements effectués par l'OCAM (art. 161 LPD).

À l'exception du dernier cas cité, le Comité permanent R opère en toute autonomie. Est-ce à dire qu'il n'y a pas de concertation ou de coopération entre les quatre instances ? Au contraire, puisque la loi prévoit notamment, dans certains cas, la possibilité ou l'obligation de coopérer ou encore d'échanger des informations (articles 98 et 131 LPD).

135 Pour plus de détails, voir COMITE PERMANENT R, *Rapport d'activités 2018*, 75-86.

Ce qui est encore plus important, c'est l'obligation de coopérer étroitement, entre autres en ce qui concerne le traitement des plaintes, les avis et les recommandations qui touchent aux compétences de deux ACC ou plus, et ce par souci de cohérence dans l'application de la réglementation nationale, européenne et internationale en matière de protection des données (art. 54/1 § 1er Loi APD). Cette disposition prévoit aussi que le traitement conjoint des plaintes, des avis et des recommandations doit se faire sur la base du principe du guichet unique qui sera assumé par l'Autorité de protection des données. Cette fonction est reprise par l'Autorité de protection des données. Par ailleurs, les ACC doivent conclure un protocole afin de réaliser la coopération requise. En 2019, les différents services ont élaboré et négocié un protocole[136], qui a été finalisé à la mi-2020.

V.3. LE CONTRÔLE DES TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL EFFECTUÉS PAR BELPIU[137]

V.3.1. LE CADRE DU CONTRÔLE DE BELPIU

La Loi du 25 décembre 2016 relative au traitement des données à caractère personnel (Loi PNR) met en œuvre les objectifs européens qui sont à la fois de prévenir et de combattre le terrorisme et les infractions graves.[138] Une 'Unité d'Information des Passagers' (UIP) a été créée à cet effet au sein du SFP Intérieur. Cette unité conserve les données des passagers dans une banque de données en vue de prévenir et de combattre les délits ou menaces fixés par la Loi PNR.

Sur la base du sous-titre 5 du Titre 3 de la LPD, le Comité permanent R est l'autorité de contrôle compétente à l'égard de *"tout traitement de données à caractère personnel par l'UIP effectué dans le cadre des finalités visées à l'article 8, § 1er, 4°, de la loi du 25 décembre 2016"* (art. 169 LPD), autrement dit, les traitements visés *"aux articles 7, 1° et 3°/1 et 11, § 1er, 1° à 3° et 5° de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité"* (art. 8, § 1er, 4° Loi PNR). Sont donc visés les traitements effectués par la VSSE et le SGRS dans le cadre de leur mission de renseignement régulière. Le Comité est

136 Le législateur prévoit d'ailleurs une évaluation de la Loi relative à la protection des données trois ans après son entrée en vigueur (art. 283 LPD). Un des aspects qui devra être abordé est la coopération entre les différentes ACC.

137 BELPIU est l'acronyme de *'Belgian Passenger Information Unit'* (Unité belge d'Information des Passagers).

138 La Loi PNR est la transposition de la Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données passagers à des fins de prévention, de détection, d'enquête et de poursuite d'infractions terroristes et de criminalité grave des infractions pénales ainsi que la Directive 2004/82/CE du Conseil du 29 avril 2004 concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (Directive API).

uniquement compétent pour contrôler le fonctionnement de l'IUP dans la mesure où elle prête son concours aux demandes d'informations et de renseignements émanant d'un des deux services de renseignement, et ce indépendamment de la forme de ces demandes (recherches ciblées, *watchlists* ou profils).

V.3.2. UNE VISITE CONCOMITANTE (LIMITÉE)

Compte tenu de leurs compétences respectives en leur qualité d'autorité de contrôle compétente en matière de traitement de données par l'Unité d'Information des Passagers, l'Organe de contrôle de l'Information policière (C.O.C.) et le Comité permanent R ont pris l'initiative d'effectuer une visite concomitante (limitée) à ce service.[139] En effet, si les compétences des deux services ne sont pas tout à fait identiques, au moins elles se recoupent.[140] La visite ne faisait pas suite à une plainte (individuelle) ni à des indications (concrètes) de non-respect de la loi et de la réglementation.

L'approche de la visite mettait l'accent sur le *compliance based* : le traitement de données des passagers est-il conforme à la loi et une norme de sécurité élevée est-elle appliquée ? La visite se concentrait plus sur la sécurité de l'information que sur les aspects juridiques.[141]

L'organisation d'une visite limitée s'expliquait simplement. Tout d'abord, l'UIP n'est opérationnelle que depuis début 2018. Ensuite, tous les transporteurs de passagers et opérateurs de voyage visés n'étaient pas encore techniquement connectés à l'UIP. La visite se limitait à deux domaines, à savoir, d'une part, la sécurité de l'ICT et la sécurité de l'information et, d'autre part, la proportionnalité du traitement des données.

Le rapport d'enquête a été finalisé en juin 2020 et présenté à la Commission parlementaire de suivi.

V.4. LES AVIS

Le Comité peut rendre un avis *'sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant des orientations politiques des ministres compétents'* dans deux cas : lorsque la loi impose son avis ou à la demande de la Chambre des représentants (art. 33, alinéa 6 L. Contrôle). Ce genre d'avis porte spécifiquement sur la problématique des traitements de

139 La visite a eu lieu le 27 novembre 2019.

140 Cette visite portait sur la manière dont les deux services de renseignement belges font usage de leurs compétences dans ce cadre. Cet aspect a été traité par le Comité dans une enquête de contrôle initiée en 2018 (cf. I.7.2).

141 Cette orientation n'a pas empêché le C.O.C. ou le Comité permanent R de prendre les mesures appropriées en cas d'identification de lacunes juridiques évidentes.

données et doit donc être distingué de la compétence d'avis générale qui porte, par exemple, sur l'efficacité et la coordination. Cette compétence d'avis générale est, en ce sens, plus large, tout en étant plus restreinte puisque limitée au fonctionnement des services de renseignement et de l'OCAM.

C'est en cette qualité qu'en 2019, le Comité a rendu, seul ou avec le Comité permanent P, neuf avis relatifs à des projets de loi ou projets d'arrêté. La préparation de ces avis représente une charge de travail supplémentaire non négligeable pour le Comité. Ces avis peuvent être consultés en intégralité sur le site internet du Comité (www.comiteri.be/avis). On se limitera ici à une énumération des avis rendus :

- Avis 001/CPR-ACC/2019 du 5 février 2019 concernant '*un avant-projet de loi visant à modifier la Loi du 25 décembre 2016 relative au traitement des données des passagers*' ;
- Avis 002/CPR-ACC/2019 du 9 avril 2019 concernant le '*un projet d'arrêté royal modifiant l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et de l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité* ' ;
- Avis 003/CPR-ACC/2019 du 27 juin 2019 concernant 'l'*avant-projet de loi modifiant la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité*' ;
- Avis 004/CPR-CPP-ACC/2019 du 27 juin 2019 concernant une demande d'avis du ministre de l'Intérieur sur '*l'avant-projet de loi relatif à l'approche administrative communale et portant création d'une Direction Évaluation de l'Intégrité pour les Pouvoirs publics (OCAM)*' ;
- Avis 005/CPR-ACC/ 2019 du 3 juillet 2019 concernant une demande d'avis du ministre de l'Intérieur sur '*l'avant-projet de loi relatif à l'approche administrative communale et portant création d'une Direction Évaluation de l'Intégrité pour les Pouvoirs publics (VSSE – SGRS)*' ;
- Avis 006/CPR-ACC/2019 du 23 août 2019 concernant une demande d'avis du ministre des Affaires étrangères sur '*le projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la République de Chypre sur la protection mutuelle des informations classifiées, fait à Bruxelles le 20 juillet 2015*' ;
- Avis 007/CPR-ACC/2019 du 23 août 2019 concernant une demande d'avis du ministre des Affaires étrangères sur '*le projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la Hongrie sur la protection mutuelle des informations classifiées, fait à Budapest le 21 septembre 2015*' ;
- Avis 008/CPR-ACC/2019 du 23 août 2019 concernant une demande d'avis du ministre des Affaires étrangères sur '*le projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la République de Finlande sur la protection mutuelle des informations classifiées, fait à Helsinki le 20 juillet 2016*' ;

– Avis 009/CPR-ACC/2019 du 23 août 2019 concernant une demande d'avis du ministre des Affaires étrangères sur *'le projet de loi portant assentiment à l'accord entre le Royaume de Belgique et le Royaume d'Espagne sur la protection mutuelle des informations classifiées, fait à Bruxelles le 15 octobre 2015'*.

V.5. LES INFORMATIONS DES SERVICES CONTRÔLÉS

Les services contrôlés par le Comité permanent R doivent tenir ou mettre à sa disposition toute une série de données[142], c'est-à-dire :
– En cas de brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement concerné la notifie au Comité permanent R dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance (articles 89, 122, 155 et 180 LPD) ;
– Un registre reprenant les informations sur les banques de données utilisées ou les activités de traitement menées (articles 90, 123, 156 et 181 LPD) ;
– La désignation d'un délégué à la protection des données (ou Data Protection Officer (DPO)) par le responsable du traitement ou le sous-traitant (articles 91, 124 et 127 LPD).

En 2019, aucun *data breach*[143] n'a été signalé au Comité. Il n'a pas non plus reçu de registres contenant des informations sur les activités de traitement. Le Comité a écrit aux autorités pour lesquelles il est compétent afin d'avoir un aperçu des délégués à la protection des données.

Compte tenu de la connaissance encore limitée des services contrôlés sur cette législation complexe, le Comité continuera de veiller à son application correcte.

V.6. LE TRAITEMENT DES PLAINTES APD INDIVIDUELLES

Le Comité permanent R traite également les demandes individuelles relatives aux traitements de données à caractère personnel par les personnes et les services susmentionnés ainsi que leurs sous-traitants (art. 34 L.Contrôle et articles 79,

142 Chaque service ne doit pas conserver ou tenir à disposition toutes les données mentionnées ici. Ceci s'applique certainement à la Commission BIM, qui ne doit pas communiquer d'informations au Comité permanent R.

143 Un *personal data breach* ou 'violation de données à caractère personnel' est défini comme *une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* (art. 4 RGPD).

113, 145 et 173 LPD). Le requérant est en droit de demander la rectification ou la suppression de données à caractère personnel inexactes le concernant. Et il peut demander à ce que le respect des règles qui sont d'application en matière de protection des données soit vérifié. Pour être recevable, la requête doit être écrite, datée, signée et motivée (art. 51/2 L.Contrôle).[144] Si la requête est manifestement non fondée, le Comité peut décider de ne pas y donner suite. Cette décision doit être motivée et communiquée par écrit au requérant.[145]

En 2018, le Comité avait reçu cinq plaintes APD de citoyens concernant d'éventuels traitements de données à caractère personnel par la VSSE et le SGRS, dont quatre ont été traitées en 2019.

En 2019, le Comité a reçu quatorze plaintes, dont trois ne relevaient pas de la compétence du Comité (mais bien de celle du C.O.C.) et une plainte jugée recevable mais manifestement infondée. Huit de ces nouvelles plaintes ont encore pu être traitées en 2019.[146] Dans ces dossiers, les plaignants ont été informés que les vérifications requises avaient été effectuées.[147] Le fonctionnaire dirigeant du service de renseignement ou le directeur de l'OCAM – et, sous réserve de l'approbation du Comité, une autre instance ou personne – reçoit '*les conclusions de l'enquête*' (art. 34, dernier alinéa L.Contrôle). Les trois enquêtes APD toujours ouvertes (dont une de 2018 et deux de 2019), ont pu être traitées en 2020.

144 Cette disposition stipule également que la requête doit '*justifier de l'identité de la personne concernée*'. Il est difficile de saisir d'emblée la signification de cette disposition. Il s'agit vraisemblablement de l'obligation de prouver son identité. Cette obligation est en fait reprise dans les dispositions concernées de la Loi relative à la protection des données (voir articles 80, 114, 146 et 174 LPD).

145 Ces vérifications sont effectuées sans frais (articles 80, 114, 146 et 174 LPD).

146 Une plainte a été traitée conjointement au Comité permanent P.

147 *'La personne concernée a le droit de demander la rectification ou la suppression de ses données à caractère personnel inexactes'* (art. 79 LDP). *'Le Comité permanent R effectue les vérifications et communique uniquement à l'intéressé qu'il a été procédé aux vérifications nécessaires'* (art. 80 LPD), donc sans plus d'explications.

CHAPITRE VI
LE CONTRÔLE DE BANQUES DE DONNÉES COMMUNES

Les ministres de l'Intérieur et de la Justice ont créé, en 2016, la banque de données commune '*foreign terrorist fighters*' (BDC FTF). Ils lui ont assigné la finalité de contribuer à l'analyse, à l'évaluation et au suivi de personnes en lien avec cette problématique. Cette banque de données commune (BDC) a été modifiée en 2018 : on parle désormais de la banque de données commune '*terrorist fighters*' (BDC TF). Celle-ci comprend, outre la catégorie générale existante des '*foreign terrorist fighters*', une catégorie visant les '*homegrown terrorist fighters*'. Toujours en 2018, une (nouvelle) banque de données commune distincte a été créée pour 'les propagandistes de haine' (BDC PH).[148]

Par un Arrêté royal paru fin 2019[149], deux nouvelles catégories ont été ajoutées à la BDC TF, à savoir les 'extrémistes potentiellement violents' (EPV) ainsi que les 'personnes condamnées pour terrorisme' (PCT).

VI.1. LES PRINCIPALES MODIFICATIONS DE LA RÉGLEMENTATION

VI.1.1. LE DÉLÉGUÉ À LA PROTECTION DES DONNÉES

La Loi du 22 mai 2019[150] a modifié la LFP afin de l'aligner sur la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. La fonction de 'conseiller en sécurité et en

148 L'article 44/11/3 *quinquies*/2 LFP assigne le contrôle du traitement des informations et des données à caractère personnel contenues dans les BDC à l'Organe de contrôle de l'information policière (C.O.C.) et au Comité permanent R (par la suite, 'les autorités de contrôle').

149 A.R. du 20 décembre 2019 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters et l'Arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er*bis* "de la gestion des informations" du chapitre IV de la loi sur la fonction de police, *M.B.*, 27 janvier 2020.

150 Loi du 22 mai 2019 modifiant diverses dispositions en ce qui concerne la gestion de l'information policière (*M.B.*, 19 juin 2019).

protection de la vie privée' a été remplacée par la 'fonction de délégué à la protection des données' (art. 44/11/3*quinquies*/1 LFP). Ce délégué est chargé :
- de la fourniture d'avis qualifié en matière de protection de données et de sécurisation des données à caractère personnel. Il veille plus particulièrement au respect des conditions générales de licéité du traitement ;
- de la mise en œuvre, de la mise à jour et du contrôle d'une politique de sécurisation et de protection des données ;
- de l'exécution des autres missions relatives à la protection des données et de sécurisation qui sont déterminées par le Roi ou qui lui sont confiées par les ministres de l'Intérieur et de la Justice.

Cette mission s'exécute en complément des missions du délégué à la protection des données prévues dans la Loi relative à la protection des données.

VI.1.2. L'ARRÊTÉ ROYAL DU 20 DÉCEMBRE 2019

L'Arrêté royal du 20 décembre 2019 (*supra*) poursuit un triple objectif. Le premier est d'ajouter de nouvelles catégories à la banque de données commune TF à savoir les "extrémistes potentiellement violents" ainsi que les "personnes condamnées pour terrorisme". Le second objectif est d'apporter des "modifications techniques" aux AR TF et PH suite à la modification de la Loi du 5 août 1992 par la Loi du 22 mai 2019. Enfin, le troisième objectif est de prévoir un accès direct pour l'Administration générale de la Trésorerie du SPF Finances aux banques de données TF et PH.

VI.1.2.1. L'ajout de l'extrémiste potentiellement violent (EPV) dans la BDC TF

L'extrémiste potentiellement violent est défini comme toute personne physique ayant un lien avec la Belgique qui répond aux critères cumulatifs suivants :
a) elle a des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme méthode d'action en Belgique ;
b) il existe des indications fiables qu'elle a l'intention de recourir à la violence, et ce en relation avec des conceptions extrémistes mentionnées en a) ;
c) en outre, l'EPV doit répondre au minimum à l'une des trois conditions suivantes qui sont considérées comme étant des facteurs de risque quant à l'utilisation de la violence :
   - il entretient systématiquement des contacts sociaux au sein des milieux extrémistes ;
   - il a des problèmes psychiques constatés par un professionnel compétent en la matière ;
   - il a commis des actes ou il présente des antécédents qui peuvent être considérés comme soit a) un crime ou un délit portant atteinte à ou

menaçant l'intégrité physique ou psychique de tiers ; soit b) des instructions ou des formations relatives à la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes vous ou substances nocives ou dangereuses, ou pour d'autres méthodes et techniques spécifiques en vue de commettre des infractions terroristes ; soit c) des agissements en connaissance de cause constituant un soutien matériel en faveur d'une organisation d'un réseau terroriste/extrémistes ; soit d) des agissements dont la nature indique un niveau de vigilance préoccupant de l'individu à l'égard de la sécurité.

VI.1.2.2. L'ajout des personnes condamnées pour terrorisme (PCT) dans la BDC TF

Il s'agit des personnes qui, cumulativement :
- ont un lien avec la Belgique ;
- qui ont été condamnées ou qui ont reçu une décision judiciaire d'internement ou, dans le cas de mineurs, fait l'objet d'une mesure de protection pour des infractions terroristes, telles que décrites au Livre II Titre I Ter du Code pénal (en Belgique) ou des faits qualifiés comme tels ou par une infraction équivalente à l'étranger ;
- et à l'égard de qui l'OCAM a estimé que le niveau de menace qu'elles représentent se définit comme moyen (niveau 2), grave (niveau 3) ou très grave (niveau 4).

De par l'insertion de cette nouvelle catégorie dans la banque de données TF, tous les acteurs qui doivent assurer un suivi des PCT (tels que la DG EPI, les Maisons de Justice, la police, les centres fermés, la VSSE, les TFL, etc.) peuvent être informés à propos des personnes concernées, de manière proactive et en temps utile.

VI.1.2.3. L'accès direct en faveur d'un nouveau service dans les BDC TF et PH

Dans l'A.R. du 20 décembre 2019, l'Administration générale de la Trésorerie se voit accorder un accès direct à la BDC TF et PH.[151] Il s'agit de l'autorité compétente en matière de sanctions financières pour le gel des fonds et des ressources économiques des personnes ou entités qui commettent, ou tentent de commettre, des infractions terroristes, les facilitent ou y participent.

[151] À noter que l'accès pour l'Administration générale de la Trésorerie ne figurait pas dans le projet d'A.R. ni dans la déclaration préalable complémentaire qui avaient été soumis au C.O.C. et au Comité permanent R.

VI.2. LA MISSION DE CONTRÔLE

VI.2.1. L'OBJET DU CONTRÔLE

Pour l'année 2019, le C.O.C. et le Comité permanent R ont décidé d'axer leur contrôle conjoint, d'une part, sur le suivi réservé à certaines recommandations formulées dans les rapports des années précédentes et, d'autre part, sur la consultation d'une série de services de base et de services partenaires en matière de contrôles de licéité et des procédures internes permettant d'assurer un traitement optimal des informations dans la BDC TF et PH.[152]

Par ailleurs, les organes de contrôle ont procédé à un examen approfondi de la coordination du traitement des informations dans la BDC TF et PH, avec notamment une attention particulière pour le rôle du *data protection officer* (DPO). À cet égard, il également a été tenu compte du nombre croissant de services disposant d'un accès à la BDC TF et PH.

VI.2.2. LE SUIVI DES RECOMMANDATIONS

VI.2.2.1. La désignation du délégué à la protection des données

Début septembre 2019 les ministres de la Justice et de l'Intérieur ont conjointement désigné un DPO pour la BDC TF et PH.[153] Ce délégué est l'interlocuteur privilégié du C.O.C. et du Comité permanent R.

VI.2.2.2. La mise en place d'un mécanisme de signalement des incidents de sécurité

Pour signaler un incident de sécurité, un onglet est disponible sur l'écran de l'application.[154] L'utilisateur de l'application peut donc établir un rapport sur le problème constaté, et le DPO du ou des service(s) concerné(s) a accès à un aperçu de tous les incidents liés à la BDC TF et PH qui sont enregistrés. Pour la bonne compréhension de l'utilisateur, les règles de gestion des incidents de sécurité sont décrites à l'écran.

La procédure à suivre est définie dans un manuel d'utilisation. Bien que cela ait été soulevé, ce manuel ne mentionne pas qu'une fuite externe de données doit

---

152 Les nouvelles catégories EPV et PCT ont été introduites par l'A.R. du 20 décembre 2019, paru au Moniteur belge le 27 janvier 2020. Elles n'ont dès lors pas été contrôlées en 2019.

153 Le C.O.C. et le Comité permanent R ont pris note du fait que cette fonction est cumulée avec, d'une part, la fonction de DPO auprès de l'OCAM et, d'autre part, le travail effectif à OCAM. Il n'était pas encore possible d'évaluer si l'emploi du temps prévu suffit pour cette fonction, ni les contours du risque de conflit d'intérêts.

154 Donnant accès à la banque de données commune TF et PH.

être systématiquement signalée au C.O.C. et au Comité permanent R, alors que cette procédure était une recommandation émise à l'égard de la Police fédérale au sens de l'article 44/11/3*quinquies*/2 dernier alinéa LFP.

VI.2.2.3. Le développement d'un outil informatique complémentaire

Il avait été constaté que l'OCAM ne disposait pas d'un outil informatique permettant de suivre les délais de conservation et la suppression des données relatives à des personnes appartenant (ou ayant appartenu) à l'une des cinq catégories FTF. Cette constatation avait conduit les autorités de contrôle à maintenir leur recommandation de développer un outil informatique.

En 2019, un contrôle a été effectué sur 487 entités figurant depuis au moins trois ans dans la BDC FTF. Pour 485 entités, l'OCAM a fait référence à un "*processus logique dans le cadre duquel aucune anomalie n'a été identifiée*". L'OCAM a fourni des explications utiles à ce propos. Néanmoins, la recommandation de développer un outil informatique permettant le suivi des délais de conservation des données visées à l'article 44/11/3*bis* § 5 LFP a été réitérée.

VI.2.2.4. L'exécution d'un contrôle spontané des loggings

Sur la base des explications fournies (principalement par la Police fédérale), une distinction doit être établie entre différentes possibilités en matière de contrôle de loggings, à savoir un 'petit logging'[155], un 'grand logging'[156] et un 'contrôle de licéité'. La demande de logging peut être introduite via l'ID des utilisateurs.

La Police fédérale a signalé avoir reçu en 2019 73 demandes de loggings au sein de ses propres services, dont 71 'petits loggings' et deux via l'onglet 'contrôle de licéité'. Aucun 'grand logging' n'a été demandé.

Le C.O.C. et le Comité permanent R ont insisté sur l'importance d'effectuer également un contrôle élargi des loggings. Au sein des services partenaires, il est nécessaire de sensibiliser davantage à propos des contrôles de licéité qui doivent être systématiquement réalisés.

VI.2.2.5. L'exception à l'obligation d'alimenter les BDC et les informations policières

Il existe deux dérogations à l'obligation d'introduire des informations dans la banque de données commune (art. 44/11/3*ter* § 5 LFP). Tout d'abord,

155 Le 'petit logging' est un logging relatif aux traitements effectués sur une entité de la banque de données commune et est accessible à tous les utilisateurs ayant un droit de lecture et/ou d'écriture.

156 Le 'grand logging' est un logging relatif aux traitements effectués par les utilisateurs de la banque de données commune et ne peut être exécuté que par la Police fédérale, en tant que gestionnaire (service DRI).

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. Par ailleurs, lorsque (et aussi longtemps que) le dirigeant d'un service de renseignement juge que l'alimentation d'une information peut compromettre la sécurité d'une personne ou la règle du tiers service, il peut en différer la transmission.

Le rapport de contrôle précédent avait révélé que les informations policières issues de rapports d'information policiers ("RIR"), code 00 ou 01[157] n'étaient pas reprises dans la BDC TF et PH. Ces codes résultent de la Circulaire MFO3 et concernent l'alimentation de la Banque de données nationale générale (BNG), mais l'exception n'est pas reprise dans la réglementation de la BDC TF et PH. *De lege lata*, la loi et l'arrêté d'exécution ne permettent pas l'exclusion de ces données des banques de données communes.

La Police fédérale a informé les autorités de contrôle qu'un groupe de travail LTF a décidé de ne reprendre que les RIR 01 dans la banque de données commune. L'utilisateur concerné peut demander qu'un RIR 01 mentionné dans la BDC TF et PH lui soit communiqué. Cette demande sera ensuite évaluée au cas par cas.

Le C.O.C. et le Comité permanent R ont observé que cette pratique s'appuie uniquement sur la Circulaire MFO3 du 14 juin 2002 (non publiée), qui ne peut cependant pas aller à l'encontre des règles régissant l'alimentation de la BDC TF et PH.

VI.2.2.6. La transmission des listes

Dans leur rapport de contrôle précédent, le C.O.C. et le Comité permanent R présentaient la réglementation et les conditions de transmission des listes. Ils rappelaient leur observation antérieurement formulée quant à la nécessaire sécurisation technique de la transmission si elle est effectuée par courriel, et ils attiraient l'attention sur l'importance que le service de base assurant la communication d'une liste informe adéquatement le destinataire.[158] Enfin, les autorités de contrôle s'interrogeaient sur la ou les autorité(s) chargée(s) de contrôler les destinataires à propos de l'utilisation des listes ainsi que sur la manière dont un contrôle pourrait s'exercer.

À la suite à l'enquête menée en 2019, la pratique consiste à envoyer chaque mois par courriel une liste des données et informations à caractère personnel figurant dans la BDC TF et PH, notamment au SPF Emploi, à l'AFCN et à Bruxelles Prévention & Sécurité. Le C.O.C. et le Comité permanent R n'ont pas

157 Ces codes sont attribués par le policier rédacteur. Un 'RIR 01' concerne des informations policières qui ne peuvent être utilisées qu'avec l'accord du rédacteur ; un 'RIR 00' concerne des informations policières qui ne peuvent en aucun cas être utilisées. Il s'agit d'informations extrêmement sensibles qui, par exemple, peuvent conduire à l'identification d'une source.

158 Par exemple, par la conclusion d'un protocole préalable entre services.

pu retrouver d'évaluation conjointe[159] de la Police fédérale, de l'OCAM et des services de renseignement et de sécurité. La recommandation antérieure d'informer les services destinataires des conditions dans lesquelles la liste peut être communiquée semble également n'avoir eu aucun effet. Dans ce contexte, le C.O.C. et le Comité permanent R se sont interrogés notamment sur le fait que l'institution Bruxelles – Prévention & Sécurité soit destinataire des listes, ceci d'autant plus qu'elle n'a pas été incluse en tant que nouveau service partenaire lors de la modification de la réglementation.[160]

Le C.O.C. et le Comité permanent R ont souligné que la communication à des instances tierces de données et informations à caractère personnel extraites de la banque de données commune est soumise à des dispositions légales strictes et cumulatives. D'autre part, au niveau de la nécessaire sécurisation technique de la transmission des listes, le contrôle effectué en 2019 a conduit à réitérer la recommandation de conclure des protocoles d'accord avec les services destinataires des listes.

VI.2.3. L'UTILISATION DE LA BANQUE DE DONNÉES TF ET PH PAR LES 'SERVICES PARTENAIRES'

VI.2.3.1. La vérification de l'accès aux banques de données TF et PH par les services partenaires et de leur alimentation

Le nombre d'utilisateurs actifs par service partenaire a été vérifié, de même que la fréquence d'accès des services partenaires à la banque de données commune. Il résulte de cette vérification qu'en décembre 2019, 17 des 47 services partenaires n'avaient prévu aucun utilisateur pour la BDC TF et PH.

En ce qui concerne les services partenaires qui, depuis plusieurs années, n'ont pas désigné d'utilisateurs ni prévu de loggings pour la BDC TF et PH, le C.O.C. et le Comité permanent R relèvent une éventuelle absence de 'besoin d'en connaître'. Il conviendrait de suivre dans quelle mesure les conditions énoncées à l'article 44/11/3*ter* § 2 LFP sont (encore) remplies. Logiquement, l'accès direct ou indirect de certains services partenaires doit être revu au regard de cette absence de nécessité.

VI.2.3.2. Politique en matière de sécurité et de protection des données

Le C.O.C. et le Comité permanent R ont constaté que le rôle du délégué à la protection des données de la BDC TF et PH est considéré comme une fonction

159 Imposée par l'art.44/11/3 *quater* LFP et mentionnée dans l'AR 11 § 2 AR TF et PH).

160 Une analyse juridique relative à Bruxelles Prevention & Sécurité et l'accès à la banque de données communes Terrorist Fighters a été soumise à la Commission de suivi en septembre 2020.

de conseil et de coordination, centrée sur la recherche d'une vision commune, appuyée par l'ensemble des services partenaires impliqués. Bien que l'intention ne soit en effet pas de prendre des décisions à la place des responsables de traitements, les autorités de contrôle ont souligné que l'initiative de la présentation d'une première proposition peut revenir au délégué à la protection des données de la BDC TF et PH. En effet, l'élaboration d'une approche commune pourrait être inutilement retardée dans l'attente d'une initiative des services partenaires pour présenter des propositions (divergentes).

Le C.O.C. et le Comité permanent R ont émis la recommandation de recevoir une copie des notes de politique que le délégué établira à la lumière des choix de sécurité et de politique posés en matière de protection des données, plus particulièrement dans le cadre de l'accès et de l'alimentation de la BDC TF et PH. Par ailleurs, le DPO de la banque de données commune a pour objectif d'établir un registre 'dynamique' des activités de traitement au cours du premier trimestre 2020. Il a été expliqué, en termes généraux, que la nature dynamique fait référence à une solution intégrée dans chacune des banques de données communes et qui peut à la fois répondre aux exigences légales et être aisément actualisée. En attendant, un registre 'classique' des activités de traitement, qui reste général, sera fourni. Par ailleurs, dans une première phase de sensibilisation, le DPO proposera un module[161] de présentation comprenant les principes du traitement, les obligations des différents acteurs impliqués dans le traitement des données à caractère personnel et le rôle du DPO.

VI.2.3.3. Deux constatations

Tout d'abord, s'agissant de l'Administration générale de la Trésorerie, la Cellule des sanctions financières est composée de quatre personnes qui disposeront d'un accès personnel. Le rapport au Roi permet d'établir que l'Administration générale de la Trésorerie est en mesure d'alimenter la BDC TF et PH avec des informations pertinentes. Cet accès et les mesures de sécurité appliquées doivent toutefois faire l'objet d'une évaluation plus approfondie.

D'autre part, la réglementation tient compte du statut indépendant du Ministère public puisqu'il n'y a aucune obligation (mais une possibilité) pour ce service partenaire d'alimenter la BDC TF et PH, même s'il a un accès direct. Le législateur a jugé que les données judiciaires proviennent principalement de la police. En ce sens, l'obligation pour les services de police d'alimenter la banque de données commune suffit, de sorte que les données pertinentes de la Police judiciaire sont enregistrées.[162]

---

161 Ce module devait être opérationnel au premier semestre 2020.

162 Le C.O.C. et le Comité permanent R ont cependant noté que ce raisonnement ne s'applique pas aux jugements et aux arrêts dont les services de police n'ont pas connaissance.

Afin de s'assurer que la banque de données TF et PH sont correctement alimentées, les autorités judiciaires ont envoyé des instructions. Il y est inscrit que les parquets n'alimenteront pas la BDC TF et PH. Toutefois, la circulaire COL10/2015 prévoit que les magistrats de référence en matière de terrorisme, énumérés limitativement, communiquent, à leur demande, les informations concernant le dossier pour lequel ils sont compétents lorsque l'intéressé fait l'objet d'une enquête fédérale par le Parquet fédéral. Les modifications de ces mesures judiciaires seront également notifiées à l'OCAM.

Ces circulaires sont en cours de révision et d'actualisation à la lumière du réseau d'expertise Terrorisme afin de fournir une circulaire intégrée et actualisée sur l'approche judiciaire des *terrorist fighters* et des propagandistes de haine. La fonction de magistrat de sécurité sera supprimée et remplacée par la fonction de magistrat-officier de sécurité. Par conséquent, le Ministère public ne dépendra plus de l'officier de sécurité du SPF Justice, mais disposera de son propre officier de sécurité.

L'objectif est d'inclure le contrôle des loggings de la BDC TF et PH dans la liste des missions du magistrat-officier de sécurité. Actuellement, les listes nominatives de tous les magistrats et collaborateurs du Ministère public ayant accès à la banque de données commune TF ont été établies par le magistrat de sécurité, mais après la fusion dans une nouvelle circulaire des différentes circulaires existantes, ces listes seront disponibles auprès d'un des cinq magistrats-officiers de sécurité (un par Cour d'appel). Dans la pratique, les mesures judiciaires sont reprises dans la BDC TF et PH via une liste que les procureurs fournissent à l'OCAM après une consultation.

Dans leur rapport, le C.O.C. et le Comité permanent R ont noté que la consultation du parquet par l'OCAM concernant les mesures judiciaires n'a, jusqu'à présent, pas eu lieu de manière systématique, ce qui signifie que certaines informations de la BDC TH et PH peuvent être datées ou incomplètes.

VI.2.3.4. La situation au niveau des habilitations de sécurité

À ce jour, il n'existe aucun mécanisme permettant de refuser l'accès à BDC TF et PH aux services partenaires au motif que l'utilisateur ne dispose pas d'une habilitation de sécurité.[163] Il existe une réglementation distincte pour le Ministère public. Ses magistrats n'ont pas besoin d'une habilitation de sécurité ; seuls les collaborateurs doivent en être titulaires. La COL 22/2016 précise que dès l'envoi de la demande d'habilitation, les collaborateurs auront accès à la banque de données commune TF. Le C.O.C. et le Comité permanent R ont estimé souhaitable de ne donner accès à la banque de données commune TF qu'après l'octroi de l'habilitation ; dans l'intervalle, la consultation de la banque de

[163] L'obligation de détenir une habilitation de sécurité résulte de l'art. 7 § 2 AR TF et PH.

données peut être laissée aux collaborateurs qui disposent déjà d'une telle habilitation.

En outre, la question se pose de la nécessité de continuer à donner accès à la BDC TF et PH aux services qui n'ont pas demandé les habilitations de sécurité requises ou qui n'ont pas soumis de liste d'utilisateurs à la Police fédérale. D'après les informations reçues de la part du DPO de la BDC TF et PH, il apparaît que, dans la pratique, plusieurs services partenaires ne prévoient pas d'utilisateurs et qu'aucun login n'est associé à ces services.

D'autre part, en ce qui concerne les listes de diffusion, le C.O.C. et le Comité permanent R ont constaté une vigilance très limitée concernant l'application correcte de l'article 44/11/3*quater* LFP. La question se pose de savoir si l'accès aux boîtes aux lettres non personnalisées est effectivement limité aux personnes disposant de l'habilitation de sécurité requise.

VI.3. LA MISSION D'AVIS

VI.3.1. LA DEMANDE DE NE PAS EFFECTUER DE TRAITEMENTS SANS BASE RÉGLEMENTAIRE ADÉQUATE

Fin mars 2019, le directeur de l'OCAM informait le président du Comité permanent R d'une lettre adressée par l'OCAM au président de l'Autorité de protection des données (APD). Ce dernier courrier portait à la connaissance de l'APD qu'une période de test pour le traitement de deux nouvelles catégories – les extrémistes potentiellement violents (EPV) et les personnes condamnées pour terrorisme (PCT)– allait être initiée début avril 2019 dans la banque de données TF. Selon le directeur de l'OCAM, l'insertion de ces deux nouvelles catégories répondait à d'importants besoins sur le terrain, notamment dans les centres de détention, et rencontrait les recommandations de la Commission d'enquête parlementaire sur les attentats terroristes. Le directeur de l'OCAM exposait que, grâce à la détermination de critères clairs, le suivi des entités par les Task force locales allait être uniformisé. Différents textes, dont le projet d'arrêté royal élaboré au niveau technique mais non validé au niveau politique, étaient annexés au courrier. Le directeur de l'OCAM entendait informer le président de l'APD "*en toute transparence démocratique*" et lui demandait de rendre un avis préliminaire sur les textes en projet.

Par un courrier adressé mi-juin 2019 aux ministres de la Justice et de la Sécurité et de l'Intérieur, les Comités permanents R et P ainsi que le C.O.C. ont rappelé que la procédure légalement exigée devait être suivie, indépendamment de la question de savoir si le traitement était envisagé pour une "période test" ou à titre définitif. Ce courrier insistait sur le fait que des données à caractère

personnel ne pouvaient être traitées dans une banque de données commune qu'après l'adoption d'un arrêté royal délibéré en Conseil des ministres (pris après avis des autorités de contrôle et du Conseil d'État) et après une déclaration préalable auprès du C.O.C. et du Comité permanent R. Ce faisant, les Comités permanents R et P ainsi que le C.O.C. rejoignaient la position adoptée par le Collège des procureurs généraux. En conséquence, il était demandé aux ministres, en leur qualité de responsables de traitement, de cesser le traitement des données relatives aux deux catégories concernées. Par un courrier envoyé mi-juillet 2019, les ministres ont confirmé avoir donné instruction à la Police fédérale de rendre techniquement impossible l'utilisation des deux nouvelles catégories.

VI.3.2. AVIS SUR LE PROJET D'ARRETÉ ROYAL INSÉRANT LES EPV ET LES PCT

Le C.O.C. et le Comité permanent R ont rendu leur avis conjoint début 2019[164] sur le projet d'arrêté royal modifiant l'AR TF. Ils relevaient tout d'abord l'élargissement important de la banque de données TF existante avec l'enregistrement des extrémistes potentiellement violents. Pointant les risques, notamment dans le cadre de transmission à des organismes (étrangers), les autorités de contrôle estimaient que le projet devait être adapté en ce sens que les personnes qui sont soumises à une 'pré-enquête' (enregistrement sur la base d'indices pendant six mois) ne devraient être connues que des services de base qui doivent utiliser leurs possibilités légales existantes pour obtenir des informations et des renseignements devant leur permettre de confirmer ou d'annuler l'enregistrement dans la banque de données.

Le C.O.C. et le Comité permanent R ont procédé à un examen approfondi des différents (sous-)critères décrivant les EPV dans le projet d'arrêté royal.

En conclusion, les autorités de contrôle disaient comprendre parfaitement la difficulté de la mission des services de police, de renseignement et de sécurité en matière de lutte (proactive) contre le terrorisme et l'extrémisme pouvant mener au terrorisme. La création de banques de données communes rencontre en ce sens les recommandations de la Commission d'enquête parlementaire sur les attentats terroristes en vue d'une circulation plus efficace des informations entre les acteurs de la chaîne de sécurité et de la chaîne pénale. Les instances de contrôle relevaient toutefois que la Commission d'enquête n'a en aucun cas recommandé d'élargir le groupe cible au point de faire disparaître le lien avec la violence terroriste, raison pour laquelle ils demandaient, d'une part, que leurs recommandations soient prises en considération et, d'autre part, que les critères

164 Avis 001/CPR-C.O.C./2019 du 1er août 2019 concernant un projet d'arrêté royal modifiant l'A.R. du 21 juillet 2016 relatif à la banque de données communes Terrorist Fighters (www.comiteri.be).

préalablement définis fassent l'objet d'une utilisation rigoureuse. Le C.O.C. et le Comité permanent R pointaient le risque qu'à défaut de suivre leurs recommandations, la base d'enregistrement dans les BDC serait ramenée, d'un part, au niveau associé aux conditions de traitement pour la police administrative et, d'autre part, à celles d'application pour les services de renseignement. De ce fait, des données très sensibles sur le plan de la vie privée sont de plus en plus souvent transmises à des services et organismes (en constante augmentation) qui ne font pas partie de la chaîne pénale ni de la chaîne de sécurité. Or, ces services (administratifs) n'ont souvent aucune expérience ou ne disposent que d'une expérience limitée en matière de gestion de telles données sensibles et parfois incertaines, avec des répercussions possibles sur la vie des intéressés.

En ce qui concerne l'élargissement de la BDC TF avec l'enregistrement des personnes condamnées pour terrorisme (PCT), le C.O.C. et le Comité permanent R ont invité les auteurs du projet à aborder la question des personnes condamnées à l'étranger, celle des mineurs s'étant vu imposer une mesure pour infractions terroristes et la question des personnes qui n'ont pas encore été définitivement condamnées.

Enfin, les autorités de contrôle s'interrogeaient quant au nouvel accès indirect prévu dans le projet d'arrêté royal en faveur de Bruxelles-Prévention & Sécurité. Ils pointaient en particulier l'absence de clarté du contexte dans lequel cet organisme se voyait désigné comme service partenaire et rappelaient l'article 44/11/3*ter*, § 3 LFP. Le projet laissant des questions ouvertes (concernant l'utilisation et le partage des données par Bruxelles-Prévention & Sécurité, les délais de conservation, les règles de sécurité d'application), le C.O.C. et le Comité permanent R ont estimé qu'il n'était pas acceptable qu'un nouvel organisme soit ajouté à la liste existante, déjà large, des destinataires de données très sensibles sur le plan de la vie privée, sans qu'en soit démontrées la pertinence et la plus-value pour la société.

VI.3.3. AVIS SUR 'LES DÉCLARATIONS PRÉALABLES COMPLÉMENTAIRES'

Par un courrier envoyé mi-juillet 2019, les ministres de la Justice et de la Sécurité et de l'Intérieur ont transmis une demande d'avis au C.O.C. et au Comité permanent R au sujet de la déclaration préalable complémentaire concernant les banques de données communes PH et TF. Cette (troisième) déclaration préalable complémentaire comprenait les modalités pratiques du traitement de données par les Maisons de Justice des Communautés, ainsi que par la *Vlaams Agentschap Jongerenwelzijn* ('VAJ', Agence flamande de l'aide sociale aux jeunes).[165]

[165] Le C.O.C. et le Comité permanent R ont déduit du contenu du courrier du 24 juillet 2019 des ministres responsables du traitement que l'Autorité nationale de sécurité ne disposait pas encore de l'accès aux BDC.

Dans leur avis conjoint de fin novembre 2019[166], le C.O.C. et le Comité permanent R pointaient que l'absence de désignation d'un DPO avait entretemps été résolue et que les (modifications des) coordonnées des DPO des (nouveaux) services disposant d'un (nouvel) accès devaient être renseignées. Pour le surplus, ils émettaient un avis favorable quant à cette déclaration complémentaire, sous réserve d'observations formulées.

166 www.comiteri.be.

CHAPITRE VII
LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Parallèlement à sa collaboration aux enquêtes de contrôle, le Service d'Enquêtes R du Comité effectue également des enquêtes sur les membres des services de renseignement suspectés d'avoir commis un crime ou un délit. Il s'agit de missions confiées au Service d'Enquêtes 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).[167]

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le directeur du Service d'Enquêtes R sont soumis à l'autorité du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a aucune autorité sur eux. Le président du Comité doit cependant veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle. La raison en est évidente : le Comité a beaucoup d'autres missions légales. Celles-ci pourraient être mises en péril si les dossiers judiciaires nécessitaient un investissement trop conséquent. 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).

Lorsque le Service d'Enquêtes R effectue des enquêtes pénales, le directeur doit remettre un rapport au Comité permanent R au terme de celles-ci. Dans ce cas, '*le rapport se limite aux informations qui sont nécessaires à l'accomplissement par le Comité permanent R de ses missions*' (art. 43, alinéa 3, L.Contrôle).

En 2019 également, le Service d'Enquêtes R a effectué des devoirs d'enquête dans le cadre de missions judiciaires, plus précisément dans le cadre de deux informations judiciaires.

---

167 En ce qui concerne les membres des autres 'services d'appui' de l'OCAM, cette disposition ne s'applique qu'à l'égard de l'obligation de communiquer des renseignements pertinents à l'OCAM (articles 6 et 14 L.OCAM).

Le Service d'Enquêtes R a finalisé, en 2019, une enquête initiée en 2017 et menée sur réquisition du Parquet fédéral. Cette enquête portait sur l'éventuelle implication d'un membre d'un service de renseignement dans un crime ou un délit contre la sûreté intérieure et/ou extérieure de l'État. L'existence d'une éventuelle violation du secret professionnel par un autre membre du même service de renseignement à l'égard de cette personne a été corrélativement examiné.[168]

À la demande d'un juge d'instruction et sous la direction du Parquet fédéral, le Service d'Enquêtes R a également effectué plusieurs devoirs d'enquête dans le cadre d'une enquête sur des infractions commises par une bande criminelle et sur les éventuelles informations détenues par les services de renseignement à ce propos.

Par ailleurs, l'article 50 L. Contrôle dispose que *'[t]out membre d'un service de police qui constate un crime ou un délit commis par un membre d'un service de renseignements rédige un rapport d'information et le communique dans les quinze jours au chef du Service d'enquêtes R'*. En 2019, le Service d'Enquêtes n'a reçu aucun signalement en ce sens.

168 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 41 ('II.9. Plainte relative à la transmission d'informations à caractère personnel à un tiers par un agent de renseignement').

CHAPITRE VIII
EXPERTISE ET CONTACTS EXTERNES

VIII.1. EXPERT DANS DIVERS FORUMS

En 2019, 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 :

- Invité par la VSSE, le président du Comité a participé, en mars 2019, à la réunion constitutive de l'*Intelligence Network Europe* (INE).[169] Cette initiative contribue à l'ambition de mettre en place une plateforme de formation pour les membres des services de renseignement, mais vise également les responsables politiques qui sont en contact avec le renseignement. Ce réseau est intergouvernemental et ne cherche pas à acquérir une infrastructure physique, mais entend se concentrer sur les connexions et le réseautage.
- Le président et le greffier ont été invités à participer, à Berlin, en mai 2019, à l'atelier de l'*European Intelligence Oversight Network* (EION), ayant pour thème '*How can oversight bodies better assess and demonstrate the effectiveness of their control instruments*', '*What insights can be distilled from other systems, such as banking supervisory authorities or antitrust compliance programs, to identify innovations for intelligence oversight ?*'
- En novembre 2019, à la demande de la *Stiftung Neue Verantwortung* allemande, le greffier a apporté sa contribution (*'A simple yet existential demand : let oversight bodies work together'*) à la nouvelle plateforme de communication en ligne (www.aboutintel.eu) qui vise notamment à être une source d'inspiration, à rendre le travail de renseignement, la technologie et la démocratie ainsi que les contributions spécialisées sur ces thèmes accessibles à un large public et à promouvoir la compréhension mutuelle des différents acteurs issus du monde du renseignement.
- Le greffier du Comité permanent R a été invité à expliquer le fonctionnement du Comité dans le cadre du module de formation 'Intelligence' du Master en relations internationales et de diplomatie (Université d'Anvers) ;

[169] À l'origine, l'initiative était dénommée 'Académie européenne de Renseignement (AeR)', mais pour souligner le caractère de réseau, le choix s'est finalement porté sur INE (et l'adage *'Enhancing a common strategic culture'*). Il s'agit de la concrétisation d'un appel lancé par le président français Macron en septembre 2017 en faveur d'une culture du renseignement européenne.

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

Avec la Loi du 12 mai 2019 et après de longues années d'insistance, l''Institut des droits de l'homme' (dont le nom complet est l''Institut fédéral pour la protection et la promotion des droits humains'), a été créé.[170] La création d'un Institut national des droits de l'homme, qui est un engagement pris lors de la signature du Protocole dans le cadre de la convention des Nations Unies contre la torture, s'est fait attendre longtemps. La Belgique s'est d'ailleurs fait réprimander à plusieurs reprises, entre autres par les Nations Unies.

En attendant la création effective de l'institut, les réunions de différentes institutions dotées d'un mandat en matière de droits de l'homme[171] ont donné lieu, en janvier 2015, à la conclusion d'un protocole de coopération.[172] Les instances participantes s'y étaient accordées pour échanger des pratiques et des méthodes, pour examiner des questions communes et pour promouvoir la coopération mutuelle.

L'institut nouvellement créé ('Institut fédéral pour la protection et la promotion des droits humains') s'est vu confier différentes missions : rendre, sur demande ou d'initiative, des avis et des recommandations sur des questions en rapport avec la promotion et la protection des droits fondamentaux, suivre la mise en œuvre des obligations internationales que les autorités belges se sont engagées à respecter et stimuler la ratification des nouveaux instruments internationaux en matière de droits humains. Un an après la publication de la loi organique, la Chambre a constitué un conseil d'administration en nommant douze personnes indépendantes issues du milieu académique, du monde judiciaire, de la société civile ainsi que du milieu des partenaires sociaux.

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

La multiplication des échanges de données au niveau international entre les services de renseignement et de sécurité pose un certain nombre de défis aux organes de contrôle nationaux. Les organes de contrôle de (au départ) cinq pays

170 Loi du 12 mai 2019 portant création d'un Institut fédéral pour la protection et la promotion des droits humains, *M.B.* 21 juin 2019.

171 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, l'Autorité de protection des données, le Médiateur fédéral, le Conseil supérieur de la Justice, les Comités permanents R et P.

172 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.

européens (la Belgique, le Danemark, les Pays-Bas, la Norvège et la Suisse)[173] collaborent afin de relever ces défis, en identifiant des méthodes de travail qui leur permettraient de limiter le risque de lacunes dans le contrôle. Après un certain temps, un nouveau partenaire a été impliqué dans ce projet, à savoir l'*Investigatory Powers Commissioner's Office (IPCO)* du Royaume-Uni. Le groupe a été rebaptisé 'Intelligence Oversight Working Group' (IOWG) et, en 2019, a été élargi à trois observateurs, à savoir le *Swedisch Foreign Intelligence Inspectorate (Statens inspektion av försvarunderättelse-verksamhet (SIUN))*, le *Swedish Board of Inventions (Statens uppfinnarnämnd, (SUN))* et la Commission G10 allemande.

Les partenaires estiment que le contrôle tel qu'il existe nécessite une collaboration plus intense entre les organes de contrôle nationaux. Le mandat qui est actuellement strictement national et les règles de classification nationales représentent des défis pour le contrôle qui, dans le cadre des échanges de données, ne peut encore voir qu'une face de la médaille. L'augmentation des volumes de transferts de données, des échanges multilatéraux et des banques de données communes constituent un autre défi pour les organes de contrôle, d'autant plus que la réglementation en la matière est plutôt sommaire et diffère d'un pays à l'autre. Enfin, les évolutions technologiques compliquent encore la mission des organes de contrôle.

Ces dernières années, des experts se sont réunis à diverses reprises en vue d'échanger leurs expériences et de discuter de leurs méthodes, de leurs meilleures pratiques ainsi que des écueils juridiques auxquels ils sont confrontés. De plus, une enquête de contrôle 'commune' a été menée (cf. I.3). Début novembre 2018, une déclaration commune et un communiqué de presse ont été rédigés par les organes de contrôle participants.[174]

En mars 2019, le Comité a organisé à Bruxelles une réunion qui s'inscrivait dans le cadre du nouveau projet d'étudier deux sujets communs avec ces instances : d'une part, les implications de l'introduction du nouveau système PNR pour le fonctionnement des services de renseignement et sur le contrôle exercé sur ceux-ci, et d'autre part, l'innovation du contrôle, en particulier en utilisant une méthodologie d'enquête commune et les moyens ICT qui y sont associés.

À la mi-décembre 2019, la '*Charter of the Intelligence Oversight Working Group*'[175] a été signée à l'initiative de la Commission de contrôle des services de renseignement néerlandaise.

---

173 Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2015*, 80-81.

174 Voir COMITÉ PERMANENT R, *Rapport d'activités 2018*, Annexe D. 'Renforcement du contrôle des échanges internationaux de données entre les services de renseignement et de sécurité'.

175 Voir l' 'Annexe D'du présent rapport d'activités.

VIII.4. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

En 2019, le Comité permanent R a continué à entretenir des contacts étroits avec plusieurs organes de contrôle étrangers.

Dans l'optique de créer un cadre normatif pour la collaboration internationale entre les services de renseignement et les organes de contrôle, les premiers contacts ont été établis avec diverses instances du Benelux. La thématique n'a cependant pas pu être mise à l'agenda du Comité de Ministres Benelux.

Lors d'un colloque qui s'est tenu début février 2019 à l'École Militaire française, les liens ont été renforcés avec les présidents de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et de la Délégation parlementaire au renseignement (DPR), qui intervenaient dans le cadre du panel intitulé '*Le droit du renseignement – un droit exorbitant du droit commun fortement contrôlé*').

Comme à l'accoutumée, il y a également eu des contacts bilatéraux avec l'organe de contrôle néerlandais ; à l'occasion d'une réunion de travail organisée à Bruxelles en avril 2019, le concept néerlandais de *system based oversight* a été expliqué, et une concertation a eu lieu sur la stratégie à suivre en matière de partenariats étrangers. En mai 2019, une réunion de deux jours a été organisée avec des représentants de la Commission spéciale chargée d'autoriser les mesures de surveillance et de contrôle des télécommunications ainsi que le repérage des données relatives au trafic et avec l'ensemble de la délégation de la Commission de contrôle du Service de renseignement de l'État'. En outre, les présidents du Comité et la Commission nationale de contrôle des techniques de renseignement (CNCTR) française se sont concertés à Paris en juin 2019. Des contacts ont été noués avec le nouvel *Investigatory Powers Commissioner* (Royaume-Uni) pour faire connaissance. À la faveur de l'entrée en vigueur, en juillet 2019, de la Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, un nouvel organe de contrôle canadien a été créé. Il s'agit de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR), qui est doté d'un mandat plus large que son prédécesseur. Les deux présidents se sont accordés sur l'organisation d'une visite de travail. Le Comité permanent R et l'Autorité (suisse) de surveillance indépendante des activités de renseignement (AS-Rens) ont entretenu des contacts privilégiés en vue de l'organisation d'un stage/d'un projet d'échange dans le courant de l'année 2020.

En octobre 2019, Londres a accueilli la troisième édition de l'*international Intelligence Oversight Forum* sur l''Intelligence oversight at a crossroads', organisé par le *Special Rapporteur for Privacy* (SRP) des Nations Unies, le Prof. Cannataci. Des représentants des organes de contrôle, des services de

renseignement, du milieu académique et des ONG y ont participé. L'objectif de ce forum était de favoriser, au sein d'un environnement confidentiel, une meilleure compréhension des défis auxquels sont confrontés, entre autres, les organes de contrôle démocratiques.[176]

VIII.5. MÉMORANDUM

Dans la foulée des élections législatives fédérales de mai 2019, le Comité permanent R a introduit un Mémorandum à l'intention des (anciens) informateurs.[177, 178] Le Comité ne doutait pas de l'intérêt mérité qui a été accordé au bon fonctionnement des services de renseignement du pays et à la nécessité du maintien d'un contrôle démocratique et effectif de ceux-ci. Le Mémorandum, qui était rédigé dans cette optique, entendait attirer l'attention des informateurs sur l'importance de certaines initiatives législatives en la matière. Les propositions reprises dans le document portaient notamment sur une adaptation de la Loi Contrôle, une intérêt pour le renforcement du Comité dans son fonctionnement, les exigences dans le cadre de la protection des données à caractère personnel (et l'installation d'un réseau sécurisé), la nécessité d'instaurer un service contrôle et d'audit interne au sein des services de renseignement ainsi que la digitalisation et la simplification des procédures pour l'Organe de recours de matière d'habilitations, d'attestations et d'avis de sécurité.

176 Avec des thèmes tels que '*Relationship between overseers and overseen (outreach, transparancy, personnel selection*', '*Oversight across the intelligence cycle*', '*Making oversight affordable and accessible for the citizen*', etc.

177 Les deux services de renseignement, les ministres de la Défense et de la Justice ainsi que le Président de la Chambre des représentants en étaient eux aussi les destinataires.

178 À la demande de l'informateur du Roi de l'époque, le Comité avait déjà pris une initiative similaire après les élections législatives fédérales de juin 2007 (COMITÉ PERMANENT R, *Rapport d'activités 2007*, 50-51).

CHAPITRE IX
L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ[179]

IX.1. INTRODUCTION

L'Organe de recours est la juridiction administrative compétente 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.[180]

L'Organe de recours est composé du président du Comité permanent R, du président du Comité permanent P et du président de la Chambre contentieuse de l'Autorité de protection des données. Le président du Comité permanent R assure la présidence de l'Organe de recours. La fonction de greffier est exercée par le greffier du Comité permanent R et le personnel du greffe est le personnel affecté par le Comité. Les activités de l'Organe de recours constituent depuis plus de vingt ans l'exemple parfait de synergie au sein de certaines institutions satellitaires du Parlement.

Le fonctionnement de l'Organe de recours est en effet supporté intégralement par le Comité permanent R. Il s'agit, d'une part, de la mise à disposition du président et de ses membres suppléants, de son greffier mais aussi de juristes et du personnel administratif qui forment le greffe de cette juridiction administrative. D'autre part, le Comité permanent R prend en charge, sur son budget, les frais de locaux comme de fonctionnement de l'Organe de recours.

---

179 Le présent rapport d'activités exécute l'article 13 de la Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité qui stipule que l'organe de recours est tenu de rédiger un rapport annuel.

180 Pour plus de détails, voir COMITÉ PERMANENT R, *Rapport d'activités 2006,* 87-120 et COMITÉ PERMANENT R, *Rapport d'activités 2018,* 111-124.

Le greffier, assisté des juristes et du personnel du Comité permanent R, veille à la tenue du greffe, la réception et la préparation des dossiers de recours en vue des audiences.

IX.2. UNE PROCÉDURE PARFOIS LOURDE ET COMPLEXE

L'augmentation du nombre de dossiers observée en 2019 (voir *infra*) va de pair avec une croissance de la charge de travail. La gestion administrative des dossiers, des audiences et des décisions, demeure complexe. Certes, la qualité du dossier qui est constitué est l'une des causes, mais l'intervention de plus en plus fréquente d'avocats a aussi un impact non négligeable. En effet, l'Organe de recours est contraint, à juste titre, de motiver ses décisions en répondant à tous les arguments soulevés par les conseils dans la défense des intérêts de leur client.

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'*. Il y aura lieu *de lege ferenda* de mieux prendre en compte la qualité, voire la fragilité, de nombreux requérants et de prévoir des dispositions légales qui n'entraînent pas la nullité de plein droit.

En outre, la manière dont les différentes autorités (de sécurité) concernées traitent administrativement ces dossiers génère parfois un surcroît de travail et du retard dans le traitement des dossiers. De toute évidence, ce retard peut aller à l'encontre des intérêts du requérant. Afin d'y remédier, l'Organe de recours a régulièrement informé ces autorités des problèmes suivants :

- Le délai légal dans lequel le dossier administratif doit être transmis à l'Organe de recours est fréquemment dépassé. Il est donc difficile pour l'Organe de recours de rendre ses décisions dans les délais impartis.
- Les dossiers administratifs transmis par les différentes autorités de sécurité, ne sont pas toujours complets, ce qui oblige le greffe à effectuer des démarches supplémentaires. Il s'avère parfois que le dossier n'est constitué qu'après l'introduction du recours.
- L'application de l'article 5 § 3 L. Org.recours est souvent problématique. Cette disposition permet à l'Organe de recours, à la demande d'un service de renseignement ou d'un service de police, de décider de soustraire certaines pièces à la consultation du requérant ou de son avocat lorsque la divulgation de ces pièces est susceptible de porter préjudice à la protection des sources, à la vie privée de tiers ou à l'accomplissement des missions légales des services de renseignement ou encore au secret de l'information ou de l'instruction judiciaire. Toutefois, il est rare que la demande soit (correctement) motivée, ou bien elle 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. En outre, il arrive souvent que ces autorités restent attachées à l'idée erronée que le requérant et son avocat ne peuvent pas consulter des données classifiées sans motivation supplémentaire, et ce en dépit de la jurisprudence constante de l'Organe de recours selon laquelle la L. Org.recours est une *lex specialis* par rapport à la Loi Classification. Enfin, il y a aussi des cas où le Président de l'Organe de recours doit soustraire d'office des éléments du dossier parce que le service concerné a manifestement omis d'invoquer l'article 5 § 3 L. Org.recours aux fins de protection de la vie privée de tiers.

- Les décisions des autorités de sécurité ne sont pas suffisamment motivées et, contrairement à ce que la loi exige, aucune décision pleinement motivée n'est établie dans les cas où l'article 22, alinéa 5 L.C&HS permet de ne pas reprendre certains éléments dans la décision qui est communiquée à l'intéressé. En outre, dans la motivation, il incombe à l'autorité de sécurité de spécifier quels faits concrets constituent une contre-indication compte tenu de la finalité réglementairement établie d'une vérification de sécurité déterminée. Il s'agit de la seule manière pour l'Organe de recours de vérifier la proportionnalité d'une décision.
- Par ailleurs, il y a lieu de constater que, dans leurs décisions, diverses autorités de sécurité n'ont pas respecté les principes formels de droit administratif (décisions dépourvues de dates ou de l'identité du fonctionnaire qui les a adoptées, problème de délégation de pouvoir, absence d'audition de l'intéressé, emploi de la langue en matière administrative).
- Les autorités de sécurité ne suivent pas la jurisprudence constante de l'Organe de recours (par exemple, en ce qui concerne la problématique des enquêtes ou des vérifications à propos de personnes qui n'ont pas la nationalité belge).

Par ailleurs, force est de constater que les audiences durent beaucoup plus longtemps qu'il y a quelques années. Les raisons sont de plusieurs ordres. De plus en plus de requérants se font assister par un (voire deux) avocat(s). La complexité de certains dossiers nécessite beaucoup de temps. Par conséquent, l'Organe de recours est contraint de multiplier les décisions avant dire droit au fond ou d'accorder des remises.

Il en résulte une multiplication des audiences. Elles sont effectivement nécessaires pour obtenir les renseignements complémentaires indispensables à la juridiction pour trancher.

Le processus de décision même requiert lui aussi davantage de temps qu'il y a plusieurs années, et ce pour deux raisons majeures. D'une part, le nombre élevé de questions procédurales (par ex. la recevabilité, l'emploi des langues, les droits de la défense ou la délégation de compétence de l'autorité qui prend sa décision).

D'autre part, l'Organe de recours est plus souvent confronté à des dossiers hautement sensibles. De tels dossiers nécessitent évidemment un traitement extrêmement minutieux et une motivation adaptée résultant de l'équilibre fragile entre la nécessité pour le justiciable de comprendre la décision et la nécessité de retenir des informations qui peuvent mettre en danger la sécurité de l'État ou de ses institutions.

Par ailleurs, il arrive que des mesures de sécurité spécifiques doivent être prises.

IX.3. L'ÉVOLUTION DU CADRE JURIDIQUE : DEUX MODIFICATIONS LÉGALES

En 2018, le cadre juridique avait considérablement évolué, tant au niveau de la L.C.&HS que de la L.Org.recours.

En 2019, seules deux modifications (d'une importance relative pour le travail de l'Organe de recours) ont été apportées par le législateur. La première concernait la définition des témoins protégés visés à l'article 3 de la L.C&HS.[181] La seconde avait pour objet d'exempter les journalistes professionnels accrédités du paiement de la rétribution visée à l'article 22*septies* de ladite loi.[182]

IX.4. LE DÉTAIL DES CHIFFRES

Cette section reprend les chiffres relatifs à la nature des décisions contestées, la qualité des autorités compétentes et des requérants, ainsi que la nature des décisions de l'Organe de recours dans le cadre des différentes procédures de recours. À des fins de comparaison, les chiffres des quatre années précédentes sont également repris.

La tendance globale des chiffres sur les dernières années montre une hausse des recours soumis à l'Organe de recours. Cette augmentation s'articule autour de trois axes principaux : tout d'abord, une recrudescence des recours concernant les habilitations de sécurité (de 36 en 2018 à 51 en 2019). Par ailleurs, après une année en recul, le contentieux en matière d'avis de sécurité est également en nette progression (de 92 en 2018 à 115 en 2019). Enfin, les recours concernant les refus d'attestations de sécurité pour le secteur nucléaire sont également en hausse (de 11 en 2018 à 17 en 2019).

---

181 Loi du 5 mai 2019 portant dispositions diverses en matière pénale et en matière de cultes, et modifiant la loi du 28 mai 2002 relative à l'euthanasie et le Code pénal social (*M.B.* 24 mai 2019).

182 Loi du 2 mai 2019 portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (*M.B.* 27 mai 2019).

On relèvera que l'Organe de recours a connu pour la première fois la question de l'octroi d'une attestation de sécurité à un imam en vue de travailler au sein des établissements pénitentiaires belges sur base du prescrit de l'arrêté royal du 17 mai 2019.[183]

La juridiction a également été saisie de la question de l'octroi de l'avis de sécurité pour les agents des douanes amenés à porter une arme dans le cadre de l'exercice de leur fonction et ce conformément au prescrit de l'arrêté royal du 15 décembre 2013.[184]

À la connaissance de l'Organe de recours, il n'a pas encore été fait usage de la nouvelle procédure d'avis de sécurité décrite dans le rapport d'activité de l'année 2018. Selon certains échos, il existerait une volonté de renforcer, à l'avenir, les contrôles d'intégrité et de moralité concernant du personnel des institutions européennes et des ports. Il est possible que cette nouvelle procédure d'avis de sécurité soit mise en œuvre à ce propos.

Enfin, 21 audiences de l'Organe de recours ont été organisées en 2019.

Tableau 1. Autorités de sécurité concernées

	2015	2016	2017	2018	2019
Autorité nationale de sécurité	68	92	129	113	114
Sûreté de l'État	1	0	0	0	0
Service Général du Renseignement et de la Sécurité	47	68	53	32	61
Agence fédérale de Contrôle nucléaire	10	8	7	10	17
Police fédérale	3	1	3	3	3
Police locale	1	0	0	0	1
TOTAL	**130**	**169**	**192**	**158**	**196**

Tableau 2. Nature des décisions contestées

	2015	2016	2017	2018	2019
Habilitations de sécurité (art. 12 et s. L.C&HS)					
Confidentiel	9	5	1	2	5
Secret	35	38	33	31	39
Très secret	4	7	6	3	7

183 Arrêté royal du 17 mai 2019 relatif aux aumôniers, aux conseillers des cultes et aux conseillers moraux auprès des prisons (article 3 § 3,1°).

184 Arrêté royal du 15 décembre 2013 déterminant les fonctions de l'Administration générale des Douanes et Accises dont l'exercice peut requérir une vérification de sécurité.

	2015	2016	2017	2018	2019
Refus	36	28	30	26	39
Retrait	7	9	7	4	16
Refus et retrait	0	0	0	0	0
Habilitation pour une durée limitée	3	4	1	1	3
Habilitation pour un niveau inférieur	0	1	0	0	0
Pas de décision dans les délais	2	7	2	5	0
Pas de décision dans les nouveaux délais	0	1	0	0	0
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	48	50	40	36	51
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)					
Refus	6	1	3	3	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	12	9	20	15	12
Retrait	1	0	0	0	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	7	11	17
Retrait	–	1	0	0	0
Pas de décision dans le délai	–	0	0	1	0
Avis de sécurité (art. 22*quinquies* L.C&HS)					
Avis négatif	63	101	122	92	115
Pas d'avis	0	0	0	0	0
Révocation d'avis positif	0	0	0	0	0
Actes normatifs d'une autorité administrative (art. 12 L. Org.recours)					
Décision d'une autorité publique d'exiger des attestations de sécurité	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des attestations de sécurité	0	0	0	0	0
Décision d'une autorité administrative d'exiger des avis de sécurité	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des avis de sécurité	0	0	0	0	0
SOUS-TOTAL ATTESTATIONS ET AVIS	82	119	152	122	145
TOTAL DÉCISIONS CONTESTÉES	130	169	192	158	196

Tableau 3. Nature du requérant

	2015	2016	2017	2018	2019
Fonctionnaire	4	2	4	5	4
Militaire	29	23	20	8	27
Particulier	93	139	164	140	163
Personne morale	4	5	4	5	2

Tableau 4. Langue du requérant

	2015	2016	2017	2018	2019
Français	75	99	115	83	101
Néerlandais	54	70	77	75	95
Allemand	0	0	0	0	0
Autre langue	1	0	0	0	0

Tableau 5. Actes du greffe

	2015	2016	2017	2018	2019
Demande du dossier complet (1)	130	167	191	154	191
Demande d'informations complémentaires (2)	7	23	36	12	18
Rappels adressés aux autorités de sécurité (3)	/	/	/	/	21[185]

(1) L'Organe de recours peut demander l'intégralité du dossier aux autorités de sécurité. Comme ce dossier contient davantage de données que le rapport d'enquête seul, cette requête est systématiquement effectuée par le greffe.

(2) L'Organe de recours peut également demander tout complément d'informations qu'il juge nécessaire pendant la procédure. Dans la pratique, le greffe se charge de demander aux autorités de compléter les dossiers.

(3) L'art. 6 de l'AR Org.recours prévoit les délais pour la communication des dossiers par les autorités de sécurité. Ces délais prennent cours lorsque le greffier transmet une copie du recours à l'autorité de sécurité concernée. Ils varient selon la nature de l'acte attaqué. Ainsi, l'autorité de sécurité doit

185 Il s'agit des rappels adressés par courriel par le greffe aux autorités de sécurité (11 rappels concernaient des dossiers d'enquête, 2 rappels concernaient des dossiers de vérification de sécurité en matière d'attestations de sécurité et 8 rappels concernaient des dossiers de vérification de sécurité en matière d'avis de sécurité). De nombreux rappels ont également été adressés par téléphone mais ne peuvent être comptabilisés ni repris, pour des raisons pratiques, dans les présentes statistiques.

communiquer son dossier dans les 15 jours en ce qui concerne les habilitations de sécurité, dans les 5 jours en matière d'attestations de sécurité et dans les 10 jours si le recours porte sur un avis de sécurité. Lorsque ces délais ne sont pas respectés, le greffe prend les contacts nécessaires. Ces données sont comptabilisées à partir de 2019.

Tableau 6. Actes juridictionnels interlocutoires pris par l'Organe de recours[186]

	2015	2016	2017	2018	2019
Audition d'un membre d'une autorité (1)	7	10	0	1	6
Décision du président (2)	0	0	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (3)	50	54	80	72	77
Décisions avant dire droit (4)	/	/	/	/	9[187]

(1) 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.
(2) 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.
(3) Si le service de renseignement ou de police concerné le demande, l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant.
(4) Il peut s'agir par exemples d'une décision de jonction de deux dossiers ou de demander un complément d'informations à propos de la situation d'un dossier judiciaire. Ces données sont comptabilisées à partir de 2019.

Tableau 7. Manière dont le requérant fait usage de ses droits de défense

	2015	2016	2017	2018	2019
Consultation du dossier par le requérant et/ou l'avocat	84	87	105	69	96
Audition du requérant (assisté ou non d'un avocat)[188]	107	127	158	111	143

186 Le nombre d'actes juridictionnels interlocutoires' (tableau 6), les 'manières dont les requérants font usage de leurs droits de défense' (tableau 7), ou encore la 'nature des décisions de l'Organe de recours' (tableau 8) 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 2019, alors que la décision n'a été rendue qu'en 2020.

187 Parmi ces décisions avant dire droit, 5 ont été prises en matière d'habilitation de sécurité, 1 en matière d'attestation de sécurité et 3 en matière d'avis de sécurité.

188 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.

Tableau 8. Nature des décisions de l'Organe de recours

	2015	2016	2017	2018	2019
Habilitations de sécurité (art. 12 et s. L.C&HS)					
Recours irrecevable	4	0	3	0	1
Recours sans objet	3	7	0	4	3
Recours non fondé	19	18	13	12	12
Recours fondé (avec octroi partiel ou complet)	24	24	24	12	25
Devoir d'enquête complémentaire par l'autorité	0	2	0	1	1
Délai supplémentaire pour l'autorité	1	2	1	1	0
Donne acte de retrait de recours	1	0	0	3	2
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)					
Recours irrecevable	0	0	1	0	0
Recours sans objet	0	0	1	0	0
Recours non fondé	4	1	0	1	1
Recours fondé (avec octroi)	2	1	1	0	3
Donne acte de retrait de recours	–	–	–	–	1
Attestations de sécurité pour lieux ou événements (art. 22*bis*, al.2 L.C&HS)					
Recours irrecevable	0	0	1	2	4
Recours sans objet	0	0	1	0	0
Recours non fondé	8	2	12	2	4
Recours fondé (avec octroi)	10	4	7	3	4
Donne acte de retrait de recours	2	0	1	2	0
Attestations de sécurité pour le secteur nucléaire (art. 8*bis* § 2 L.C&HS)					
Recours irrecevable	–	1	1	0	1
Recours sans objet	–	1	0	1	0
Recours non fondé	–	0	1	1	5
Recours fondé (avec octroi)	–	7	5	6	7
Donne acte de retrait de recours	–	–	–	2	0
Avis de sécurité (art. 22*quinquies* L.C&HS)					
Organe de recours non compétent	0	0	20[189]	12	0

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

	2015	2016	2017	2018	2019
Recours irrecevable	6	15	10	3	7
Recours sans objet	0	0	1	3	1
Confirmation de l'avis négatif	28	42	49	46	40
Transformation en avis positif	23	46	41	27	43
Donne acte de retrait de recours	0	0	1	0	1
Recours contre des actes normatifs d'une autorité administrative (art. 12 L. Org.recours)	0	0	0	0	0
TOTAL	135[190]	173	195	144	166

IX.5. PERSPECTIVES

Sous l'impulsion du Président, de vastes réflexions et démarches ont été entamées en vue de moderniser le fonctionnement de l'Organe de recours. Plusieurs grands objectifs sont en ligne de mire : la simplification et l'uniformisation de la procédure, l'amélioration de l'accès à la juridiction par le citoyen et le traitement informatisé des dossiers par le greffe.

Comme d'autres juridictions, l'Organe de recours s'est engagé à simplifier son langage juridique.

Transformer l'Organe de recours en une juridiction plus accessible, plus performante et plus moderne nécessite de modifier la loi organique et l'Arrêté royal réglant la procédure devant l'Organe de recours. Dans cette démarche de révision des textes de base, il a été fait appel à un expert externe. Il s'agit de Monsieur Ivan Verougstraete, ancien Président de la Cour de cassation, avec qui plusieurs réunions ont eu lieu.

Dans ce cadre, une procédure plus simple comprenant des délais de recours uniformes doit être élaborée. Cette même procédure devra en outre permettre l'introduction par le justiciable de sa requête par voie électronique et d'obtenir du greffe, par la même voie, les courriers et autres notifications de décisions.

Enfin, ce projet entend créer les conditions d'une consultation à distance des dossiers en tenant compte des questions de classification éventuelle de certaines pièces composant le dossier.

Ad futurum, la communication électronique sécurisée tant du dossier avec ses pièces que des décisions devra être la règle avec les diverses autorités de sécurité.

Cette volonté de simplification va de pair avec le développement d'une plateforme informatique destinée à permettre au greffe de traiter intégralement un recours par voie informatique.

190 Il y avait encore deux autres décisions spécifiques donnant acte de retrait de recours, ce qui portait le total à 137 en 2015.

Parallèlement à cette initiative, un site internet spécifique à la juridiction est en cours de développement. Les justiciables, les barreaux ainsi que les autorités administratives trouveront toutes les informations utiles. Il sera conçu de telle manière qu'il puisse permettre, dans la perspective d'une évolution législative, d'introduire les recours par voie électronique. En outre, les parties pourront être en contact avec le greffe via cette plateforme au sujet de leur dossier.

Relevons encore que des réflexions sont en cours concernant la publication des décisions sur ce site internet. Il est important que la jurisprudence de l'Organe de recours soit accessible à tous. Ceci est un gage de transparence d'une institution pour le citoyen. Cette publication prendra une forme anonymisée en ayant égard à ce que l'information ne soit pas de nature à porter atteinte à un intérêt majeur de l'État, au secret d'une information ou d'une instruction judiciaire en cours, à la protection des sources ou à la protection de la vie privée de tiers.

CHAPITRE X
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

X.1. COMPOSITION DU COMITÉ PERMANENT R

En 2019, la composition du Comité n'a subi aucune modification. Serge Lipszyc, premier substitut de l'auditeur du travail près de l'auditorat du travail de Liège (F), qui a prêté serment en septembre 2018[191], a en effet continué à remplir sa mission de président. Le conseiller Laurent Van Doren (F), précédemment commissaire divisionnaire de police[192], et le conseiller Pieter-Alexander De Brock (N) sont restés en fonction. Bien que le mandat de ce dernier arrivait à son terme en mai 2019, sa reconduction n'est intervenue qu'à la mi-janvier 2020.[193]

Un changement est en revanche intervenu au sein du Service d'Enquêtes, avec le recrutement d'un commissaire auditeur supplémentaire, spécialisé en Technologies de l'Information et de la Communication (ICT). Il a quitté le service quelques mois après son entrée en fonction et a été remplacé en septembre 2019. Le Service d'Enquêtes est désormais composé de six commissaires auditeurs, dont le directeur Frank Franceus (N).

Le cadre administratif du Comité permanent R, placé sous la direction du greffier Wouter De Ridder (N), est resté inchangé en 2019 et comptait 18 collaborateurs. Des offres d'emploi sont néanmoins parues pour pourvoir au recrutement d'un(e) juriste statutaire francophone, d'un(e) juriste statutaire néerlandophone et d'un(e) secrétaire statutaire francophone.[194] Le Comité a pu continuer à faire appel au *Data Protection Officier* (DPO), désigné pour tous les traitements de données qui ne relèvent pas de la 'sécurité nationale' (par ex. les traitements effectués dans le cadre de la gestion du personnel et de la logistique).

---

191 Le 28 février 2019, Vanessa Samain et Didier Maréchal ont été désignés respectivement comme premier et second président suppléant.

192 Plusieurs appels à candidats ont dû être lancés en 2018 pour les mandats de premier et second membre suppléant du membre francophone du Comité. Le 28 février 2019, Thibaut Vandamme et Michel Croquet ont respectivement été désignés comme premier et second suppléant.

193 *C.R.I.* Chambre 2019-20, PLEN 020, 52.

194 *M.B.* 13 juin 2019 et *M.B.* 22 octobre 2019.

X.2. RÉUNIONS AVEC LA COMMISSION DE SUIVI

La Chambre des représentants a adapté son règlement lors de sa séance plénière du 17 octobre 2019, ce qui a modifié la composition 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. Désormais, il est procédé à autant de nominations qu'il est nécessaire pour que chaque groupe politique représenté dans les commissions permanentes soit représenté par un membre au moins au sein de la commission. Chaque groupe politique qui n'est pas représenté au sein de la commission désigne parmi ses membres un membre qui participera aux activités de la commission, mais sans voix délibérative.[195] Les membres avec voix délibérative sont les suivants[196] : Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen), Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Marco Van Hees (PVDA-PTB), Egbert Lachaert (Open Vld) et Meryame Kitir (sp.a). Depuis juin 2019, la Commission se réunit sous la présidence du Président de la Chambre Patrick Dewael (Open Vld). Georges Dallemagne (cdH) participe en tant que membre ne disposant pas d'une voix délibérative.

Dans le courant de l'année 2019, deux réunions seulement ont eu lieu avec la Commission. Plusieurs enquêtes de contrôle clôturées par le Comité permanent R ont été discutées lors de réunions à huis clos. Du temps a également été consacré au rapport annuel sur l'application des méthodes spécifiques et exceptionnelles par les services de renseignement et au contrôle exercé par le Comité sur la mise en œuvre de ces méthodes (art. 35 L.Contrôle) ainsi qu'au rapport rédigé dans le cadre de sa compétence de contrôle – conjointement à l'Organe de contrôle de l'information policière (C.O.C.) – concernant les banques de données (art. 44/6 LPD). Lors de sa réunion du 17 décembre 2019, le *Rapport d'activités 2018* du Comité permanent R a été discuté.[197] Le Comité a été remercié pour *'son rapport fouillé qui constitue un instrument très utile pour la commission'*. Une série de thématiques ont particulièrement retenu l'attention des Députés, comme le fonctionnement du SGRS, le contrôle du suivi des mandataires politiques, ou encore le suivi des recommandations. En guise de conclusion, la Commission a pris *'acte du rapport d'activités 2018 du Comité R'*.

---

195 *M.B.* 25 octobre 2019. *'Cette modification du règlement prévoit une composition plus restreinte [des commissions de suivi, à savoir (l)]es Comités P et R, ce qui devrait en augmenter l'efficacité'*, *C.R.I.* Chambre 2019-20, 17 octobre 2019, PLEN 009, 33.

196 *C.R.I.* Chambre 2019-20, 24 octobre 2019, PLEN 010, 2.

197 La Commission se réfère à cet effet à l'article 66*bis*, § 2, L.Contrôle, tel que modifié par la loi du 6 janvier 2014 modifiant diverses lois de réformes institutionnelles, *M.B. 31 janvier 2014*.

Contrairement aux années précédentes, la Commission n'a pas explicitement souscrit aux recommandations du Comité.[198]

Courant décembre 2019, le Président de la Chambre a reçu la 'Charter of the Intelligence Oversight Working Group' signée dans le cadre du développement des relations internationales de six organes de contrôle[199] ainsi que le 'Plan de gestion 2019-2022 du Comité permanent'.[200] Ce plan renferme un 'mission statement' visant à établir le rôle institutionnel du Comité, la finalité des missions et les valeurs qu'il souhaite promouvoir, et il reprend une énumération des objectifs stratégiques et opérationnels.

X.3. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

En 2019, cinq réunions communes ont été organisées, sans compter les contacts informels. Les articles 52 à 55 L.Contrôle déterminent les cas où le Comité permanent R et le Comité permanent P doivent organiser des réunions communes et la manière dont ils doivent les organiser. La présidence de ces réunions communes est exercée en alternance par les présidents des deux Comités (art. 54 L.Contrôle). Ces rencontres poursuivent un double objectif : d'une part, échanger des informations, et, d'autre part, initier des enquêtes de contrôle communes et discuter des enquêtes en cours.

En 2019, il a été question d'une seule enquête de contrôle commune : l'enquête initiée précédemment sur les services d'appui de l'OCAM (cf. I.7.1). Il a été décidé de ne pas démarrer d'autre enquête commune (par ex. sur l'extrémisme de droite).

Par ailleurs, toute une série de points ont été mis à l'ordre du jour : le statut commun du personnel administratif, la rédaction d'une charte déontologique et l'adaptation du règlement d'ordre intérieur, la contradiction dans le cadre des enquêtes de contrôle, ou encore la recherche d'éventuelles synergies entre les deux institutions. En ce qui concerne ce dernier point, un protocole a notamment été conclu en ce qui concerne l'utilisation de la salle d'audience 'audio et vidéo', un entraînement au tir (commun) des commissaires auditeurs a été étudiée et une formation a été organisée dans le cadre des descentes judiciaires.

198 *Doc. parl.*, Chambre 2019-20, 55-0888/001, 20 janvier 2020 (Rapport d'activités 2018 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).

199 Voir l''Annexe D' du présent rapport d'activités.

200 Le plan a été approuvé le 18 octobre et transmis au Président de la Chambre le 9 décembre 2019.

X.4. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Le 'budget 2019' du Comité permanent R a été fixé à 4,211 millions d'euros, ce qui représente une augmentation de 12,02 % par rapport à 2018.[201] Cet accroissement important était dicté par l'implication du Comité dans l'exécution de la Loi du 30 juillet 2018 (*M.B.* 5 septembre 2018) relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, découlant directement du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Le Titre III de cette loi désigne le Comité permanent R comme 'autorité de protection des données à caractère personnel par les services de renseignement et de sécurité et par leur sous-traitants'. Cette nouvelle mission imposait un renfort en personnel par l'adjonction de deux juristes et d'un commissaire auditeur.

Les sources de financement attribuées par la Chambre des représentants[202] sont les suivantes : 89,76 % au titre du budget de dotation et 10,24 % de boni de 2017.

La démission du Gouvernement le 21 décembre 2018 n'a pas permis de voter le projet de loi contenant le budget général des dépenses pour l'année budgétaire 2019. Cependant, la chronologie des travaux parlementaires a permis d'approuver formellement le budget 2019 et d'appliquer les dispositions de l'article 2 de la Loi du 25 décembre 2016[203], évitant ainsi l'application des dispositions concernant les douzièmes provisoires.

L'exécution du budget 2019 a produit un boni comptable de 475.019 euros, représentant la différence entre le budget approuvé et les dépenses constatées.

Traditionnellement, le budget est composé de différentes sources de financement dont le seul apport en termes de trésorerie nette est constitué par la dotation inscrite au budget général de l'État. Jusqu'en 2017, cette dotation ne suffisait pas à couvrir les dépenses réelles du Comité, ce qui générait une perte structurelle. La tendance à appliquer autant que possible l'article 57 alinéa 1er L.Contrôle, qui stipule que les crédits de fonctionnement sont inscrits au budget des dotations, permet à ce jour au Comité de financer ses activités.

Le dégagement d'un boni comptable considérable provient essentiellement de l'écart temporel existant entre l'approbation des budgets et notamment l'entrée effective en service du personnel à cause de la longueur des procédures de recrutement et de l'obtention des habilitations de sécurité requises. On peut cependant augurer que lorsque les nouveaux collaborateurs seront à charge de la

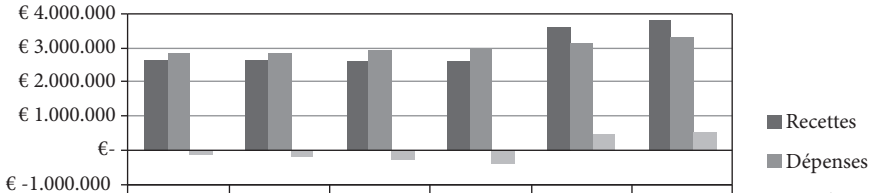
201 *C.R.I.* Chambre 2019-20, PLEN 020, 52.

202 *Doc. parl.* 2017-2018 Chambre, 54-3418/001, 57-58 et *C.R.I.* Chambre 2019-20, 20 décembre 2018, PLEN 264.

203 Loi du 25 décembre 2016 modifiant la loi du 22 mai 2003 portant organisation du budget et de la comptabilité de l'État fédéral, *M.B.* 29 décembre 2019 3° ed.

dotation, il y aura équilibrage naturel *ceteris paribus* entre les recettes et les dépenses.

Comité permanent R : Évolution du résultat



	2014	2015	2016	2017	2018	2019
Recettes	€ 2.626.	€ 2.597.	€ 2.570.	€ 2.565.	€ 3.582.3	€ 3.780.9
Dépenses	€ 2.799.	€ 2.792.	€ 2.889.	€ 2.937.	€ 3.106.8	€ 3.284.9
Résultat	€ -173.6	€ -194.9	€ -318.8	€ -372.5	€ 475.494	€ 496.019

Parallèlement à l'appropriation des nouvelles missions qui lui sont attribuées, le Comité permanent R veille à maintenir la recherche et la mise en place de synergies entre les différentes institutions émargeant au budget des dotations.

X.5. MISE EN ŒUVRE DES RECOMMANDATIONS DE L'AUDIT DE LA COUR DES COMPTES

À la demande de la Commission de la Comptabilité de la Chambre des représentants, la Cour des comptes a, dès 2017, initié une enquête sur les institutions à dotation, conjointement à Ernst & Young. Le Comité permanent R était donc concerné. La Cour des comptes s'est surtout concentrée sur les aspects budgétaires (une analyse des recettes et des dépenses) et sur la délimitation des missions des différentes institutions. De son côté, Ernst & Young était principalement chargé de procéder à une analyse approfondie des processus, des systèmes et de l'organisation de chacune de ces institutions. Le rapport d'audit[204] reprenant des recommandations concernant les 'missions' des neuf institutions à dotation concernées par l'audit a été transmis fin mars 2018. La caractéristique commune des missions de ces institutions *'ligt in het doel om tot een betere rechtsbescherming voor burgers te komen door het uitoefenen van verschillende vormen van toezicht in specifieke beleidsdomeinen'*.[205]

[204] *Institutions à dotation. Missions – Recettes– Dépenses.* Audit réalisé à la demande de Commission de la Comptabilité de la Chambre des représentants, Rapport approuvé le 28 mars 2018 par l'assemblée générale de la Cour des comptes.

[205] '*Réside dans l'objectif de parvenir à une meilleure protection juridique des citoyens en exerçant différentes formes de contrôle dans des domaines politiques spécifiques*' (traduction libre).

L'année 2019 a été placée sous le signe de la mise en œuvre de nombreuses recommandations de l'audit. Cet audit a mobilisé les énergies au Comité permanent R, venant s'ajouter à une charge de travail croissante (*supra*).[206]

X.6. FORMATIONS

Compte tenu de l'intérêt pour l'organisation, le Comité permanent R encourage ses membres et ses collaborateurs à suivre des formations générales (informatique, management, etc.) ou propres au secteur, ou encore à participer à des conférences.[207] Dans ce cadre, un protocole de coopération a été conclu en avril 2019 entre le Comité et l'Institut de Formation Judiciaire.[208] Un ou plusieurs membre(s) du Comité permanent R ou membre(s) de son personnel a/ont assisté aux journées d'étude reprises dans le tableau ci-dessous.

DATE	TITRE	ORGANISATION	LIEU
2019-2020	Hautes études de sécurité et défense	Institut royal supérieur de défense	Bruxelles
24-25 janvier 2019	Oversight	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD)	La Haye
31 janvier 2019	'Radicalisering, burgerschapszin en onderwijs'	Belgian Intelligence Studies Centre (BISC)	Willebroek
8 février 2019	Le droit du renseignement	Académie du renseignement	Paris
5 mars 2019	Réunion constitutive de l'Intelligence Network Europe (INE)	Gouvernement français	Paris
7-8 mars 2019	Oversight on intelligence services		Bruxelles
29-30 mars 2019	Bonne gouvernance dans le domaine de la sécurité	Democratic Centre for Armed Forces (DCAF) / MinInt Tunisie	Tunis
2 avril 2019	'22ème congrès sur le secteur public : le fonctionnaire numérique'	4Instance	Bruxelles
25 avril 2019	European Defence – the capability issue	Institut royal supérieur de défense	Bruxelles

206 Ceci a donné lieu à un 'rapport de suivi' en 2020 : COUR DES COMPTES, *Institutions à dotation. Suivi des recommandations formulées en 2018*, 57 p.

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

208 Protocole de coopération entre le Comité permanent de Contrôle des services de renseignement et de sécurité et l'Institut de Formation judiciaire, 4 avril 2019.

DATE	TITRE	ORGANISATION	LIEU
14 juin 2019	Données et études du terrorisme en Belgique – Regards croisés entre praticiens et chercheurs	Institut Egmont et Organe de coordination pour l'analyse de la menace (OCAM)	Bruxelles
31 juillet 2019	Visite de travail	Coordination nationale du renseignement et de la lutte contre le terrorisme, Unité de coordination de la lutte anti-terroriste, Service national du renseignement pénitentiaire	Paris
13 septembre 2019	De politionele omgang met geesteszieken en suïcidalen	Comité permanent P	Bruxelles
8-9 octobre 2019	International Intelligence Oversight Forum (IIOF 2019)	UN-High Commissioner for Human Rights	Londres
2-3 décembre 2019	Visite de travail	MI5	Londres
12-13 décembre 2019	European Intelligence Oversight Conference 2019	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD)	La Haye

Par ailleurs, des briefings ont été très régulièrement organisés au Comité. Des experts sont ainsi venus développer des thématiques d'actualité qui sont importantes pour la communauté du renseignement (par ex. les relations entre les services de renseignement et la Direction générale de la police judiciaire (le Directeur général Éric Snoeck), la vision stratégique pour la Défense belge (le CHOD Marc Compernol), la création de *Joint Intelligence Centers* et de *Joint Decision Centers*[209] (le Procureur général Johan Delmulle), etc. Ces briefings doivent promouvoir, d'une part, une discussion approfondie sur le fonctionnement, les compétences et le contrôle des services de renseignement et de sécurité et de l'OCAM et, d'autre part, promouvoir le travail de renseignement.

[209] Un *Joint Intelligence Centre* (JIC) doit permettre une concertation hebdomadaire aux services concernés (les deux services de renseignement, l'OCAM et la Police judiciaire fédérale) sur de nouvelles informations opérationnelles, les priorités et la répartition des tâches. Le *Joint Decision Center* (composé des services précités et du Parquet fédéral) décide, sur la base d'une conception commune du JIC, quel service est chargé de poursuivre l'enquête. Ainsi, la séparation (stricte) entre la police, les services de renseignement et la justice est dès lors abandonnée et remplacée par une approche circulaire et collégiale. Voir *Doc. parl.,* Chambre, 2017-18, n° 54-1752/008, 58.

CHAPITRE XI
RECOMMANDATIONS

À la lumière des enquêtes de contrôle, des contrôles et des inspections clôturés en 2019, le Comité permanent R formule les recommandations reprises ci-après, parfois conjointement à l'Organe de contrôle de l'information policière. Ces recommandations portent à la fois sur la protection des droits que la Constitution et la loi confèrent aux personnes, sur la coordination et l'efficacité des services de renseignement, de l'OCAM et des services d'appui et sur l'optimalisation des possibilités d'enquête du Comité permanent R.

XI.1. RECOMMANDATION RELATIVE À LA PROTECTION DES DROITS QUE LA CONSTITUTION ET LA LOI CONFÈRENT AUX PERSONNES

XI.1.1. LA PUBLICATION D'UN ARRÊTÉ ROYAL SUR LES INTERCEPTIONS

L'article 44 L.R&S stipule que le Comité, *'sans préjudice des autres compétences attribuées à ce Comité par la loi du 18 juillet 1991, a le droit de faire cesser des interceptions, intrusions ou prises d'images en cours lorsqu'il apparaît que celles-ci ne respectent pas les dispositions légales ou l'autorisation [ministérielle]. Il ordonne l'interdiction d'exploiter les données recueillies illégalement et leur distribution, selon les modalités à fixer par le Roi.'* L'article 44/5 L.R&S nécessite également un arrêté d'exécution. De tels Arrêtés royaux n'ont cependant pas encore été pris. Le Comité permanent R insiste (une nouvelle fois) pour qu'ils le soient dans les meilleurs délais.

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. DIVERSES RECOMMANDATIONS CONCERNANT L'ENQUÊTE DE CONTRÔLE SUR LES SCREENINGS DE SÉCURITÉ[210]

XI.2.1.1. Une législation cohérente et simplifiée en matière de screening

La législation en matière de screening présente une certaine complexité et une certaine diversité. Le Comité permanent R recommande que le législateur simplifie cette législation et la rende plus cohérente. En outre, le contenu et la finalité de chaque screening doivent être décrits. Le législateur doit également déterminer dans quels cas une enquête de renseignement complémentaire doit être autorisée. Il est aussi indiqué que le législateur précise dans quelles circonstances les services de renseignement peuvent collecter des informations complémentaires concernant la personne qui fait l'objet d'une vérification. Cette collecte d'informations peut s'avérer nécessaire pour, par exemple, actualiser ou contextualiser des données existantes.

XI.2.1.2. Accords avec les autorités qui reçoivent les décisions de l'instance de recours

Le Comité permanent R recommande que les deux services de renseignement concluent les accords requis avec les autorités qui reçoivent les décisions de l'instance de recours en matière de screening de sécurité. De tels accords permettraient aux deux services de prendre connaissance de ces décisions. Ils pourraient ainsi analyser la jurisprudence et en tenir compte dans le cadre des futurs screenings.

XI.2.1.3. Concertation sur la finalité du screening

Le Comité permanent R recommande que la VSSE et le SGRS se concertent régulièrement avec les différentes autorités/les différents clients qui reçoivent leurs avis de sécurité ou leurs renseignements, et ce afin de s'assurer que les renseignements transmis répondent à la finalité du screening demandé.[211]

---

210 Voir Chapitre I.1. ('La réalisation de screenings de sécurité par les services de renseignement').

211 Quelles informations sont nécessaires et doivent être communiquées à l'autorité requérante ? Dans le cadre de quel type de vérification ou de screening ? (par ex. l'interprétation de la notion d'*'empêchement résultant de faits personnels graves'* dans le cadre d'une procédure de naturalisation).

XI.2.1.4. Questionnement systématique des services partenaires étrangers

Le Comité permanent R recommande de prévoir les moyens (en personnel) et les procédures nécessaires, en particulier pour permettre de questionner de manière systématique les services partenaires étrangers si le screening de sécurité concerne une personne qui a séjourné pendant une longue période à l'étranger.[212]

XI.2.1.5. La mise en place d'un système d'enregistrement et de consultation

Le Comité permanent R recommande que la VSSE et le SGRS créent un système d'enregistrement et de consultation des dossiers. Il s'agit plus précisément d'une '*consultation list*' dans laquelle sont mentionnés les dossiers qui ont été examinés par les services. Ceci doit permettre d'enregistrer de manière systématique et centralisée tous les mouvements internes dans un dossier. Il est tout aussi important de parvenir à une gestion centralisée de toutes les réponses qui sont transmises par le service (par ex. par les services d'analyse) à l'autorité/au client concerné(e). Ceci est nécessaire pour s'assurer du respect d'éventuels délais de réponse et de la cohérence dans la manière de communiquer avec les partenaires. Il est également indiqué de conserver et de classer toutes les pièces d'un dossier d'origine constitué dans le cadre d'un screening. L'exécution d'un contrôle (de qualité) en dépend.

XI.2.1.6. Une composition uniforme des dossiers comme objectif

La manière dont la VSSE et le SGRS traitent les dossiers dans le cadre des screenings dépend aussi de facteurs externes. Un de ces facteurs est la manière dont les autorités/les clients transmettent les dossiers à traiter aux services. Leur composition diverse (numérique) et les éventuelles imprécisions peuvent influencer/compliquer le traitement. Par conséquent, le Comité permanent R recommande de composer les dossiers de manière uniforme, et même pour la demande et le traitement des screenings, de procéder à une intégration des systèmes ICT dans les différents services. La création d'une plateforme commune, comme c'est déjà le cas par exemple pour les demandes d'habilitations de sécurité, est également recommandée.

XI.2.1.7. L'instauration d'un système de contrôle interne

Le Comité permanent R recommande à la VSSE et au SGRS d'instaurer un système de contrôle interne, entre autres, en déterminant des indicateurs de prestation et de gestion. Ils doivent prévoir un échantillon suffisamment large et systématique pour contrôler et maintenir la qualité des vérifications.

---

212 L'alternative est la conclusion d'accords clairs entre, d'une part, la VSSE et le SGRS, et d'autre part, l'ANS, pour permettre à cette autorité de questionner les services étrangers.

XI.2.1.8. Une automatisation poussée des demandes

Le Comité permanent R recommande également une automatisation poussée des demandes de vérification. L'idéal serait de développer un outil IT permettant d'effectuer un contrôle automatique des noms repris dans une banque de données.

XI.2.1.9. L'élaboration d'un vademecum

Le Comité permanent R recommande que tant la VSSE que le SGRS élaborent un vademecum décrivant la procédure interne, en ce compris le flux d'informations et la méthodologie, pour la réalisation des vérifications de sécurité et des screenings.

XI.2.1.10. Une meilleure intégration du Service Vérifications de Sécurité dans le système de gestion de l'information de la VSSE

Le Comité permanent R recommande une meilleure intégration du Service Vérifications de Sécurité dans le système de gestion de l'information de la VSSE. Les documents rédigés par ce service doivent pouvoir être consultés par d'autres départements. De plus, il convient de créer un mécanisme pour que les incomplétudes observées par le Service VVS dans la banque de données de la VSSE soient signalées et corrigées. Il est essentiel de développer un système *'flagging'* dans la banque de données. En vertu de ce système, toutes les personnes figurant dans la banque de données et qui font ou ont fait l'objet d'une vérification de sécurité sont mentionnées en tant que telles. Cela permettrait à tous les départements de le constater. En outre, de nouvelles informations pertinentes concernant la personne en question pourraient être ajoutées, après quoi un nouvel avis de sécurité pourrait être transmis, si nécessaire, à l'autorité concernée.

XI.2.1.11. Encadrement de la mission en matière de screening de sécurité au SGRS

Le Comité permanent R estime que la mission en matière de vérification de sécurité et de screening est délaissée par le SGRS et n'est pas encadrée convenablement par la hiérarchie. Il y a lieu de définir une ligne hiérarchique claire et de désigner la personne responsable en dernier ressort.[213]

XI.2.1.12. Vérifications dans toutes les banques de données du SGRS

Le Comité permanent R recommande qu'au SGRS, la Cellule Screenings puisse effectuer des vérifications dans toutes les banques de données du service.

[213] La solution envisagée par le SGRS à ce propos est d'intégrer la Cellule Screenings dans le nouvel organe de coordination DISCC. Mais cela suffira-il à résoudre le problème de l'ambiguïté entourant la responsabilité hiérarchique ? Pour le Comité, le fait que la Cellule Screenings opère indépendamment de la Direction S constitue un problème.

En outre, le SGRS doit prendre les mesures appropriées pour s'assurer que toutes les banques de données utilisées en son sein sont suffisamment alimentées en informations pertinentes et qu'elles le sont en temps utile.

XI.2.1.13. Enregistrement des données chiffrées relatives aux screenings de sécurité effectués

Le Comité permanent R recommande au SGRS d'œuvrer à court terme à la gestion des données chiffrées concernant le nombre de vérifications de sécurité effectuées et à effectuer, et ce afin de pouvoir procéder à une évaluation régulière de la charge de travail et de la possibilité de respecter les délais de réponse. Des tendances pourraient ainsi être dégagées, ce qui permettrait d'anticiper une augmentation du nombre de demandes, et le cas échéant, d'affecter des moyens (en personnel) supplémentaires. Ces données chiffrées seraient de préférence groupées selon le type de vérification (base légale).

XI.2.2. RECOMMANDATIONS CONCERNANT L'ENQUÊTE DE CONTRÔLE SUR CARLES PUIGDEMONT[214]

XI.2.2.1. Une adaptation de la directive en matière de coopération internationale

En ce qui concerne la collaboration avec des services étrangers, le Comité recommande d'adapter et de compléter la directive du Conseil national de sécurité. Cette directive devrait préciser le contenu des renseignements échangés avec les services étrangers et devrait tenir compte du Titre 3 de la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Celui-ci prévoit des dispositions particulières en vue du traitement de données à caractère personnel par les services de renseignement et de sécurité, et notamment des modalités particulières en fonction du caractère européen ou non du service étranger.

XI.2.2.2. La conclusion d'un accord de coopération entre le SGRS et la VSSE

En ce qui concerne la répartition des tâches visant à rechercher, analyser et traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge, le Comité permanent R recommande l'adoption

214 Voir Chapitre I.5. ('Carles Puigdemont et les éventuelles activités menées par des services de renseignement étrangers en Belgique').

de directives par le Conseil national de sécurité, ainsi que la conclusion d'un accord de coopération entre la VSSE et le SGRS, en exécution de l'article 20, § 4, L.R&S.

XI.2.2.3. L'établissement d'une liste des services de renseignement et de sécurité étrangers

En ce qui concerne la nature des services étrangers, le Comité permanent R recommande que la VSSE et le SGRS dressent une liste des services étrangers pouvant être qualifiés de "services de renseignement et de sécurité", et ce par analogie avec la recommandation émise dans le cadre de l'enquête sur les contacts internationaux de l'OCAM.[215]

XI.2.2.4. L'élaboration d'une méthodologie commune en matière d'analyse de la menace

En ce qui concerne l'évaluation de la menace, le Comité permanent R recommande à la VSSE et au SGRS d'adopter une méthodologie commune, inspirée de la méthodologie de la VSSE permettant de décider des mesures à prendre, après une évaluation du risque, en termes de crédibilité, de possibilités d'action et de proportionnalité. Une telle méthodologie doit également permettre, notamment :
- d'assurer la traçabilité des documents et des décisions en vue de garantir *a posteriori* un contrôle effectif par le Comité permanent R ;
- de s'assurer que le service de renseignement communique ses décisions et les mesures qu'il a prises au ministre compétent.

XI.2.3. RECOMMANDATIONS CONCERNANT L'ENQUÊTE DE CONTRÔLE SUR LE FONCTIONNEMENT DE LA SECTION HUMINT DU SGRS[216]

XI.2.3.1. Recommandations pour la gestion et la planification des activités de renseignement

Le Comité permanent R recommande :
- d'indiquer, dans les différents plans du SGRS, les motifs pour lesquels les pays ou les thématiques sont repris à un niveau de priorité donné, en faisant explicitement référence aux intérêts nationaux et internationaux ;

---

215 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 106-108.

216 Voir Chapitre I.2. ('Analyse du fonctionnement de la Section HUMINT du service de renseignement militaire').

- d'uniformiser l'utilisation des différents documents de gestion, les Plans Directeur du Renseignement, les *IntelFocus* et les *Intelligence Collection Plans*. Il y a lieu, le cas échéant, de motiver explicitement les éventuelles divergences constatées entre ces documents de gestion (par ex. pourquoi des pays qui sont considérés comme prioritaires dans un plan ne le sont pas dans un autre) ;
- de veiller à ce que les *Intelligence Collection Plans* (ICP) au sein de la Direction Intelligence du SGRS présentent une structure fixe et uniforme pour tous les services de collecte (donc, y compris I/H) et soient continuellement actualisés ;
- de dresser un inventaire de l'utilisation des ressources de ses divers services de collecte en vue d'identifier d'éventuelles lacunes, de même que les menaces ou priorités qui concentrent particulièrement l'attention et les moyens. Cet aperçu permettrait *in fine* d'optimaliser et de rendre complémentaires les services de collecte ;
- que le SGRS procède à une évaluation (ponctuelle, permanente ou périodique, en fonction de la situation) des sources afin de vérifier si l'utilisation de celles-ci correspond aux priorités ;
- que SGRS s'assure de la coordination et, le cas échéant, de la gestion mutuelle des sources humaines de ses différents organes de collecte, dont la Section I/H. À cet égard, le Comité permanent R recommande également de trier les sources existantes afin de dégager des capacités et de recruter de nouvelles sources en vue d'assurer de cette manière un certain mouvement/ renouvellement ;
- de s'assurer du suivi, de l'évaluation et de la mise à jour des différents documents de gestion, du Plan Directeur du Renseignement, de l'*IntelFocus* et des *Intelligence Collection du Plans*.

XI.2.3.2. Recommandations sur les moyens de la Section I/H

Une fois que la gestion et la planification des activités de renseignement de la Section I/H ont été définis (en complément d'autres services de collecte du SGRS), des moyens doivent être alloués. En ce qui concerne l'organigramme et l'affectation du personnel, le Comité permanent R a constaté plusieurs problèmes desquels le SGRS doit informer le ministre de la Défense afin que des investissements soient réalisés. Dès lors, le Comité :

- recommande de réaliser une analyse des besoins réels en personnel[217], d'établir un tableau organique axé sur l'avenir et de mettre à niveau les

[217] En tenant compte, entre autres, du nombre de sources que peut gérer un officier traitant et de l'appui qui lui est nécessaire. Ceci requiert une collaboration avec des spécialistes en 'Personnel et Organisation' de la Défense et un '*benchmarking*' auprès d'autres services investis des mêmes missions.

effectifs du service en se basant sur les besoins réels d'un service de gestion de sources humaines œuvrant dans le cadre de missions telles que celles du SGRS ;
- recommande de limiter la rotation du personnel de la Défense au sein de la Section I/H ;
- rappelle également que le développement d'une nouvelle branche 'renseignements' à la Défense ou l'élaboration de solutions alternatives peut/peuvent contribuer à attirer du personnel expert en renseignement et à développer leur carrière. Le Comité se réfère à ses recommandations précédentes.[218]

XI.2.3.3. Recommandations pour la gestion des sources et pour les procédures

Une fois que la gestion et la planification des activités de renseignement ainsi que les moyens ont été mobilisés pour les concrétiser, il convient d'élaborer des processus et des procédures de travail. Le Comité permanent R soulignait que le recours à des sources humaines pour la collecte de données (cf. article 18 de la L. R&S) nécessitait des directives du Conseil national de sécurité.

Le Comité permanent R a constaté que, malgré l'absence, à ce moment-là, de directive du Conseil national de sécurité, la majorité des directives internes (SOP) de la Section I/H ont été actualisées en 2018. Le Comité recommande néanmoins :
- que la Section I/H poursuive ses efforts en matière d'évaluation des sources et des bulletins d'information. À propos de ces derniers, I/H et les services d'analyse doivent établir un planning commun en vue d'atteindre ensemble cet objectif[219] ;
- de mettre en œuvre un processus de contrôle interne en vue de maintenir une attention constante sur le respect des procédures, en particulier les procédure mises en place au sein de la Section I/H[220] ;
- de reprendre les différentes directives (SOP) dans un vademecum classifié à l'attention du personnel.

---

218 Voir COMITÉ PERMANENT R, *Rapport d'activités 2011*, p. 12 et 106, *Rapport d'activités 2018*, p. 135, Recommandations concernant la gestion du personnel et des carrières, la formation et l'entraînement.

219 L'évaluation de la source incombe à la Section I/H elle-même, tout en sachant qu'elle est à son tour dépendante de l'évaluation des bulletins d'information et du feedback des services d'analyse à qui les informations sont *in fine* destinées. La réorganisation du SGRS, début 2020, devrait impliquer le rassemblement de tous les services de collecte du SGRS dans un pilier et les services d'analyse dans un autre, alors que dans la situation actuelle ces services sont mélangés. Cette réorganisation pourrait être mise à profit pour planifier l'objectif précité. Mais l'approche doit être réaliste, en ce sens qu'il faut tenir compte des moyens disponibles.

220 Le Comité permanent R reconnaît que cette recommandation, à défaut d'être mesurable, peut sembler irréaliste.

XI.2.4. RECOMMANDATIONS CONCERNANT LES BANQUES DE DONNÉES COMMUNES

XI.2.4.1. Évaluation des conflits d'intérêts et de l'emploi du temps du délégué à la protection des données

Compte tenu de la multitude de fonctions assumées par le délégué à la protection des données de la BDC TF et PH, il est important qu'en vue d'un prochain contrôle du C.O.C. et du Comité permanent R, une évaluation claire de tout conflit d'intérêts soit réalisée. Il importe tout autant que soit évalué le temps consacré aux tâches qui incombent au délégué à la protection des données de la banque de données commune.

XI.2.4.2. Attention pour le principe de 'need to know'

Compte tenu de l'accroissement imminent du nombre de services partenaires qui auront un accès direct à la BDC TF et PH, il est important que le DPO de la BDC TF et PH surveille étroitement la mesure dans laquelle la banque de données est alimentée par les différents services partenaires et dans quelle mesure un tel chevauchement viole le principe du '*need to know*'. Il doit y avoir une 'nécessité' pour les services habilités à accéder directement ou indirectement à la BDC TF et PH lorsqu'ils prennent des décisions qui relèvent de leurs compétences. Dans ce contexte, il faut souligner qu'un service partenaire (à l'exception du Ministère public) doit faire les efforts nécessaires pour alimenter la banque de données. Le but ne peut en aucun cas être de fournir un accès direct avec des droits d'écriture pour s'assurer qu'un des services disposant d'un droit introduise les informations pertinentes dans la BDC TF et PH.

XI.2.4.3. Démarche en cas d'incident de sécurité

La procédure standard en cas d'incident de sécurité doit être suffisamment communiquée aux services concernés, afin qu'ils connaissent son existence et qu'ils se familiarisent avec son fonctionnement. En outre, le C.O.C. et le Comité permanent R doivent être informés (plus rapidement) de la survenance de tels incidents et doivent être (plus étroitement) impliqués. Tous les services concernés doivent effectuer plus systématiquement tant les 'petits' loggings que les 'grands' loggings. Le gestionnaire opérationnel occupe une position clé à cet égard.

XI.2.4.4. Protocoles en matière de transmission des listes de diffusion

Le responsable opérationnel de la banque de données commune, ainsi que le délégué à la protection des données, doivent veiller à ce que les listes de diffusion à des instances tierces en vertu de l'article 44/11/3*quater* LFP puissent s'appuyer

sur des protocoles réglant les conditions de ces diffusions. L'interdiction pour ces instances tierces de rediffuser ces données doit figurer dans ces protocoles, dont l'élaboration fera l'objet d'un suivi dans un prochain rapport.

XI.2.4.5. Évaluation de l'accès direct pour les services partenaires

En ce qui concerne les services partenaires qui n'ont pas désigné d'utilisateur pour la BDC TF et PH ni établi de connexion depuis plusieurs années, le C.O.C. et le Comité permanent R signalent une éventuelle absence de 'besoin d'en connaître' ('*need to know*').

Il conviendra à l'avenir d'évaluer dans quelle mesure les conditions de l'article 44/11/3*ter* § 2 LFP sont toujours remplies. Après évaluation, une révision de l'accès direct ou indirect à certains services partenaires pourrait s'imposer.

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

XI.3.1. INFORMATIONS PRÉCISES SUR LE FONCTIONNEMENT DES BANQUES DE DONNÉES COMMUNES

Le C.O.C. et le Comité permanent R doivent être informés plus étroitement des décisions impactant la politique menée, des concertations entre les services concernés, des rapports (annuels) et des rapports de réunion portant sur (le fonctionnement de) la BDC TF et PH.

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 2019 AU 31 DÉCEMBRE 2019)

Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *M.B.* 3 mai 2019

Loi du 2 mai 2019 modifiant diverses dispositions relatives au traitement des données des passagers, *M.B.* 24 mai 2019

Loi du 9 mai 2019 modifiant la loi du 2 octobre 2017 réglementant la sécurité privée et particulière en ce qui concerne le traitement des données personnelles, *M.B.* 5 juin 2019

Loi du 3 juillet 2019 portant modification de la loi du 21 décembre 2013 portant le Code consulaire et de la loi du 10 février 2015 relative aux traitements automatisés de données à caractère personnel nécessaires aux passeports et titres de voyage belges, *M.B.* 22 août 2019

A.R. 17 août 2018 exécutant l'article 2, premier alinéa, 2°, g) de la loi du 10 juillet 2006 relative à l'analyse de la menace – addendum, *M.B.* 10 janvier 2019

A.R. 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attritions de certaines autorités, *M.B.* 18 janvier 2019

A.R. 31 janvier 2019 modifiant l'arrêté royal du 2 juin 2015 portant création du Comité stratégique et du Comité de coordination du renseignement et de la sécurité, *M.B.*11 février 2019

A.R. 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant les obligations pour les transporteurs HST et les distributeurs de tickets HST, *M.B.* 12 février 2019

A.R. 3 février 2019 relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant les obligations pour les transporteurs par bus, *M.B.* 12 février 2019

A.R. 26 avril 2019 portant répartition partielle, pour ce qui concerne la lutte contre le terrorisme et le radicalisme, du crédit provisionnel inscrit au programme 06-90-1 de la loi du 27 mars 2019 ouvrant des crédits provisoires pour les mois d'avril, mai, juin et juillet 2019 et destiné à couvrir les dépenses concernant le renforcement des mesures prises ainsi que des initiatives nouvelles en matière de lutte contre le terrorisme et le radicalisme, *M.B.* 6 mai 2019

A.R. 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, *M.B.* 18 juillet 2019

A.R. 16 juillet 2019 modifiant l'arrêté royal du 26 juin 2002 relatif à la détention et au port d'armes par les services de l'autorité ou de la force publique, *M.B.* 2 août 2019

A.R. 1er octobre 2019 modifiant divers arrêtés royaux portant exécution de la loi sur les armes, *M.B.* 9 octobre 2019

A.R. 2 octobre 2019 modifiant l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, *M.B.* 4 novembre 2019

Sélection comparative francophone d'accession au niveau A (3ème série) pour la Sûreté de l'État : Attachés analystes (m/f/x) – numéro de sélection : BFG19005, *M.B.* 25 février 2019

Sélection comparative francophone d'accession au niveau C (épreuve particulière) pour la Sûreté de l'État : Assistants desécurité(m/f/x). – Numéro de sélection : BFG19006, *M.B.* 25 février 2019

Résultat de l'épreuve préalable de la sélection comparative d'inspecteurs pour les services extérieurs (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État – numéro de sélection : ANG18253, *M.B.* 5 mars 2019

Résultat de la sélection comparative d'experts recrutement et sélection (m/f/x) (niveau B), francophones, pour la Sûreté de l'État – numéro de sélection : AFG18285, *M.B.* 5 mars 2019

Résultat de la sélection comparative de l'épreuve préalable en vue de la constitution d'une réserve d'inspecteurs pour la Sûreté de l'État (m/f/x) (niveau B), francophones, pour la Sûreté de l'État – numéro de sélection : AFG18249, *M.B.* 6 mars 2019

Avis prescrit par l'article 74 de la loi spéciale du 6 janvier 1989, par requête adressée à la Cour par lettre recommandée à la poste le 13 mars 2019 et parvenue au greffe le 14 mars 2019, un recours en annulation de l'article 5 de la loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme (publiée au Moniteur belge du 14 septembre 2018) a été introduit par l'ASBL "TCC-Accueil, ASBL", l'ASBL "AtMOsphères", l'ASBL "Bureau d'Accueil et de Défense des Jeunes", l'ASBL "Coordination des Organisations non gouvernementales pour les droits de l'enfant", l'ASBL "Dynamo international", l'ASBL "Dynamo", l'ASBL "Fédération Laïque de l'Aide à la Jeunesse", l'ASBL "Kinderrechtencoalitie Vlaanderen", l'ASBL "Ligue des droits humains", l'ASBL "Samarcande" et l'ASBL "Uit de marge/CMGJ". Cette affaire est inscrite sous le numéro 7141 du rôle de la Cour, *M.B.* 19 avril 2019

Résultat de la sélection comparative de Juristes Service général du renseignement et de la sécurité (m/f/x), (niveau A1), néerlandophones, pour le Ministère de la Défense – numéro de sélection : ANG18305, *M.B.* 7 mai 2019

Extrait de l'arrêt n° 41/2019 du 14 mars 2019, numéro du rôle : 6758, en cause : le recours en annulation des articles 4, 4°, et 5, litterae e), f) et g), deuxième tiret, 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" (nouvel article 2, § 3, article 3, 12°, article 3, 12°/1, et article 3, 14°, litterae a) et b), de la loi précitée du 30 novembre 1998), introduit par l'ASBL "Liga voor Mensenrechten", *M.B.* 8 mai 2019

Personnel – désignation d'un titulaire d'une fonction de management, *M.B.* 21 mai 2019

Règlement du 24 avril 2019 d'ordre intérieur du comité de direction de la Sûreté de l'État, *M.B.* 31 mai 2019

Résultat de la sélection comparative néerlandophone d'accession au niveau C (épreuve particulière) pour la Sûreté de l'État : Assistants de sécurité (m/f/x) – numéro de sélection : BNG19005, *M.B.* 11 juin 2019

Résultat de la sélection comparative francophone d'accession au niveau C (épreuve particulière) pour la Sûreté de l'État : Assistants de sécurité (m/f/x) – numéro de sélection : BFG19006, *M.B.* 11 juin 2019

Comité permanent de contrôle des services de renseignement et de sécurité – recrutement pour l'entrée en service d'un(e) juriste statutaire néerlandophone (niv. A) et la constitution d'une réserve de recrutement, *M.B.* 13 juin 2019

Comité permanent de contrôle des services de renseignement et de sécurité – recrutement pour l'entrée en service d'un(e) juriste statutaire francophone (niv. A) et la constitution d'une réserve de recrutement, *M.B.* 13 juin 2019

Résultat de la sélection comparative, néerlandophones, d'accession au niveau A (3e série) pour la Sûreté de l'État Attachés Analystes (m/f/x) – numéro de sélection : BNG19004, *M.B.* 19 juillet 2019

Résultat de la sélection comparative, francophone, d'accession au niveau A (3e série) pour la Sûreté de l'État : Attachés analystes (m/f/x) – numéro de sélection : BFG19005, *M.B.* 19 juillet 2019

Sélection comparative d'Ingénieurs du Renseignement et de la Sécurité (m/f/x) (niveau A1), néerlandophones, pour le Ministère de la Défense – numéro de sélection : ANG18292, *M.B.* 2 août 2019

Extrait de l'arrêt n°112/2019 du 18 juillet 2019, numéros du rôle : 6749 et 6755, en cause : les recours en annulation totale ou partielle de la loi du 24 février 2017 modifiant la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers afin de renforcer laprotection de l'ordre public et de la sécurité nationale, introduits par l'Ordre des barreaux francophones et germanophone et par l'ASBL " Association pour le droit des Étrangers » et autres, *M.B.* 26 août 2019

Sélection comparative de Cyber Security Expert (A2) (m/f/x) (niveau A2), neérlandophones, pour le Ministère de la Défense – numéro de sélection : AFG19115, *M.B.* 2 septembre 2019

Sélection comparative de Cyber Security Expert (A2) (m/f/x) (niveau A2), francophones, pour le Ministère de la Défense – numéro de sélection : AFG19115, *M.B.* 2 septembre 2019

Sélection comparative de spécialistes des réseaux opérationnels (m/f/x) (niveau B), francophones, pour le Ministère de la Défense – numéro de sélection : AFG19118, *M.B.* 9 septembre 2019

Sélection comparative de Senior system engineer (m/f/x) (niveau A2), francophones, pour le Ministère de la Défense – numéro de sélection : AFG19119, *M.B.* 9 septembre 2019

Sélection comparative de psychologues (m/f/x) (niveau A1), néerlandophones, pour la Sûreté de l'État – numéro de sélection : ANG19287, *M.B.* 19 septembre 2019

Résultat de la sélection comparative d'Ingénieurs du Renseignement et de la Sécurité (m/f/x), (niveau A1), néerlandophones pour le Ministère de la Défense – numéro de sélection : ANG18292, *M.B.* 21 octobre 2019

Comité permanent de contrôle des services de renseignement et de sécurité, constitution d'une réserve de recrutement d'un(e) secrétaire francophone statutaire (niv. B), *M.B.* 22 octobre 2019

Comité permanent de contrôle des services de renseignement et de sécurité, recrutement pour l'entrée en service d'un(e) juriste statutaire francophone (niv. A) et la constitution d'une réserve de recrutement, *M.B.* 22 octobre 2019

Règlement de la Chambre des représentants, modifications, *M.B.* 25 octobre 2019

Extrait de l'arrêt n°111/2019 du 18 juillet 2019, numéros du rôle : 6733, 6750 et 6753, en cause : les recours en annulation totale ou partielle de la loi du 15 mars 2017 modifiant l'article 39/79 de la loi du 15 décembre 1980 sur l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers, introduits par l'ASBL "Liga voor Mensenrechten" et l'ASBL "Ligue des Droits de l'Homme", par l'Ordre des barreaux francophones et germanophone et par l'ASBL "Association pour le droit des Étrangers" et autres, *M.B.*8 novembre 2019

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 2019 AU 31 DÉCEMBRE 2019)

Sénat

Conférence interparlementaire sur la politique étrangère et de sécurité commune (PESC) et sur la politique de sécurité et de défense commune (PSDC), Helsinki, 4-6 septembre 2019, *Doc. parl.*, Sénat, 2019, nº 7-10/1

Chambre des représentants

La problématique de la délivrance des visas humanitaires – audition de : F. Roosemont, directeur général de l'Office des étrangers ; D. Van den Bulck, commissaire général aux Réfugiés et aux Apatrides ; François De Smet, directeur, A. Declercq et I. Vandenberghe, collaboratrices auprès de Myria, *C.R.I.*, Chambre, 2018-2019, 29 janvier 2019, COM 1021, p. 1

La problématique de la délivrance des visas humanitaires – audition de : J. De Volder et P. Wieërs, représentants de Sant'Egidio ; M. Geleyn, ex-directeur général du SPF Affaires étrangères ; J.-F. Parmentier, consul belge à Beyrouth, *C.R.I.*, Chambre, 2018-2019, 5 février 2019, COM 1027, p. 1

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du président et des premier et du second présidents suppléants – candidatures introduites, *C.R.I.*, Chambre, 2018-2019, 7 février 2019, PLEN 269, p. 56

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du premier et du second président suppléant, *C.R.I.*, Chambre, 2018-2019, 28 février 2019, PLEN 273, p. 29

Proposition de résolution concernant l'évolution et la modernisation du cadre de réserve des forces armées, *Doc. parl.*, Chambre, 2018-2019, nos 54-2683/6, 54-2683/9 à 54-2683/11

Projet de loi établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, *Doc. parl.*, Chambre, 2018-2019, nos 54-3340/3 et 54-3340/4

Rapport d'activités 2017 du Comité permanent de contrôle des services de renseignement et de sécurité, *Doc. parl.*, Chambre, 2018-2019, no 54-3375/1

Le rapport de la commission d'enquête de l'assemblée nationale de la République française sur "la sûreté et la sécurité des Installations nucléaires" et les centrales nucléaires belges : analyse de l'AFCN, *Doc. parl.*, Chambre, 2018-2019, no 54-3479/1

Proposition de loi portant des dispositions diverses en matière pénale et en matière de cultes, *Doc. parl.*, Chambre, 2018-2019, nos 54-3515/1 à 54-3515/3, 54-3515/5 à 54-3515/11 et 54-3515/14

Proposition de loi portant dispositions diverses en matière d'informatisation de la justice et de modernisation du statut des juges consulaires, *Doc. parl.*, Chambre, 2018-2019, no 54-3549/1

Proposition de loi portant modification de la loi du 21 décembre 2013 portant le Code consulaire et de la loi du 10 février 2015 relative aux traitements automatisés de données à caractère personnel nécessaires aux passeports et titres de voyage belges (3574/1-3), *Doc. parl.*, Chambre, 2018-2019, no 54-3574/1 et *C.R.I.*, Chambre, 2018-2019, 28 mars 2019, PLEN 278, p. 4

Proposition de loi portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *Doc. parl.*, Chambre, 2018-2019, nos 54-3575/1 à 54-3575/6 et *C.R.I.*, Chambre, 2018-2019, 21 février 2019, PLEN 271, p. 91

La problématique de la délivrance des visas humanitaires – échange de vues avec la ministre des Affaires sociales et de la Santé publique, et de l'Asile et la Migration concernant les résultats de l'enquête administrative, *C.R.I.*, Chambre, 2018-2019, 13 mars 2019, COM 1056, p. 1

Projet de loi modifiant la loi du 2 octobre 2017 réglementant la sécurité privée et particulière en ce qui concerne le traitement des données personnelles, *Doc. parl.*, Chambre, 2018-2019, nos 54-3639/1, 54-3639/2, 54-3639/5 à 54-3639/7

Proposition de résolution visant à favoriser les investissements de la Défense dans l'innovation à double usage, civil et militaire, et à les comptabiliser dans l'objectif de l'OTAN de consacrer 2% du PIB au budget de la Défense, *Doc. parl.*, Chambre, 2018-2019, no 54-3641/1

Projet de loi modifiant la loi du 25 décembre 2016 relatives au traitement des données des passagers, *Doc. parl.*, Chambre, 2018-2019, nos 54-3652/1, 54-3652/3 et 54-3652/4

Proposition portant révision du Règlement de la Chambre des représentants visant à améliorer le suivi des recommandations du Comité P et du Comité R, *Doc. parl.*, Chambre, 2018-2019, nº 54-3654/1

Proposition de loi modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et visant à élargir les conditions de nomination des greffiers du Comité R et du Comité P, *Doc. parl.*, Chambre, 2018-2019, nº 54-3658/1

Proposition de loi modifiant diverses dispositions en ce qui concerne la gestion de l'information policière, *Doc. parl.*, Chambre, 2018-2019, nºs 54-3697/1, 54-3697/3, 54-3697/4 et de 54-3697/6 à 54-3697/8

Élargissement éventuel de la "loi caméras", *Doc. parl.*, Chambre, 2018-2019, nº 54-3727/1

Proposition de résolution visant à la création d'une agence fédérale du renseignement, *Doc. parl.*, Chambre, 2019-2020, nº 55-0287/1

Proposition de résolution visant à instaurer un mécanisme de filtrage des investissements étrangers dans les entreprises opérant dans les secteurs stratégiques, *Doc. parl.*, Chambre, 2019-2020, nº 55-0422/1

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du membre néerlandophone et des premier et second membres suppléants – candidatures introduites, *C.R.I.*, Chambre, 2019-2020, 26 septembre 2019, PLEN 006, p. 43

Proposition de modification de l'article 149 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, 2019-2020, nºs 55-0520/1 à 55-0520/3

La situation sécuritaire des prisons au nord de la Syrie et le sort des Foreign Terrorist Fighters belges suite à l'offensive militaire turque audition – du lieutenant-général Cl.. Van de Voorde, chef du Service général du Renseignement et de la Sécurité (SGRS) ; de P. Van Tigchelt, directeur de l'Organe de coordination pour l'analyse de la menace (OCAM) ; de F. Van Leeuw, procureur fédéral, *C.R.I.*, Chambre, 2019-2020, 16 octobre 2019, COM 032, p. 1

Règlement de la Chambre, *C.R.I.*, Chambre, 2019-2020, 17 octobre 2019, PLEN 009, p. 52

Composition commission suivi Comité permanent P + R, *C.R.I.*, Chambre, 2019-2020, 24 octobre 2019, PLEN 010, p. 2

Proposition de résolution relative à la politique des ressources humaines au sein de la Défense, *Doc. parl.*, Chambre, 2019-2020, nº 55-0567/6

Proposition de résolution relative au rapatriement des enfants des combattants belges en Syrie, *Doc. parl.*, Chambre, 2019-2020, nº 55-0674/1

Suivi des recommandations de la commission d'enquête parlementaire 'Attentats terroristes'. Échange de vues avec le ministre de la Sécurité et de l'Intérieur, chargé du Commerce extérieur, *C.R.I.*, Chambre, 2019-2020, 5 novembre 2019, COM 044, p. 1

Suivi des recommandations de la commission d'enquête parlementaire "Attentats terroristes" réponses du Vice-Premier ministre et ministre de la Justice, chargé de la Régie des Bâtiments, et ministre des Affaires européennes, et du ministre de la Sécurité et de l'Intérieur, chargé du Commerce extérieur, *C.R.I.*, Chambre, 2019-2020, 10 décembre 2019, COM 069, p. 1

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 renseignement et de sécurité, Médiateurs fédéraux, Autorité de protection des données, Commissions de nomination pour le notariat, Commission BIM, Organe de contrôle de l'information policière, Commission fédérale de déontologie, Conseil central de surveillance pénitentiaire – comptes de l'année budgétaire 2018 – ajustements budgétaires de l'année 2019 – propositions budgétaires pour l'année 2020 (867/1-3), *C.R.I.*, Chambre, 2019-2020, 19 décembre 2019, PLEN 018, p. 94

Proposition portant révision du Règlement de la Chambre des représentants visant à améliorer le suivi des recommandations du Comité P et du Comité R, *Doc. parl.*, Chambre, 2019-2020, nº 55-0868/1

Nomination du membre effectif néerlandophone et des premier et second membres suppléants du Comité permanent de contrôle des services de renseignements et de sécurité, *Doc. parl.*, Chambre, 2019-2020, nº 55-0878/1

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 2019 AU 31 DÉCEMBRE 2019)

Sénat

Question écrite de L. Bajart au ministre des Finances sur les 'organisations caritatives religieuses – contrôle plus strict de l'administration fiscale – Pays-Bas – chiffres' (Sénat, 2018-2019, 11 janvier 2019, Q. nº 6-2114)

Question écrite de L. Bajart au ministre de l'Intérieur sur le 'réseau d'aide à des terroristes condamnés – appels à la libération de détenus – contrôle – Sûreté de l'État' (Sénat, 2018-2019, 11 janvier 2019, Q. nº 6-2118)

Question écrite de L. Bajart au ministre de l'Intérieur sur les 'terroristes condamnés – communication via smartphones – présence de GSM dans les prisons – Sûreté de l'État' (Sénat, 2018-2019, 11 janvier 2019, Q. nº 6-2119)

Question écrite de L. Bajart au ministre de l'Intérieur sur le 'réseau d'aide à des terroristes condamnés – rôle possible d'incubateur de terroristes – droit de visite dans les prisons – Sûreté de l'État' (Sénat, 2018-2019, 14 janvier 2019, Q. nº 6-2124)

Question écrite de L. Bajart au ministre de l'Intérieur sur les 'enfants de combattants pour la Syrie belges – endoctrinement par l'EIIS – traumatismes – risques pour notre société' (Sénat, 2018-2019, 14 janvier 2019, Q. nº 6-2130)

Question écrite de L. Bajart au ministre de l'Intérieur sur les 'djihadistes mineurs – enfants soldats – risques pour notre société – confirmation d'une présence détectée au sein des demandeurs d'asile dans notre pays' (Sénat, 2018-2019, 14 janvier 2019, Q. nº 6-2138)

Question écrite de L. Bajart au ministre de l'Intérieur sur les 'associations caritatives religieuses – dons provenant des États du golfe – Pays-Bas – chiffres' (Sénat, 2018-2019, 14 janvier 2019, Q. nº 6-2140)

Question écrite de L. Bajart au ministre de l'Intérieur sur la 'Sûreté de l'État (VSSE) – services partenaires étrangers – demande d'identification téléphonique – délai de réponse – terrorisme' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2174)

Question écrite de L. Bajart au ministre de l'Intérieur sur le 'Service Général du Renseignement et de la Sécurité (SGRS) – opération "Vigilant Guardian" – attentat de Paris – deux rapports sur la présence d'un coauteur à Zaventem – transfert d'informations entre les services' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2176)

Question écrite de L. Bajart au ministre des Affaires étrangères sur le 'Service général du renseignement et de la sécurité (SGRS) – opération "Vigilant Guardian" – attentat de Paris – deux rapports sur la présence d'un coauteur à Zaventem – transfert d'informations entre les services' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2177)

Question écrite de L. Bajart au ministre de l'Intérieur sur le 'Service général du renseignement et de la sécurité (SGRS) – "Force protection" – opération "Vigilant Guardian" (OVG) – transmission et réception de l'information' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2178)

Question écrite de L. Bajart au ministre des Affaires étrangères sur le 'Service Général du Renseignement et de la Sécurité (SGRS) – "Force protection" – opération "Vigilant Guardian" (OVG) – transmission et réception de l'information' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2179)

Question écrite de L. Bajart au ministre de l'Intérieur sur le 'Service général du renseignement et de la sécurité (SGRS) – présence de M. Abaaoud dans la région de Bruxelles en 2015 – circulation de l'information entre les services' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2180)

Question écrite de L. Bajart au ministre des Affaires étrangères sur le 'Service général du renseignement et de la sécurité (SGRS) – présence de M. Abaaoud dans la région de Bruxelles en 2015 – circulation de l'information entre les services' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2181)

Question écrite de L. Bajart au ministre de l'Intérieur sur le 'Service général du renseignement et de la sécurité (SGRS) – opération "Vigilant Guardian" – suspect filmant le dispositif de sécurité à Zaventem en novembre 2015 – signalement – circulation de l'information entre les services' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2182)

Question écrite de L. Bajart au ministre des Affaires étrangères sur le 'Service général du renseignement et de la sécurité (SGRS) – opération "Vigilant Guardian" – suspect filmant le dispositif de sécurité à Zaventem en novembre 2015 – signalement – circulation de l'information entre les services' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2183)

Question écrite de L. Bajart au ministre des Affaires étrangères sur le 'potentiel scientifique et économique (PSE) – protection – relations entre la Sûreté de l'État, les centres de recherche et le secteur privé' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2184)

Question écrite de L. Bajart au ministre de l'Intérieur sur le 'femmes djihadistes – risques pour notre société – retour dans notre pays' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2185)

Question écrite de L. Bajart au ministre des Affaires étrangères sur le 'Sûreté de l'État (VSSE) – Service Général du Renseignement et de la Sécurité (SGRS) – Social Media Intelligence (SOCMINT) – personnel – recrutement – personnel disposant de connaissances linguistiques (arabe) et d'une connaissance des milieux allochtones' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2189)

Question écrite de L. Bajart au ministre de la Justice sur les 'salafistes – menace de violence – Pays-Bas – salafisation de mosquées en difficulté – activités antidémocratiques – propagande – aide financière de la part de pays étrangers – approche belge' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2222)

Question écrite de L. Bajart au ministre de l'Intérieur sur le 'niveau de la menace – changement dans l'évaluation de la menace terroriste – mouvement djihadiste – diffusion du message djihadiste – discours de vengeance – mesures' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2223)

Question écrite de L. Bajart au ministre de la Justice sur le 'niveau de la menace – changement dans l'évaluation de la menace terroriste – mouvement djihadiste – diffusion du message djihadiste – discours de vengeance – mesures' (Sénat, 2018-2019, 15 janvier 2019, Q. nº 6-2224)

Question écrite de P. Van Rompuy au ministre de l'Intérieur sur les 'combattants partis pour la Syrie et rentrés dans notre pays – enquêtes – registre de la population – radiation' (Sénat, 2018-2019, 24 janvier 2019, Q. nº 6-2272)

Question écrite de G. D'haeseleer au ministre de l'Intérieur sur les 'services de sécurité – suicides – nombre' (Sénat, 2019-2020, 29 janvier 2019, Q. nº 6-2314)

Question écrite de B. Anciaux au ministre de la Justice sur les 'radicalisation – lutte – mosquées – reconnaissance – soutien procédure – simplification – mesures – coopération entre l'État fédéral et les Communautés et Régions' (Sénat, 2019-2020, 19 septembre 2019, Q. nº 7-51)

Question écrite de C. Van Cauter au ministre de l'Intérieur sur 'l'extrême droite et extrême gauche – menace de violence – augmentation – indicateurs – nombres de faits de violence – répression – déradicalisation' (Sénat, 2019-2020, 19 septembre 2019, Q. nº 7-64)

Question écrite de W.-F. Schiltz au ministre des Télécommunications sur les 'infox – vidéos hypertruquées – manipulation politique – Sûreté de l'État – médias sociaux' (Sénat, 2019-2020, 14 octobre 2019, Q. nº 7-83)

Question écrite de G. Daems au ministre de l'Intérieur sur les 'services de renseignements – conséquences du Brexit – sécurité terrorisme – mandat d'arrêt européen' (Sénat, 2019-2020, 14 octobre 2019, Q. nº 7-91)

Question écrite de G. D'haeseleer au ministre de l'Intérieur sur 'l'État islamique (EI) – combattants de l'EI – rapatriement d'enfants – suivi' (Sénat, 2019-2020, 25 novembre 2019, Q. nº 7-99)

Question écrite de G. Van Goidsenhoven au ministre de l'Intérieur sur les Cellules de sécurité intégrale locales (CSIL R) – création – évolution – activités – missions – fonctionnement' (Sénat, 2019-2020, 25 novembre 2019, Q. nº 7-160)

Question écrite de P. Van Rompuy au ministre des Télécommunications sur le 'futur réseau 5G – déploiement – cybersécurité – menace potentielle d'Huawei' (Sénat, 2019-2020, 17 décembre 2019, Q. nº 7-246)

Chambre des représentants

Questions jointes d'A. Carcaci et F. Dewinter au ministre de l'Intérieur sur 'les propos antisémites du président de la Ligue des imams de Belgique' (*C.R.I.*, Chambre, 2018-2019, 10 janvier 2019, PLEN 265, p. 43, Q. n^{os} 3326 à 3328)

Question de B. Lutgen au ministre de l'Intérieur sur le 'détachement de la police fédérale vers les polices locales' (*Q.R.*, Chambre, 2018-2019, 4 février 2019, n^{o} 179, p. 38, Q. n^{o} 3385)

Question de P. Buysrogge au ministre de l'Intérieur sur 'les investissements dans les infrastructures de la Sûreté de l'État' (*Q.R.*, Chambre, 2018-2019, 4 février 2019, n^{o} 179, p. 55, Q. n^{o} 3796)

Question de S. Van Hecke au ministre de la Justice sur 'les déclarations de la ministre Schauvliege relatives à la Sûreté de l'État' (*C.R.I.*, Chambre, 2018-2019, 6 février 2019, COM 1028, p. 4, Q. n^{o} 28659)

Questions jointes de S. Van Hecke et G. Dallemagne au ministre de la Justice sur 'la restructuration de la Sûreté de l'État' (*C.R.I.*, Chambre, 2018-2019, 6 février 2019, COM 1028, p. 6, Q. n^{os} 28526 à 28529 et 28658)

Question de K. Metsu au ministre de la Justice sur 'les combattants partis en Syrie' (*C.R.I.*, Chambre, 2018-2019, 20 février 2019, COM 1042, p.1, Q. n^{o} 28862)

Questions jointes et débat d'actualité de R. Hedebouw, M. Van Hees, V. Waterschoot, W. De Vriendt, S. Smeyers, M. De Coninck, G. Dallemagne et J. Fernandez Fernandez au Premier ministre sur 'la problématique de la délivrance des visas humanitaires' (*C.R.I.*, Chambre, 2018-2019, 20 février 2019, COM 1043, p. 12, Q. n^{os} 28366 à 28369, 28394, 28466, 28572, 28851, 28858 et 28864)

Question de S. Smeyers à la ministre des Affaires sociales sur 'la libération imminente et obligatoire d'un ressortissant marocain radicalisé' (*C.R.I.*, Chambre, 2018-2019, 20 février 2019, COM 1043, p. 51, Q. n^{o} 28522)

Questions jointes de F. Dewinter, Ph. Pivin, H. Vuye, C. Van Cauter, H. Bonte et N. Ben Hamou au Premier ministre sur 'le retour possible des djihadistes belges' (*C.R.I.*, Chambre, 2018-2019, 21 février 2019, PLEN 271 p. 3, Q. n^{os} 3437 à 3442)

Question de V. Waterschoot à la ministre de la Justice sur 'l'enquête de l'ONU sur la mort de Dag Hammarskjöld et les archives de la Sûreté de l'État' (*C.R.I.*, Chambre, 2018-2019, 27 février 2019, COM 1046, p. 12, Q. n^{o} 28909)

Question de R. Deseyn au ministre des Finances sur 'l'incidence du Brexit sur les services de douane' (*Q.R.*, Chambre, 2018-2019, 28 février 2019, n^{o} 181, p. 76, Q. n^{o} 2508)

Question de C. Cassart-Mailleux au ministre des Affaires étrangères sur 'l'explosion d'un F-16 à Florennes' (*Q.R.*, Chambre, 2018-2019, 28 février 2019, n^{o} 181, p. 105, Q. n^{o} 1656)

Question de J.-J. Flahaux au ministre de l'Intérieur sur 'l'explosion d'un F-16 à Florennes' (*Q.R.*, Chambre, 2018-2019, 28 février 2019, n^{o} 181, p. 152, Q. n^{o} 3810)

Questions jointes de B. Pas, K. Metsu et J.-J. Flahaux au Premier ministre sur 'la sécurité de Brussels Airport' (*C.R.I.*, Chambre, 2018-2019, 28 février 2019, PLEN 272, p. 34, Q. n^{os} 3474 à 3476)

Questions jointes de W. De Vriendt et P. Buysrogge au ministre des Affaires étrangères sur 'le malaise au sein du service de renseignement militaire' (*C.R.I.*, Chambre, 2018-2019, 13 mars 2019, COM 1053, p. 4, Q. n^{os} 28883 et 29085)

Question d'A. Top au ministre des Affaires étrangères sur 'le fonctionnement du SGRS' (*C.R.I.*, Chambre, 2018-2019, 13 mars 2019, COM 1053, p. 20, Q. nº 29078)

Question de K. Degroote au ministre de la Justice sur 'le fonctionnement des services de renseignement espagnols sur notre territoire' (*C.R.I.*, Chambre, 2018-2019, 13 mars 2019, COM 1055, p. 11, Q. nº 29083)

Question de B. Pas au ministre de l'Intérieur sur 'la banque de données en matière de terrorisme et d'extrémisme' (*Q.R.*, Chambre, 2018-2019, 13 mars 2019, nº 182, p. 224, Q. nº 3792)

Questions jointes de J. Fernandez Fernandez et M. De Coninck au ministre des Affaires sociales sur 'les visas humanitaires' (*C.R.I.*, Chambre, 2018-2019, 20 mars 2019, COM 1062, p. 33, Q. nºs 29124 et 29145)

Question de J. Fernandez Fernandez au ministre des Affaires étrangères sur 'la situation du bataillon ISTAR' (*Q.R.*, Chambre, 2018-2019, 21 mars 2019, nº 183, p. 160, Q. nº 1623)

Question de G. Dallemagne au ministre de la Justice sur les 'mesures de surveillance à l'égard de Monsieur Jean-Louis Denis' (*Q.R.*, Chambre, 2018-2019, 21 mars 2019,
Q. nº 183, p. 248, Q. nº 2977)

Question de K. Degroote au ministre de la Justice sur 'l'utilisation des stands de tir par des criminels selon le service fédéral des armes du SPF Justice' (*Q.R.*, Chambre, 2018-2019, 21 mars 2019, nº 183, p. 252, Q. nº 3012)

Question de C. Van Cauter au ministre de la Justice sur 'la surveillance et l'analyse des messages extrémistes diffusés sur des plateformes numériques' (*Q.R.*, Chambre, 2018-2019, 21 mars 2019, nº 183, p. 260, Q. nº 3066)

Question de C. Van Hecke au ministre de la Mobilité sur 'la délégation de la sécurité aéroportuaire à l'exploitant privé de l'aéroport' (*Q.R.*, Chambre, 2018-2019, 21 mars 2019, nº 183, p. 337, Q. nº 3546)

Questions jointes d'A. Laaouej et H. Bonte au ministre de l'Intérieur sur 'le niveau d'alerte à la suite de l'attentat en Nouvelle-Zélande' (*C.R.I.*, Chambre, 2018-2019, 21 mars 2019, PLEN 276, p. 21, Q. nºs 3506 et 3507)

Questions jointes de S. Van Hecke, S. Becq et V. Van Peel au ministre de la Justice sur 'les abus sexuels au sein des témoins de Jéhovah' (*C.R.I.*, Chambre, 2018-2019, 28 mars 2019, PLEN 277, p. 33, Q. nºs 3530 et 3532)

Question de H. Bonte au ministre de la Justice sur 'le sort des enfants de combattants de l'EI restés en Syrie' (*C.R.I.*, Chambre, 2018-2019, 28 mars 2019, PLEN 277, p. 42, Q. nº 3534)

Question de S. Schlitz au ministre de l'Intérieur sur 'la sécurité des déchets nucléaires stockés à Tihange' (*Q.R.*, Chambre, 2018-2019, 4 avril 2019, nº 184, p. 327, Q. nº 3904)

Question de S. Van Hecke au ministre des Finances sur 'la douane belge et l'affaire de l'isopropanol' (*Q.R.*, Chambre, 2018-2019, 4 avril 2019, nº 184, p. 199, Q. nº 2556)

Question de G. Calomne au ministre de la Justice sur les 'personnes qui n'ont pas de résidence en Belgique – traitement des demandes de port d'armes à feu.' (*Q.R.*, Chambre, 2018-2019, 4 avril 2019, nº 184, p. 337, Q. nº 2142)

Question de K. Jadin au ministre de la Justice sur 'les armes saisies en Belgique' (*Q.R.*, Chambre, 2018-2019, 4 avril 2019, nº 184, p. 343, Q. nº 2517)

Question de F. Dewinter au ministre de la Justice sur le 'financement de mosquées et d'organisations islamistes depuis l'étranger' (*Q.R.*, Chambre, 2018-2019, 4 avril 2019, nº 184, p. 356, Q. nº 2909)

Question de B. Pas au ministre de la Justice sur 'la banque de données en matière de terrorisme et d'extrémisme' (*Q.R.*, Chambre, 2018-2019, 4 avril 2019, nº 184, p. 368, Q. nº 3009)

Question de B. Kir au ministre de l'Intérieur sur 'l'attentat en Nouvelle-Zélande – messages de haine sur Internet' (*Q.R.*, Chambre, 2018-2019, 15 mai 2019, nº 184, p. 236, Q. nº 3951)

Question de B. Pas au ministre de la Justice sur 'l'agrément des mosquées' (*Q.R.*, Chambre, 2018-2019, 22 mai 2019, nº 187, p. 127, Q. nº 2992)

Question de P. Buysrogge au ministre de la Justice sur 'les investissements dans les infrastructures de la Sûreté de l'État' (*Q.R.*, Chambre, 2018-2019, 22 mai 2019, nº 187, p. 131, Q. nº 3044)

Question de K. Ravyts au ministre des Affaires étrangères sur 'la contribution de la Belgique à l'enquête de l'ONU sur la mort de Dag Hammarskjöld' (*Q.R.*, Chambre, 2019-2020, 9 septembre 2019, nº 001, p. 36, Q. nº 2)

Question de S. Rohonyi au VPM Justice sur 'l'évaluation des sections spéciales de déradicalisation (Deradex) dans les prisons' (*C.R.I.*, Chambre, 2019-2020, 18 septembre 2019, COM 012, p. 3, Q. nº 174)

Questions jointes de J. Crombez, K. Bury, K. Van Vaerenbergh et N. Boukili au VPM Justice sur 'l'organisation du procès sur les attentats de Bruxelles' (*C.R.I.*, Chambre, 2019-2020, 18 septembre 2019, COM 012, p. 29, Q. nºs 410, 433, 438 et 496)

Question de S. Van Hecke au VPM Justice sur 'le retrait de la reconnaissance de la mosquée Al Ihsaan à Louvain' (*C.R.I.*, Chambre, 2019-2020, 18 septembre 2019, COM 012, p. 41, Q. nº 480)

Question de N. Boukili au VPM Justice sur 'le timing du classement sans suite d'un dossier visant un ministre' (*C.R.I.*, Chambre, 2019-2020, 2 octobre 2019, COM 20, p. 4, Q. nº 700)

Question de T. Francken au ministre des Affaires étrangères sur 'l'entretien inversé' (*Q.R.*, Chambre, 2019-2020, 2 octobre 2019, nº 003, p. 48, Q. nº 32)

Question de F. Demon au ministre des Affaires étrangères sur les 'contrôles des sociétés privées de gardiennage dans les aéroports' (*Q.R.*, Chambre, 2019-2020, 2 octobre 2019, nº 003, p. 63, Q. nº 20)

Question de D. Senesael au VPM Affaires étrangères sur 'les crimes et délits attribués à l'extrême droite' (*C.R.I.*, Chambre, 2019-2020, 9 octobre 2019, COM 24, p. 24, Q. nº 323)

Question de G. Colebunders au ministre de l'Intérieur sur 'le profilage ethnique au sein de la police' (*C.R.I.*, Chambre, 2019-2020, 9 octobre 2019, COM 24, p. 50, Q. nº 844)

Questions jointes de C. Thibaut et S. Cogolati au ministre de l'Intérieur sur 'l'ambassade du Rwanda et la sécurité du territoire belge' (*C.R.I.*, Chambre, 2019-2020, 16 octobre 2019, COM 034, p. 3, Q. nºs 746, 774 et 775)

Question de K. Jadin au ministre de la Justice sur 'l'arsenal législatif contre l'espionnage' (*Q.R.*, Chambre, 2019-2020, 25 octobre 2019, nº 004, p. 41, Q. nº 10)

Question G. Dallemagne au ministre de l'Intérieur sur la 'tuerie à la préfecture de Paris' (*Q.R.*, Chambre, 2019-2020, 25 octobre 2019, nº 004, p. 179, Q. nº 200)

Questions jointes de T. Francken et K. Verduyckt au ministre des Affaires étrangères sur 'Ia surveillance du camp d'Al-Hol' (*C.R.I.*, Chambre, 2019-2020, 6 novembre 2019, COM 046, p. 24, Q. nºs 381 à 383 et 1365)

Questions jointes d'E. Samyn, W. De Vriendt, Y. Kherbache, K. Jadin, Ch. Lacroix, G. Dallemagne, N. Boukili, J. Soors et P. De Roover au ministre des Affaires

étrangères sur 'l'évolution relative aux combattants de l'EI après le Conseil des affaires étrangères du 14/10/19' (*C.R.I.*, Chambre, 2019-2020, 12 novembre 2019, COM 49, p. 3, Q. nos 933, 973, 976, 1048, 1129, 1148, 1370, 1470,1490, 1501 et 1527)

Question de K. Bury au ministre de la Justice sur 'les activités d'une ASBL musulmane extrémiste' (*Q.R.*, Chambre, 2019-2020, 12 novembre 2019, no 005, p. 47, Q. no 45)

Question de J. Soors au ministre de la Justice sur 'le criblage des communautés religieuses par la Flandre' (*Q.R.*, Chambre, 2019-2020, 12 novembre 2019, no 005, p. 67, Q. no 99)

Question de M. Dillen au ministre de la Justice sur la 'coopération entre le ministère public et les autorités fiscales' (*Q.R.*, Chambre, 2019-2020, 12 novembre 2019, no 005, p. 86, Q. no 81)

Question de W. Vermeersch au ministre de l'Intérieur sur le 'voyage en Chine de la police de Flandre occidentale' (*Q.R.*, Chambre, 2019-2020, 12 novembre 2019, no 005, p. 156, Q. no 249)

Question de L. Dierick au ministre des Télécommunications sur 'la sécurité de la 5G' (*Q.R.*, Chambre, 2019-2020, 12 novembre 2019, no 005, p. 249, Q. no 29)

Question de Ph. Goffin au ministre de la Justice sur 'le bourreau de Raqqa' (*Q.R.*, Chambre, 2019-2020, 29 novembre 2019, no 006, p. 73, Q. no 43)

Question de K. Bury au ministre de la Justice sur les 'imams, mosquées et associations prêchant le radicalisme islamique' (*Q.R.*, Chambre, 2019-2020, 29 novembre 2019, Q. no 006, p. 86, Q. no 77)

Question de Ch. Lacroix au ministre des Affaires étrangères sur les 'menaces hybrides' (*Q.R.*, Chambre, 2019-2020, 29 novembre 2019, no 006, p. 143, Q. no 88)

Question de S. Cogolati au VPM Affaires étrangères sur 'les services de renseignement chinois en Belgique' (*C.R.I.*, Chambre, 2019-2020, 4 décembre 2019, COM 64, p. 7, Q. no 1441)

Questions jointes de W. De Vriendt et S. Cogolati au VPM Justice sur 'la collaboration entre les services de renseignements belges et rwandais' (*C.R.I.*, Chambre, 2019-2020, 4 décembre 2019, COM 64, p. 35, Q. nos 1762 et 1868)

Question de J. Soors au ministre de l'Intérieur sur 'les organisations d'extrême droite et la violence en Belgique' (*C.R.I.*, Chambre, 2019-2020, 4 décembre 2019, COM 65, p. 49, Q. no 1795)

Questions jointes de C. Thibaut et J. Arens au ministre de l'Intérieur sur 'l'important déploiement des forces de police pour une manifestation à Arlon' (*C.R.I.*, Chambre, 2019-2020, 4 décembre 2019, COM 65, p. 56, Q. nos 1878 et 1937)

Question de Ph. Pivin au VPM Justice, sur 'l'élargissement de la banque de données des combattants terroristes' (*C.R.I.*, Chambre, 2019-2020, 12 décembre 2020, PLEN 017, p. 28, Q. no 286)

Question de S. Creyelman au ministre des Affaires étrangères sur la 'cybersécurité' (*Q.R.*, Chambre, 2019-2020, 17 décembre 2019, no 007, p. 240, Q. no 132)

Questions jointes de K. Verduyckt, H. Bayet et Ch. Lacroix au ministre des Affaires étrangères sur 'Ia réorganisation au sein du SGRS' (*C.R.I.*, Chambre, 2019-2020, 18 décembre 2019, COM 78, p. 17, Q. nos 1295, 1399 et 1323)

Question de K. Aouasti au Ministre de l'Emploi, sur la 'discrimination à l'embauche à l'aéroport de Bruxelles-National' (*C.R.I.*, Chambre, 2019-2020, 19 décembre 2020, PLEN 018, p. 11, Q. no 317)

ANNEXE D.
CHARTER OF THE INTELLIGENCE OVERSIGHT WORKING GROUP

1. **Members of the European Intelligence Oversight Group**
   This Charter establishes the Intelligence Oversight Working Group, an informal cooperation between the following oversight bodies :
   - Belgian Standing Intelligence Agencies Review Committee,
     Comité permanent de contrôle des services de renseignement et de sécurité /Vast Comité van Toezichtop de inlichtingen- en veiligheidsdiensten (Belgium) ;
   - Danish Intelligence Oversight Board,
     Tilsynet med Efterretningstjenesterne (Denmark) ;
   - Review Committee on the Intelligence and Security Services,
     Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (The Netherlands) ;
   - EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee, *EOS-utvalget* (Norway) ;
   - Independent Oversight Authority for Intelligence Activities (OA-IA),
     Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND (Switzerland) ;
   - Investigatory Powers Commissioner's Office, (United Kingdom).

2. **Purposes of the Intelligence Oversight Working Group**
   The Intelligence Oversight Working Group aims to :
   - strengthen cooperation between the participating oversight bodies ;
   - increase transparency between oversight bodies within the limits and according to the standards set by national legislators, in order to support effective oversight of international cooperation between intelligence and security services ;
   - exchange knowledge, experiences and best practices of oversight ;
   - provide a platform for developing new and/or more effective oversight methods ;
   - maintain contact, share information and provide each other with mutual assistance as appropriate, in accordance with the boundaries set by national laws and regulations.

3. **Meetings**
   a) Chair meetings
      The Intelligence Oversight Working Group shall annually hold at least one meeting between the chairs of the oversight bodies, or a member of the oversight body representing the chair. In principle, each chair will be supported by their head of secretariat and/or another senior staff member.

b) Staff meetings
The intelligence Oversight Working Group shall regularly, when appropriate, hold staff meetings. The staff meetings are aimed at practically substantiating the purposes referred to in Section 2 of this Charter and carrying out the cooperation projects referred to in Section 4 of this Charter.

c) Preparation of meetings
Chair meetings shall be prepared by the oversight body hosting the meeting in cooperation with the informal secretariat referred to in Section 5 of this Charter. Staff meetings shall be prepared by the oversight body hosting the meeting. All Members voluntarily contribute to hosting meetings on a rotation basis.

4. Cooperation projects

The Intelligence Oversight Working Group may decide to enter into cooperation projects. Cooperation projects relate to a specific interest of the Group. The decision to enter into a cooperation project will be taken during a Chair meeting on the basis of a project proposal. Project proposals are prepared at staff level and shall include at a minimum :

- the intended goals for the project ;
- the proposed methods to reach those goals ;
- the timeframe in which the project is to be carried out.

5. Informal secretariat

The informal secretariat will be responsible for :

- reporting conclusions of the chair meetings ;
- reporting conclusions of the staff meetings in cooperation with the oversight body that organised the respective meeting ;
- monitoring progress on the cooperation projects ;
- communication with regard to outside interest in the Group. The secretariat will rotate every two years.

6. Information exchange

The participating oversight bodies commit to facilitating information sharing within the Group to further the purposes referred to in Section 2 of this Charter, where appropriate and in accordance with the boundaries set by national laws and regulations. The nature and extent of information sharing within the Group may also be defined by or dependent upon bilateral and/or multilateral agreements between the intelligence and security services overseen by the participating oversight bodies.

7. Membership

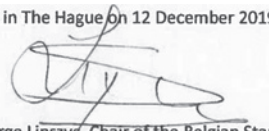
Extending membership of the Intelligence Oversight Working Group to other European oversight bodies on their request, shall take place on the basis of a decision by consensus taken during a Chair meeting.

8. Status, Implementation and Amendment of the Charter

This Charter reflects the intent of the participating oversight bodies within the Intelligence Oversight Working Group. Each participating oversight body commits

to implementing this Charter. Amendment of this Charter shall take place on the basis of a decision by consensus taken during a Chair meeting. This Charter is not legally binding.

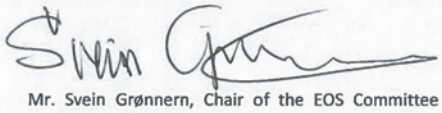
Signed in The Hague on 12 December 2019,



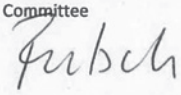
Mr. Serge Lipszyc, Chair of the Belgian Standing Intelligence Agencies Review Committee

Mr. Michael Kistrup, Chair of the Danish Intelligence Oversight Board

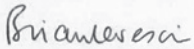
Mr. Nico van Eijk, Chair of the Dutch Review Committee on the Intelligence and Security Services



Mr. Svein Grønnern, Chair of the EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee



Mr. Thomas Fritschi, Director of the Swiss Independent Oversight Authority for Intelligence Activities



Sir Brian Leveson, Investigatory Powers Commissioner, United Kingdom

ACTIVITEITENVERSLAG 2019
RAPPORT D'ACTIVITÉS 2019

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 4, 1000 Brussel (02 286 29 88).

Reeds verschenen in deze reeks

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Vast Comité I, *Activiteitenverslag 2006,* 2007, 147 p.
3) Vast Comité I, *Activiteitenverslag 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, 2010, 220 p.
5) Vast Comité I, *Activiteitenverslag 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Vast Comité I, *Activiteitenverslag 2009,* 2010, 127 p.
8) Vast Comité I, *Activiteitenverslag 2010,* 2011, 119 p.
9) Vast Comité I, Activiteitenverslag 2011, 2012, 134 p.
10) W. Van Laethem en J. Vanderborght (eds), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, 2013, 565 p.
11) Vast Comité I, *Activiteitenverslag 2012*, 2013, 115 p.
12) Vast Comité I, *Activiteitenverslag 2013*, 2014, 210 p.
13) Vast Comité I, *Activiteitenverslag 2014*, 2015, 135 p.
14) Vast Comité I, *Activiteitenverslag 2015*, 2016, 132 p.
15) Vast Comité I, *Activiteitenverslag 2016*, 2017, 230 p.
16) Vast Comité I, *Activiteitenverslag 2017*, 2018, 152 p.
17) Vast Comité I, *Activiteitenverslag 2018*, 2019, 166 p.
18) J. Vanderborght (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, 2020, 151 p.
19) Vast Comité I, *Activiteitenverslag 2019*, 2020, 149 p.

ACTIVITEITENVERSLAG 2019

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de
inlichtingen- en veiligheidsdiensten

INTERSENTIA

Antwerpen – Gent – Cambridge

Voorliggend *Activiteitenverslag 2019* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 28 oktober 2020.

(*getekend*)
Serge Lipszyc, voorzitter
Pieter-Alexander De Brock, raadsheer
Laurent Van Doren, raadsheer
Wauter Van Laethem, dienstdoend griffier

Activiteitenverslag 2019
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

© 2020 Lefebvre Sarrut Belgium NV
Hoogstraat 139/6 – 1000 Brussel

ISBN 978-94-000-1209-7
D/2020/7849/68
NUR 823

Alle rechten voorbehouden. Behoudens uitdrukkelijk bij wet bepaalde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, op welke wijze ook, zonder de uitdrukkelijke voorafgaande toestemming van de uitgever.

Ondanks alle aan de samenstelling van de tekst bestede zorg, kunnen noch de auteurs noch de uitgever aansprakelijkheid aanvaarden voor eventuele schade die zou kunnen voortvloeien uit enige fout die in deze uitgave zou kunnen voorkomen.

INHOUD

LIJST MET AFKORTINGEN

ADIV	Algemene Dienst Inlichting en Veiligheid
AG	Administrateur-generaal (VSSE)
AGA	adjunct-Administrateur-generaal (VSSE)
ANG	Algemene Nationale Gegevensbank
AVG	Algemene Verordening Gegevensbescherming
BELPIU	*Belgian Passenger Information Unit*
BIM	Bijzondere inlichtingenmethoden
BIM-Commissie	Bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door inlichtingen- en veiligheidsdiensten
BIM-Wet	Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten
BISC	*Belgian Intelligence Studies Centre*
BPR	*Business Process Re-engineering*
BS	Belgisch Staatsblad
BSS	*British Security Service* (ook gekend als MI5)
BTA	Bevoegde toezichthoudende autoriteit
CCIRM	*Collection Coordination Information Requirement Management* (ADIV)
CGVS	Commissariaat-Generaal voor de vluchtelingen en de staatlozen
CHOD	*Chief of Defence*
CI	*Counterintelligence*
CNCTR	*Commission nationale de contrôle des techniques de renseignement*
COC	Controleorgaan voor politionele informatie
CRAB	Compte Rendu Analytique – Beknopt Verslag
CRIV	Compte Rendu Intégral – Integraal Verslag
CTG	*Counter Terrorism Group*
CTIVD	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten
DA	Directeur Analyse (VSSE)
DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
Dienst VVS	Dienst Veiligheidsverificaties (VSSE)

DISCC	*Defense Intelligence and Security Coordination Centre* (ADIV)
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
DVZ	Dienst Vreemdelingenzaken
EION	*European Intelligence Oversight Network*
EVRM	Europees Verdrag voor de Rechten van de Mens
FANC	Federaal Agentschap voor Nucleaire Controle
FOD	Federale overheidsdienst
FTF	*Foreign terrorist fighters*
GBA	Gegevensbeschermingsautoriteit
GBA-Wet	Wet van 3 december 2017 tot oprichting van de gegevensbeschermingsautoriteit
GBW	Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoons-gegevens (Gegevensbeschermingswet)
GCHQ	*General Communications Headquarters*
GGB	Gemeenschappelijke gegevensbank
HTF	*Homegrown terrorist fighters*
Hand.	Handelingen
HP	Haatpropagandisten
HUMINT	*Human intelligence*
ICP	*Intelligence collection plan*
ICT	Informatie- en communicatietechnologie
IMINT	*Image intelligence*
INE	Intelligence Network Europe
IOWG	*Intelligence Oversight Working Group*
ISTAR	*Intelligence, surveillance, target acquisition and reconnaissance*
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 TF	Koninklijk besluit van 23 april 2018 tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' en

	tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de Wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' naar de gemeenschappelijke gegevensbank 'Terrorist Fighters'
KB HP	Koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de WPA
KB OCAD	Koninklijk besluit van 28 november 2006 tot uitvoering van de Wet van 10 juli 2006 betreffende de analyse van de dreiging
M.B.	Ministerieel besluit
MoU	*Memorandum of Understanding*
NA	*Note aux autorités*
NAVO	Noord-Atlantische Verdragsorganisatie
NOS	*Nato Office of Security*
NSIP	Nationaal Strategisch Inlichtingenplan
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open sources intelligence*
OT	Organieke tabel
Parl. St.	Parlementaire Stukken van Kamer en Senaat
PDR	*Plan Directeur du Renseignement* (Inlichtingenstuurplan)
PGE	Potentieel gewelddadige extremisten
PNR-Wet	Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens
POC	*Point of contact*
SIGINT	*Signals intelligence*
SIS	*Secret Intelligence Service* (ook gekend als MI6)
SOP	*Standard Operating Procedures*
TF	*Terrorist fighters*
TV	Terrorisme-veroordeelden
Vast Comité I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten
Vr. en Antw.	Schriftelijke vragen en antwoorden (Kamer of Senaat)
VSSE	Veiligheid van de Staat
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen

W.C&VM	Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
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 coördinatie-orgaan voor de dreigingsanalyse

WOORD VOORAF

Reeds in september 1994 wees het Vast Comité I bij de publicatie van zijn eerste activiteitenverslag op het tekort aan mankracht bij de Veiligheid van de Staat en de Algemene Dienst Inlichting (later ADIV).[1] Zesentwintig jaar na datum geldt deze vaststelling helaas nog steeds.

Het Comité stelt vast dat de inlichtingengemeenschap in de praktijk niet de plaats heeft die haar toekomt in België. Dit komt door het gebrek aan evenwicht tussen de verplichtingen en de verwachtingen waaraan de twee diensten tegemoet moeten komen enerzijds en hun structurele onderbezetting anderzijds. Dit hoeft evenwel niet noodzakelijk een onoplosbaar probleem te zijn!

De activiteitenverslagen van het Comité kunnen, evenzeer als de verslagen van de parlementaire commissies, geen catalogus van herinneringen of aanbevelingen meer zijn. En, '*kort na de aanslagen bestempelden sommigen in binnen- en buitenland België als een failed state. Maanden van noeste arbeid in de onderzoekscommissie maakten duidelijk dat dit een zwaar overtrokken beeld is. De meeste dingen liepen en lopen wél geolied, alleen zat en zit er hier en daar zand in de machine, zo werd het verwoord door de heer Dewael. De aanbevelingen van de onderzoekscommissie zijn er precies op gericht dat zand uit de machine te halen*'.[2]

Ons land wordt vandaag de dag, net als de meeste Europese landen, geconfronteerd met een breed scala aan dreigingen. Er is ongetwijfeld het jihadistisch of extreemrechts terrorisme. Er zijn de verontrustende ontwikkelingen inzake inmenging- en spionageactiviteiten door buitenlandse mogendheden. Deze dreigingen vereisen dat onze diensten in staat zijn om hierop te reageren. Zij hebben allen hetzelfde doel: het bestrijden van aanvallen op het democratisch fundament van onze Staat.

Is er gegronde reden tot klagen? Nee, het is alleen een bezorgdheid. We kunnen vaststellen dat de opeenvolgende rapporten van het Comité aan de verantwoordelijken binnen Defensie ervoor hebben gezorgd dat een *change management* werd opgestart dat onontbeerlijk is geworden bij de ADIV.

Maar deze belangrijke verbetering is ontoereikend om voldoening te schenken. Het uitgevoerd toezichtonderzoek inzake veiligheidsscreenings binnen de inlichtingendiensten in België, wijst ontegensprekelijk op een reëel probleem.

1 VAST COMITÉ I, *Activiteitenverslag 1994*, 51.

2 BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS, *Onderzoekscommissie terroristische aanslagen 22 maart 2016. Beknopt overzicht van de werkzaamheden en aanbevelingen*, 2018, 13.

Hoe kunnen we, ondanks de aanbevelingen van de onderzoekscommissie naar de terroristische aanslagen, aanvaarden dat nieuwe informatie die in het bezit is van de politie-, justitie- en veiligheidsdiensten niet *in real time* wordt uitgewisseld, maar pas veel later wordt gedeeld, op basis van aanvragen om verlenging van veiligheidsmachtigingen, -attesten of -adviezen? Deze informatie blijft onaanvaardbaar lang opgeslagen in hermetisch afgesloten silo's. Deze vaststelling is meer dan verontrustend. De aanbeveling van de parlementaire commissie blijft op dit punt een dode letter: *'Relevante informatie moet vlot doorstromen van het ene beleidsniveau naar het andere, van de ene overheidsdienst naar de andere. Die vlotte informatiedoorstroming moet er ook zijn tussen de Belgische diensten en haar internationale tegenhangers. Op die manier moeten de veiligheidsdiensten potentiële terroristen vroeg op het spoor komen, snel kunnen overleggen en flexibel prioriteiten kunnen afbakenen.*'[3]

De aanslagen in Parijs en Brussel hebben geleid tot een lawine aan wetgevende initiatieven. De twee inlichtingendiensten alsook het Comité zien dat hun bevoegdheden daarop werden uitgebreid. Voor het Comité betreft deze uitbreiding ongetwijfeld een garantie voor de bescherming van de private levenssfeer, de rechten van de burgers en de goede werking van de instellingen. Helaas werden deze wettelijke maatregelen genomen zonder rekening te houden met de werkelijke capaciteit van de instellingen die ze moeten uitvoeren. Het Comité beschouwt het als zijn taak om regelmatig terug te komen op dit beginsel en erop toe te zien dat de wetgevende en de uitvoerende macht ook de nodige gevolgen geven aan deze wetgevende ontwikkelingen.

Onze rol is vandaag de dag des te belangrijker, aangezien de nieuw toegekende bevoegdheden een effectieve controle vergen. Zonder deze controle kunnen we onze rol als bewaker van de democratie niet waarmaken. Het is niet alleen de taak van het Comité om een zorgvuldig toezicht uit te oefenen op de twee inlichtingendiensten; het Comité moet ook, al naargelang een ingewikkelde bevoegdheidsverdeling, hetzij met het Vast Comité P, hetzij met het Controleorgaan op de politionele informatie (COC), de goede werking van het Coördinatieorgaan voor de dreigingsanalyse (OCAD), zijn gegevensbanken en zijn ondersteunende diensten nagaan.

Sinds 2018 werd het Comité de gegevensbeschermingsautoriteit op het vlak van het inlichtingenwerk. Daarmee werd het Comité dus de bewaker en beschermer van de gegevens van de burger. In een wereld waar gegevensbanken en metadata *legio* worden, wordt de rol van het Comité uitgebreid. Het Comité moet in staat zijn om zowel de gegevensbanken, hun veiligheidslacunes evenals het gebruik van cyber te controleren. Daarnaast moet het Comité ook het vraagstuk van de oprichting van een kruispuntbank voor de veiligheid opvolgen.

3 *Ibid.*, 38.

Is het dan ook niet vanzelfsprekend dat het Comité naast deze taken ook wordt belast met het toezicht op de andere overheidsdiensten die buiten elke controle of buiten elk wettelijk kader om inlichtingenwerk verrichten?

Naast het toezicht op de inlichtingendiensten is de rol van het Comité als ondersteuning van het Beroepsorgaan – een administratief rechtscollege – van het grootste belang. Op die manier kan het Comité garanderen dat het een rol speelt als 'een justitiële openbare dienst' op het gebied van dagdagelijkse veiligheid.

Kunnen we in het licht van deze dreigingen, van de nieuwe bevoegdheden, van de vele aanbevelingen die zonder gevolg blijven, zomaar passief blijven? Het Comité is van mening dat de algemene context waarin de ADIV en de VSSE dagelijks hun opdrachten vervullen, krachtige engagementen vereisen om de veiligheid te bevorderen.

Voorliggend activiteitenverslag wordt opgedragen aan Wouter De Ridder, die na een professionele carrière te hebben gewijd aan onze instelling, op rust wordt gesteld. Als griffier heeft hij er gedurende bijna 30 jaar toe bijgedragen om van het Comité een model te maken van een toezichtsorgaan op de inlichtingen- en veiligheidsdiensten dat wereldwijd werd uitgedragen. We willen hem hiervoor oprecht bedanken.

Serge Lipszyc,
Voorzitter van het Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

26 oktober 2020

HOOFDSTUK I
DE TOEZICHTONDERZOEKEN

Diverse instanties of personen kunnen het Vast Comité I 'vatten' met een toezichtonderzoek: de parlementaire Begeleidingscommissie, de voogdijministers, elke (rechts)persoon die klacht of aangifte wenst te doen … Het Comité kan ook zelf het voortouw nemen. In 2019 finaliseerde het Vast Comité I zes toezichtonderzoeken (I.1 tot I.6). Daarvan werden twee onderzoeken ambtshalve opgestart, werden twee onderzoeken uitgevoerd op verzoek van de parlementaire Begeleidingscommissie en werden ten slotte twee onderzoeken geïnitieerd vanuit een individuele klacht.[1] Verder opende het Comité in 2019 zeven nieuwe onderzoeken. Een korte omschrijving van nog lopende en/of opgestarte onderzoeken, volgt in I.7. De naar aanleiding van de toezichtonderzoeken geformuleerde aanbevelingen werden gebundeld in Hoofdstuk XI.

In totaal ontving het Comité in 2019 90 klachten of aangiften.[2] Na een kort vooronderzoek en de verificatie van een aantal objectieve gegevens, wees het Comité 82 klachten of aangiften af omdat ze kennelijk niet gegrond waren[3] (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 (Vast Comité P, Federale Politie, procureur des Konings of andere instanties). Van de acht behandelde klachten konden er zes worden afgerond in 2019.

Naast toezichtonderzoeken opent het Vast Comité I ook zogenaamde 'informatiedossiers' die moeten toelaten om een respons te bieden op vragen met betrekking tot de werking van de inlichtingendiensten en het OCAD.[4] Indien

---

1 Met de VSSE werd in januari 2019 een protocol afgesloten waarbij de dienst toegang verleent tot zijn centrale database aan individueel gemandateerde leden van de Dienst Enquêtes I voor consultaties in het kader van de wettelijke opdrachten van het Comité of de veiligheid van de uitvoering van de opdrachten.

2 Eerst wordt de ontvankelijkheid bestudeerd en wordt de klacht door de Dienst Enquêtes I behandeld. Indien zich een algemene 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).

3 Het Comité is bestemmeling van nogal wat klachten en aangiften van mensen met waanbeelden.

4 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 ….

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 2019 werden onder meer informatiedossiers geopend over het sociaal overleg binnen de inlichtingendiensten, over veiligheidsrisico's en mogelijke dysfuncties bij de ADIV of nog, over de werkzaamheden van de Opvolgingscommissie terroristische aanslagen.[5]

I.1. DE UITVOERING VAN VEILIGHEIDSSCREENINGS DOOR DE INLICHTINGENDIENSTEN

De VSSE en de ADIV onderzoeken jaarlijks meerdere duizenden personen die een of andere vergunning of toelating willen bekomen of die een bepaalde functie willen bekleden. Met deze onderzoeken willen ze nagaan of de betrokkenen voldoende garanties bieden op het vlak van betrouwbaarheid en veiligheid.

De rol die de inlichtingendiensten spelen in het kader van deze betrouwbaarheidsonderzoeken is niet steeds dezelfde. Soms beperkt deze zich tot het doorgeven aan andere overheden van (persoons)gegevens die ze in hun bezit hebben. Soms gaan ze actief op zoek naar bijkomende gegevens. Soms verlenen ze een gemotiveerd advies en in enkele specifieke gevallen nemen ze (alleen of als onderdeel van een veiligheidsoverheid) ook de uiteindelijke beslissing omtrent het al dan niet toekennen of intrekken van de vergunning of de toelating.

Het Comité achtte het legitiem om, vertrekkende vanuit een individuele klacht, een breder toezichtonderzoek te openen naar de wijze waarop de inlichtingendiensten veiligheidsscreenings[6] uitvoeren.[7]

---

5 Voluit de 'Opvolgingscommissie 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'.

6 Onder 'veiligheidsscreenings' wordt begrepen: *"een door of krachtens de wet opgelegde beoordeling door een administratieve overheid op basis van eigen of aangeleverde (persoons)gegevens waarbij uitgemaakt wordt of een private (rechts)persoon een profiel vertoont waaruit een risico blijkt dat hij/zij een niet-geëigend gebruik zal of zou kunnen maken van een bepaalde toelating en daarbij of daardoor bepaalde fundamentele (staats)belangen in het gedrang kan brengen zodat diezelfde of een andere (buitenlandse) overheid geïnformeerd kan beslissen over de toekenning, intrekking of beperking van die toelating*". Definitie ontleend aan: W. VAN LAETHEM, 'Veiligheidsscreenings', Praktijkseminarie, 22 november 2016 (Brussel, Politeia).

7 'Toezichtonderzoek over de manier waarop de VSSE en de ADIV veiligheidsverificaties uitvoeren, de gegevens evalueren nodig bij het toekennen van veiligheidsattesten of het formuleren van veiligheidsadviezen, dit in toepassing van artikelen 22*bis* tot 22*sexies* van de Wet van

I.1.1. HET JURIDISCH KADER

I.1.1.1. De wettelijke opdrachten

De Wet van 30 november 1998 heeft de opdrachten en bevoegdheden van de twee inlichtingendiensten strikt omschreven. Voor de VSSE zijn de opdrachten terug te vinden in artikel 7 W.I&V; voor de ADIV in artikel 11 W.I&V. Naast de inlichtingenopdracht (art. 7, 1° en 3°/1 W.I&V) en het voeren van veiligheidsonderzoeken (art. 7, 2° W.I&V), mag de VSSE alleen andere opdrachten uitvoeren '*die haar door of krachtens de wet worden toevertrouwd*' (art. 7, 4° W.I&V). Voor de ADIV is de wetgever zelfs strenger geweest in die zin dat niet werd voorzien in de mogelijkheid om taken '*krachtens de wet*' uit te voeren. Voor de screenings die uitgevoerd worden door de inlichtingendiensten of waaraan zij hun medewerking verlenen door gegevens over te zenden naar andere overheden, betekent het voorgaande dus dat er een specifieke, wettelijke basis moet voorhanden zijn die deze activiteiten toelaten.

Wat dat betreft, bestaan er vele wettelijke bepalingen die het mogelijk maken dat de VSSE en/of de ADIV (in sommige procedures is de ADIV geen betrokken partij) de inlichtingen waarover ze beschikken, doorzenden naar diverse overheden die op basis hiervan een evaluatie maken. Uit de juridische analyse bleek evenwel dat al deze regelingen – soms fundamenteel, soms oppervlakkig – verschillen.

Los daarvan, kon het Comité vaststellen dat bij beide inlichtingendiensten – soms in te beperkte mate en soms geen – rekening werd gehouden met deze diverse regelgevingen (*infra*). Tevens bleek dat de wetgeving onvoldoende gekend was en/of dat de diensten onvoldoende kritisch waren bij de vraag of hun medewerking aan bepaalde screenings wettelijk toegelaten was (en zoja, onder welke voorwaarden). Ook bleek dat de inlichtingendiensten nog steeds verwezen naar artikel 19 W.I&V. Nochtans had het Comité reeds eerder[8] gesteld dat dit specifieke artikel in het kader van screenings geen wettelijke basis bood voor het systematisch doorgeven van gegevens aan andere overheden met het oog op een beoordeling.[9]

---

11 december betreffende de classificatie en de veiligheidsmachtigingen, -attesten en –adviezen (W.C&VM)'. Het onderzoek werd geopend in februari 2017 en afgesloten in maart 2019.

8 VAST COMITÉ I, *Activiteitenverslag 2003*, 278-288. Het Comité waarschuwde voor mogelijke juridische problemen indien een overheid zijn beslissingen blijft baseren op informatie die zij in het kader van een systematische screening van de VSSE of de ADIV verkrijgt, zonder specifieke wettelijke basis. Het onderzoek toonde aan dat deze situatie zich nog steeds voordeed.

9 Deze analyse heeft overigens geleid tot de Wet van 3 mei 2005 waarbij in de Classificatiewet van 11 december 1998 een ruim kader werd gecreëerd voor screenings in de meest uiteenlopende domeinen.

I.1.1.2. Aangepaste wetgeving

Op het moment van het toezichtonderzoek, was er geen wettelijke basis voor de screening van bepaalde gevoelige functies en sectoren (bijv. penitentiaire beambten). Nog tijdens de onderzoeksfase werd de wetgeving inzake veiligheidsverificaties aangepast door de Wet van 23 februari 2018[10], met een toenemend aantal vragen tot verificaties (bijv. openbaar vervoer, private veiligheidssector …) tot gevolg. Dezelfde wetgeving voorzag ook een nieuwe opdracht voor de VSSE en de ADIV; de diensten werden verantwoordelijk voor dreigingsanalyses met betrekking tot verschillende sectoren op het vlak van spionage.

I.1.2. VEILIGHEIDSSCREENINGS BIJ DE VSSE

I.1.2.1. Organisatie

Aanvragen voor veiligheidsverificaties worden binnen de VSSE in eerste instantie behandeld door de Dienst Veiligheidsverificaties (VVS). Deze dienst valt onder de hiërarchische verantwoordelijkheid van de adjunct-Administrateur-generaal (AGA). Bepaalde types van screenings worden in een tweede fase behandeld door de analysediensten, dewelke vallen onder de verantwoordelijkheid van de Directeur van de Analyse (DA).

Het Comité kon vaststellen dat er geen specifieke vorming is voorzien voor het personeel van de Dienst VVS. Zij beschikken over dezelfde, eerder generieke, vormingsmogelijkheden als het overige administratieve personeel, bovenop de basisvorming over de algemene structuur en de taken van de VSSE. Naar luid van het diensthoofd van de Dienst VVS, werden er in het verleden evenwel geen lacunes vastgesteld in de vormingsbehoeften. De specifieke, taakgebonden vorming gebeurt *'on the job'*.

De Directie-generaal van de VSSE ziet de uitvoering van screenings als een specifieke opdracht, die men dan ook volledig centraal zou willen laten behandelen binnen deze dienst. Het was de intentie van de VSSE om een herstructurering door te voeren van de wijze waarop de opdracht van de dienst inzake screenings wordt uitgevoerd. *In concreto* zal alles wat screenings betreft, worden gecentraliseerd binnen de Dienst VVS. In de loop van het onderzoek startte een werkgroep met het bekijken van de toekomst van de Dienst VVS, en over de oprichting van een pijler 'Veiligheid en Advies' die de Diensten VVS, VES (veiligheidsonderzoeken) en VBS (veiligheidsbureau) zou groeperen. De beslissing van de Directie-

[10] Wet van 28 februari 2018 houdende wijziging van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, de veiligheidsattesten en de veiligheidsadviezen, *B.S.* 1 juni 2018.

generaal om in de toekomst de behandeling van alle veiligheidsverificaties te centraliseren binnen één dienst, had tot gevolg dat de effectieven werden verhoogd.

II.1.2.2. Kwantitatieve gegevens

Uit de cijfergegevens[11] die door de Veiligheid van de Staat ter beschikking werden gesteld, bleek een gestage toename van het aantal uitgevoerde verificaties. Opvallend was vooral de toename in het kader van naturalisaties en verklaringen van nationaliteit en het sterk toegenomen aantal verificaties op vraag van de Dienst Vreemdelingenzaken (DVZ) en het Commissariaat-generaal voor Vluchtelingen en Staatlozen (CGVS). Een andere kwantitatief belangrijke categorie van veiligheidsscreenings is deze in het kader van de afgifte van toegangsbadges voor (bepaalde delen van) de luchthavens.

Binnen de VSSE wordt een bepaalde norm gehanteerd van het aantal verificaties die kunnen worden verricht. Voor 2017 zat men 12% boven deze norm. Het feit dat deze norm wordt overschreden, hield het risico in dat in geval van afwezigheid van één of meerdere personeelsleden er een probleem van achterstand dreigde te ontstaan. Er was dus geen reserve om afwezigheden op te vangen.

I.1.2.3. Werkprocessen

Bij het uitvoeren van screenings treedt de VSSE op als leverancier van informatie aan andere overheden enerzijds, en als veiligheidsoverheid anderzijds.[12]

Alle vragen tot screenings worden in eerste instantie in behandeling genomen door de Dienst VVS. Het Comité merkte op dat er bij ontvangst van de namenlijsten geen controle plaatsgreep over de wettelijkheid van de vraag, wat in sommige gevallen niettemin noodzakelijk is (bijv. voor de niet-routinematige vragen). Wel voert de Dienst VVS onmiddellijk een verificatie uit in de databank van de VSSE. Indien een individu niet bekend is, antwoordt de behandelende medewerker rechtstreeks aan de bevoegde overheid/cliënt. In geval van een positieve *'hit'*, wordt dit voorgelegd aan het diensthoofd, die een beoordeling maakt van de beschikbare informatie en vervolgens een antwoord opstelt voor de aanvragende overheid/cliënt.

Voor die screenings waar de Nationale Veiligheidsoverheid (NVO) de bevoegde veiligheidsoverheid is (bijv. bij veiligheidsverificaties die moeten leiden

---

11 De cijfergegevens zijn eerder indicatief. De gehanteerde werkwijze laat niet toe statistieken te genereren betreffende het exacte aantal positieve verificaties of *'hits'*. Daardoor is het niet mogelijk om (op langere termijn) de resultaten van de dienst te monitoren. Dit heeft ook een impact op de strategievorming in de zin dat het moeilijk is doelstellingen vast te leggen (en middelen toe te kennen of een gefundeerde werklastverdeling tussen de Dienst VVS en de analysediensten te bepalen).

12 Dit laatste is het geval wanneer tijdelijk personeel (bijv. voor onderhoudswerken) toegang moet worden verleend tot de gebouwen van de dienst en wanneer de dienst zelf evenementen organiseert.

tot een veiligheidsattest of -advies) wordt alle relevante informatie collegiaal met alle betrokken diensten besproken bij de NVO. Enkel in het kader van beroepsprocedures wordt een volledige, gecontextualiseerde nota meegedeeld aan de NVO.

Een andere werkwijze wordt gehanteerd bij aanvragen in het kader van een naturalisatieaanvraag en aanvragen door de DVZ of het CGVS. Indien er in deze gevallen sprake is van een *'hit'*, wordt de aanvraag overgemaakt aan de (geografisch) bevoegde analysedienst, die de in de databank beschikbare informatie evalueert en een antwoord opmaakt in de vorm van een gecontextualiseerde nota. Er werden in 2017 meerdere duizenden dossiers behandeld door de analysediensten.[13] In bepaalde gevallen werd daarbij beslist tot bijkomend onderzoek door de buitendiensten die instaan voor de collecte van informatie (bijv. wanneer de informatie die beschikbaar is over een persoon onzeker (onbevestigd) of niet geactualiseerd is). Dergelijk bijkomend onderzoek vormde geen prioriteit voor de collectiediensten.

De bovenstaande processen werden niet schriftelijk beschreven in dienstnota's of in een vademecum.

Uit het onderzoek van het Comité is gebleken dat de Dienst VVS screenings uitvoert zonder dat daarbij de wettelijke basis duidelijk kan aangegeven worden (*supra*). In bepaalde gevallen is het daarbij niet duidelijk wat de precieze finaliteit is van de vraag, met andere woorden of het om een veiligheidsscreening gaat of om een andere controle in de databank van de VSSE.[14] Hiervoor verwees de VSSE (verkeerdelijk, *supra*) systematisch naar artikel 19 W.I&V. Alhoewel het nuttig en raadzaam kan zijn dat de Belgische diensten worden geconsulteerd met betrekking tot Belgische ingezetenen aan wie eventueel toegang zou worden verschaft tot de installaties van in België gevestigde internationale instellingen, is hiervoor een wettelijk mandaat vereist.[15]

Ten slotte kon worden vastgesteld dat bij de uitvoering van de screenings de relatie met de buitenlandse partnerdiensten ontbrak. Door de hoge werklast is het onmogelijk om buitenlandse autoriteiten te bevragen in het kader van screenings. Dit tast evenwel de informatiepositie van de VSSE aan waardoor het risico bestaat

---

13 Op het moment van het onderzoek waren geen gestandaardiseerde criteria in gebruik voor het opstellen van een antwoord in het kader van een screening. Elke dienst (VVS of analysedienst) stelde een antwoord op naar eigen inzicht.

14 Zo worden bijvoorbeeld screenings uitgevoerd op vraag van de veiligheidsdienst van de NAVO, de Nato Office of Security (NOS). Het gaat hierbij om een screening van personen aan wie al dan niet toegang wordt verleend tot de installaties van de NAVO.

15 Dergelijke screenings werden mogelijk gemaakt door de Wet van 23 februari 2018. Alvorens er voor een internationale instelling veiligheidsverificaties kunnen worden aangevraagd, moet er onder meer een overeenkomst worden afgesloten tussen de bevoegde administratieve overheid en de desbetreffende instelling alsook een dreigings-, risico- en impactanalyse worden uitgevoerd (Wet van 23 februari 2018 houdende wijziging van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen).

dat personen van buitenlandse origine bij veiligheidsverificaties door de mazen van het net glippen. Omgekeerd antwoordt de Dienst VVS wél op vragen van buitenlandse inlichtingendiensten, terwijl de wettelijke basis ook hier onduidelijk is.

I.1.2.4. Middelen

De VSSE is van mening dat de verantwoordelijkheid van de dienst in het kader van een screening ten behoeve van andere veiligheidsoverheden, zich beperkt tot het nagaan of de entiteit (persoon) bekend is in de eigen documentatie (interne gegevensbank).

De VSSE maakt daarbij gebruik van één centrale databank. Tijdens het onderzoek werd duidelijk dat de door de Dienst VVS opgemerkte onvolkomenheden in deze databank, niet gecorrigeerd werden.[16] Bij de ontwikkeling van deze databank werd destijds weinig of geen rekening gehouden met het bestaan van de Dienst VVS noch met diens opdracht. Dit heeft tot gevolg dat, omwille van de manier waarop de databank is gestructureerd, de Dienst VVS weliswaar eigen documenten kan opstellen (bijv. interne verslagen van overlegvergaderingen met externe partners waaraan werd deelgenomen) en invoeren in de databank, maar dat deze documenten enkel zichtbaar zijn voor de medewerkers van de Dienst VVS zelf.

Wat betreft de eigen IT-middelen, zullen met betrekking tot de opdracht van screenings verbeteringen worden aangebracht in de structuur van de databank. Deze verbeteringen kaderen echter in de meer algemene hervorming van de dienst, waarvan de precieze timing onduidelijk was.

Als gevolg van de aangepaste wetgeving inzake veiligheidsverificaties (*supra*) werd voorzien dat 25% van de retributiekost die zal moeten worden betaald door de aanvrager van een veiligheidsattest en -advies, zal vloeien naar de dienst(en) die de verificatie uitvoeren.[17] Deze kredieten kunnen worden geïnvesteerd in bijkomende middelen.

---

16 Het weze vermeld dat de aanleiding tot het toezichtonderzoek, namelijk een klacht van een persoon die in het kader van een naturalisatieprocedure een negatief resultaat kreeg, het gevolg was van het gebruik van informatie die niet volledig kon worden hardgemaakt, of die minstens niet *up to date* was. Het feit dat er in de VSSE-databank onvolledige of onjuiste identiteiten voorkomen, vergroot het risico op 'valse' resultaten bij veiligheidsverificaties. Het niet-aanvullen van informatie staat haaks op de principes van de bescherming van persoonsgegevens.

17 KB van 8 mei 2018 tot vaststelling van de bedragen van de retributies die verschuldigd zijn voor de veiligheidsmachtigingen, voor de veiligheidsattesten en veiligheidsadviezen afgegeven door de Nationale Veiligheidsoverheid en voor de veiligheidsattesten afgegeven door het Federaal Agentschap voor Nucleaire Controle alsook van de verdeelsleutels bedoeld in artikel 22*septies*, zesde en achtste lid, van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *BS* 1 juni 2018.

I.1.2.5. Verbetertraject

De VSSE zag een aantal mogelijkheden tot verbeteringen op het vlak van screenings.

Eén van de meest nuttige en noodzakelijke verbeteringen is de creatie van een *'flagging'* systeem, waarbij alle personen die in de databank bekend zijn en die het voorwerp uitmaken of hebben uitgemaakt van een screening, als dusdanig staan aangeduid. Dit zou aan de analyse- en buitendiensten toelaten om eventuele nieuwe, relevante informatie met betrekking tot de persoon te kaderen in een veiligheidsverificatie, en onder de aandacht te brengen van de Dienst VVS.

Tevens zou de dienst het als een positieve evolutie beschouwen als er met de 'cliënten' een akkoord tot stand zou kunnen worden gebracht omtrent een uniforme *template* voor de aanvragen.

Een andere mogelijke verbetering is de creatie van een IT-portaal voor het invoeren van aanvragen voor veiligheidsverificaties.

De VSSE streeft ook naar een betere afstemming van de screenings op de behoeften van de 'cliënten'. Zo werd overleg gepleegd met de parketten van Antwerpen en Luik met als doel na te gaan hoe beter bepaald kan worden welke inlichtingen pertinent zijn in het kader van procedures van nationaliteitsverwerving.

Ten slotte wordt ook een vademecum ontwikkeld, waarin de te volgen interne procedures bij screenings, worden geformaliseerd.

Het Vast Comité I achtte het aanbevelenswaardig om deze initiatieven ook te ontwikkelen voor andere begunstigden.[18] De VSSE zag voor het invoeren van dergelijke initiatieven voor verbetering een cruciale rol weggelegd voor de Nationale Veiligheidsoverheid (NVO).

I.1.2.6. Bijzondere aandacht

Uit het onderzoek bleek opnieuw dat er geen actieve, systematische opvolging in de tijd is van de situatie van een persoon voor wie een screening werd verricht. Dit brengt risico's met zich mee, niet in het minst bij de dienst die de screening heeft aangevraagd en eventueel een individu in dienst heeft genomen op basis van een gunstige beoordeling. Zo bijvoorbeeld wordt een toegangsbadge voor de terreinen van een luchthaven verstrekt voor een periode van vijf jaar, wat relatief lang is. In deze periode van vijf jaar zal enkel een nieuwe verificatie plaatsvinden, indien de betrokken persoon een nieuwe functie verkrijgt.

---

[18] Het Vast Comité I wees erop dat in de diverse reglementaire bepalingen waarbij screenings toegelaten zijn, elementen zijn opgenomen die aangeven welke informatie relevant is bij de beoordeling van de betrouwbaarheid van een persoon in het licht van de betrokken toelating, vergunning, functie … Een betere kennis van deze reglementaire bepalingen is dan ook cruciaal om de diverse cliënten van de juiste informatie te voorzien.

Dit heeft ook een procesmatige dimensie: door de structuur van de databank van de VSSE, wordt de Dienst VVS niet automatisch op de hoogte gesteld van nieuwe negatieve informatie betreffende een persoon die in het verleden het voorwerp uitmaakte van een veiligheidsverificatie.[19]

I.1.3. VEILIGHEIDSSCREENINGS BIJ DE ADIV

I.1.3.1. Organisatie[20]

De Cel Screenings werd opgericht in 2015[21] en situeerde zich binnen de structuur van de ADIV formeel onder de hiërarchische verantwoordelijkheid van het hoofd van het zogenaamde *Collection Coordination & Information Requirement Management* (CCIRM), (op dat ogenblik) verantwoordelijk voor de registratie en toewijzing van alle inkomende en uitgaande informatie. De cel bestaat uit slechts enkele onderofficieren en bevindt zich in een ambigue situatie: de medewerkers hadden immers als administratieve chef het hoofd van de Directie S(ecurity) en als functionele chef het hoofd van het CCIRM. Zij beschikten niet over een vast aanspreekpunt in de hiërarchie in geval van vragen, problemen of wanneer er nood was aan een beslissing.

De Cel Screenings bleek in zijn werking zeer autonoom; er was vanuit de hiërarchie geen supervisie van de werking, de cel kreeg van hogerhand geen of nauwelijks instructies. Deze dubbelzinnige situatie deed ook vragen rijzen omtrent de eindverantwoordelijkheid binnen de ADIV en de interne (kwaliteits)controle.

Het ingezette personeel was ontoereikend om de taken uit te voeren. Een alsmaar toenemend aantal vragen tot verificatie heeft geleid tot een achterstand in de behandeling ervan. In de organieke tabel (OT) werd een versterking voorzien, maar deze diende zich vooralsnog niet aan. Ze was bovendien enkel voorzien om de toen actuele werklast het hoofd te bieden; er werd niet geanticipeerd op een nog te verwachten groeiende werklast.

Zoals reeds aangehaald, is de werking van de Cel Screenings binnen de ADIV eerder 'organisch' geëvolueerd, zonder duidelijke richtlijnen vanuit de hiërarchie. De personeelsleden kregen nooit specifieke vorming op juridisch vlak noch op het

19 Een '*flaggingssysteem*' kan hier soelaas bieden.

20 Het onderzoek was gebaseerd op de periode januari tot april 2018 en hield geen rekening met de oprichting van het *Defence Intelligence and Security Coordination Centre* (DISCC) binnen de structuur van de ADIV. Dit DISCC kreeg uitgebreide bevoegdheden toegewezen, en werd onder andere het *single point of entry & exit* dat alle inkomende en uitgaande informatie van de ADIV registreert en toewijst aan de bevoegde Directie. De Cel Screenings legt vanaf juni 2018 op zowel administratief als functioneel vlak verantwoording af aan het Hoofd van het DISCC. Het DISCC bestaat uit een bundeling van het CCIRM, het CTR (het communicatiecentrum van de ADIV) en een centraal secretariaat.

21 Vóór mei 2015 werden screenings voor de ADIV behandeld door een personeelslid van de Cel Databank, een sectie die deel uitmaakt van de pijler Steun aan Operaties van de Directie CI.

vlak van het gebruik van de beschikbare technische middelen. Zij hebben de uitvoering van hun taken *'on the job'* en vanuit de dagelijkse praktijk aangeleerd.

Ten slotte kon worden vastgesteld dat er bij de ADIV geen gecentraliseerde registratie en beheer was van (antwoorden op) vragen tot verificatie. Dit betekende dat er ook geen latere opvolging mogelijk was. Dit bracht risico's met zich mee, niet in het minst bij de dienst die de screening heeft aangevraagd en eventueel een individu in dienst heeft genomen op basis van een gunstige screening.

I.1.3.2. Kwantitatieve gegevens

Het Vast Comité I stelde vast dat er bij de ADIV geen integrale statistieken worden bijgehouden met betrekking tot de door de dienst uitgevoerde veiligheidsverificaties en screenings. Dit betekent dat er in feite geen oordeel kan gevormd worden over de kernresultaten van de dienst, noch over welke middelen de dienst nodig heeft om zijn opdracht tot een goed eind te brengen. Zonder zicht op de resultaten en benodigde middelen is strategievorming en een goede planning problematisch.

Naar aanleiding van het toezichtonderzoek en de vraag om cijfergegevens, werd door de Cel Screenings het initiatief genomen om statistieken op te vragen bij de Stafdienst J6 (ICT). Dit resulteerde in een aantal cijfergegevens betreffende het aantal verrichtte opzoekingen via één zoekmethode in één databank van de ADIV, met name de databank van de Directie CI. Het aantal zoekopdrachten zou *grosso modo* overeenkomen met het aantal te verifiëren entiteiten. Dit cijfer was in vergelijking met de cijfers van de VSSE onverklaarbaar hoog.

Bij oprichting van de Cel Screenings was het aantal te verwerken aanvragen goed beheersbaar, maar sinds eind 2016 was er sprake van een steeds grotere toename. Dit heeft ertoe geleid dat er een achterstand is ontstaan in de behandeling van de aanvragen en dat bepaalde types screenings terzijde werden geschoven. De Cel Screenings bepaalde zelf – naar eigen inzicht – aan welke screenings al dan niet prioriteit werd gegeven.

I.1.3.3. Werkprocessen

Alle types van screenings

Verzoeken tot screenings komen bij de Cel Screenings terecht via diverse kanalen: het geclassificeerde netwerk (via het CCIRM), via andere diensten (bijv. Directie S) of nog, via het niet-geclassificeerde netwerk (rechtstreeks van de 'cliënt').[22]

[22] De Cel Screenings stelde voor (aan het CCIRM) om dit te vereenvoudigen, en ervoor te zorgen dat alle aanvragen via één en dezelfde weg, met name via het CCIRM, zouden worden overgemaakt aan de Cel Screenings.

De rol van deze cel beperkt zich tot het nagaan of een entiteit (persoon) al of niet bekend is in de databanken van de ADIV. Zij doen dit door in eerste instantie een zoekopdracht uit te voeren via een zoekprogramma. Indien er over de bewuste persoon geen informatie beschikbaar is, verstuurt de dienst rechtstreeks een antwoord *'nothing significant to report'* (NSTR) naar de aanvragende overheid/cliënt. In geval van een positieve '*hit*', wordt aangegeven bij welke directie en in welke databank informatie over de entiteit beschikbaar is. Vervolgens kan de cel nog een bijkomende zoekopdracht uitvoeren in de desbetreffende databank. Voor een inhoudelijk overzicht van de beschikbare informatie wendt de Cel Screenings zich echter tot de bevoegde (analyse)dienst die de informatie in de databank heeft ingevoerd, die deze verder behandelt. Wanneer er in het kader van een veiligheidsverificatie verontrustende informatie aan het licht komt, maken de analysediensten deze per nota over aan, naargelang van het geval, de Nationale Veiligheidsoverheid of het Federaal Agentschap voor Nucleaire Contole (FANC). Wanneer het minder ernstige elementen betreft, wordt de informatie overgemaakt aan de cel voor mondeling overleg bij de NVO.

Volgens de analysediensten van de ADIV is men er zich van bewust dat de informatie die men meedeelt met betrekking tot een individu, verstrekkende gevolgen kan hebben voor de betrokkene. Men zou dus eerder terughoudend zijn bij het aanleveren van informatie. De dienst stelt dat de informatie die wordt meegedeeld in principe enkel betrekking heeft op het individu dat voorwerp uitmaakt van de verificatie of screening. In bepaalde gevallen zal ook pertinente informatie worden meegedeeld over de onmiddellijke omgeving van de betrokkene ter contextualisering. Er werden evenwel geen uniforme criteria vastgesteld bij de analysediensten over welke informatie en in welke vorm deze informatie wordt meegedeeld.[23] Het al dan niet meedelen van bepaalde informatie hangt af van de beoordeling van de individuele analist.

Uitgezonderd kandidaat-militairen

De hierboven beschreven procedure wordt toegepast voor alle types van screenings, uitgezonderd één type. In het geval van een verificatie in het kader van een veiligheidsadvies voor een kandidaat-militair, is de betrokken 'cliënt' een dienst binnen Defensie zelf, met name het Directoraat-generaal Human Resources (DG HR). Het is *in casu* de Dienst Veiligheidsmachtigingen (Habilitaties) van de Directie S(ecurity) van de ADIV die de formulering van het veiligheidsadvies coördineert, en die hiervoor ook een bevraging doet bij de VSSE en de Federale Politie.

[23] Er werd gesuggereerd om over het vastleggen van criteria gezamenlijk na te denken met de andere betrokken diensten zoals de VSSE, de Federale Politie, en het OCAD. Dit geldt des te meer nu de wetgeving van februari 2018 ook voorzag dat de diensten dreigingsanalyses dienen op te stellen in het kader van veiligheidsverificaties.

De Cel Screenings ontvangt de vraag tot deze veiligheidsverificaties – in de vorm van namenlijsten – zowel rechtstreeks van DG HR, als via de Dienst Veiligheidsmachtigingen. Het is pas vanaf het moment dat de Dienst Veiligheidsmachtigingen zijn fiat geeft, dat de Cel overgaat tot de verificaties in de databanken. Eventuele '*hits*' worden meegedeeld aan deze Dienst Veiligheidsmachtigingen. Wanneer de ADIV zelf optreedt als veiligheidsoverheid, werd de beslissingsbevoegdheid ter zake door de Chef van de ADIV gedelegeerd aan het hoofd van de Directie S(ecurity).

Behoudens voor feiten die verband houden met bezit, gebruik en handel in verdovende middelen, zijn er door de ADIV geen formeel vastgestelde criteria om te bepalen op welke basis een kandidaat-militair een positief of negatief advies krijgt. Er wordt in de praktijk gekeken of het om al dan niet zwaarwichtige feiten gaat, en er wordt ook rekening gehouden met het feit of de betrokkene ten tijde van deze feiten minder- of meerderjarig was. Een bijkomend criterium is hoe recent de eventuele negatieve feiten zijn.

Indien er negatieve informatie beschikbaar is over een kandidaat-militair, wordt uiteindelijk een collegiale beslissing genomen door het hoofd van de Directie S en twee andere officieren van de Dienst Veiligheidsmachtigingen.[24]

Zonder wettelijke basis

Uit het onderzoek bleek dat de Cel Screenings ook veelvuldig bevraagd wordt om screenings uit te voeren zonder dat er een duidelijke wettelijke basis voorhanden is. Het gaat dan om vragen van het OCAD, de Dienst DJSoc Terro van de Federale Politie, de Dienst External Relations Office (ERO) van de ADIV zelf (bijv. met betrekking tot buitenlandse defensie-attachés gestationeerd in België), de Cel voor Financiële Informatieverwerking (CFI), de Nato Office of Security (NOS), Europol/Interpol …

Op de vraag wie binnen de ADIV beslist welke soort opzoekingsopdrachten in de databanken dienen te worden uitgevoerd door de Cel Screenings, werd geen afdoend antwoord bekomen. In de meeste gevallen gaat het om inkomende berichten die door het CCIRM zonder meer aan de Cel Screenings ter behandeling worden overgemaakt. Er vindt geen aftoetsing plaats van de wettelijke basis van de vraag om informatie.

De leden van de Cel Screenings bleken beperkt op de hoogte te zijn van de wettelijke basis van hun werk. De Cel wordt door de hiërarchie of de juridische dienst van de ADIV ook niet systematisch op de hoogte gehouden van voor de uitvoering van hun taken relevante wettelijke aanpassingen en/of nieuwigheden

[24] In ongeveer 5% van de gevallen wordt er een negatieve beslissing genomen. Er zijn ook naar schatting een 15% 'twijfelgevallen' waarbij er wel negatieve informatie beschikbaar is over de kandidaat maar waarbij deze wel toegelaten wordt als militair, en waarbij de veiligheidsofficier van de toekomstige eenheid gevraagd wordt om tijdens de eerste maanden na toewijzing aan de eenheid een verhoogde aandacht te besteden aan de betrokkene.

of van gesloten protocolakkoorden met partners. Zij dienen zelfstandig op zoek te gaan naar dergelijke informatie.

Wel ontvangt de cel systematisch de beslissingen van het Beroepsorgaan. Hiervan doen zij echter geen verwerking. Er vindt met andere woorden geen analyse plaats van deze beslissingen. Dit beschouwt de Cel niet als haar taak.[25]

Met in het achterhoofd de oprichting van de DISCC *(zie infra)*, werd een denkoefening geïnitieerd over hoe de Cel Screenings in de toekomst beter zou kunnen functioneren. Dit zou moeten leiden tot het op punt stellen van de gehanteerde werkprocedures, die in een latere fase ook zouden worden uitgeschreven.

I.1.3.4. Middelen

Uit eerdere toezichtonderzoeken van het Vast Comité I met betrekking tot de werking van de ADIV, bleek dat verschillende databanken worden gebruikt. Alleen al de Directie S(ecurity) maakte gebruik van tenminste vijf verschillende databanken. Daarnaast waren er nog de overige directies (I, CI) die elk over hun eigen databanken beschikten. Dit zorgde ervoor dat het werk van de Cel Screenings tijdsintensief was en dat de opdracht van screenings zeer moeilijk centraal te coördineren viel. De Cel Screenings diende voor elke verificatie meerdere zoekmiddelen in te zetten. Het Comité wees in dit verband ook op de zwakheid die het bij een eerder onderzoek vaststelde[26] en waarbij tot uiting kwam dat bij de vermelde dienst een achterstand bestond bij de invoering van relevante informatie in de databank. Ook hier ontstond het risico dat bepaalde voorhanden zijnde, relevante inlichtingen – en in dit geval de meest actuele inlichtingen – bij een screening niet werden teruggevonden, met mogelijke gevolgen voor zowel de betrokken persoon als voor de dienst die de screening had gevraagd. Dit was evenmin gunstig voor de betrouwbaarheid van de dienst naar zijn partners toe.

Naast het personeelsgebrek, werd het gebrek aan performante technische middelen door de personeelsleden van de Cel Screenings aangehaald als het belangrijkste obstakel bij de uitvoering van hun opdracht. De Cel Screenings zou gebruik kunnen maken van een nieuwe zoekmachine, die moet toelaten om zowel in de databanken als rechtstreeks in documenten in de folderstructuur van de Directie I, opzoekingen te verrichten. Dit kaderde in de verbetering van het algemene informatiebeheer bij de ADIV.

De leden van de Cel Screenings waren niet op de hoogte van eventuele initiatieven met externe partners over het gebruik van gemeenschappelijke technologische middelen. *Qua* externe databanken, heeft de Cel Screenings enkel toegang tot het Rijksregister, en dan enkel nog één personeelslid van de Cel. De Cel

---

25 Het feit dat de beslissingen van het Beroepsorgaan enkel terechtkomen bij de Cel Screenings, en dat zij hiermee niets (kunnen) doen, werd door de Cel reeds aangekaart bij de hiërarchie. Er werd hierrond echter geen actie ondernomen.

26 *'Toezichtonderzoek naar de werking van de Directie Counterintelligence (CI) van de ADIV'.*

Screenings geeft aan dat andere toegangen tot externe databanken niet noodzakelijk zijn.

Een ander probleem is dat aanvragen bij de Cel Screenings terechtkomen in allerhande formaten (Excel-lijsten, pdf-documenten …). Met andere woorden, er is geen gestandaardiseerde *template* in gebruik voor aanvragen tot veiligheidsverificaties.

I.2. DE WERKING VAN DE AFDELING HUMINT BIJ DE MILITAIRE INLICHTINGENDIENST DOORGELICHT

Het beroep doen op menselijke bronnen (*human intelligence* of HUMINT) vormt een essentieel middel voor de inlichtingen- en veiligheidsdiensten in het kader van hun opdracht om informatie te vergaren. De Afdeling HUMINT van de Divisie Intelligence (kortweg Afdeling I/H) heeft als opdracht om netwerken van bronnen en informanten op te richten ten einde de ADIV toe te laten inlichtingen te verzamelen over buitenlandse fenomenen.

Eerder behandelde het Comité een specifieke klacht met betrekking tot de werking van deze afdeling, en meer specifiek over de uitvoering van bepaalde opdrachten in het buitenland.[27] Immers, de Afdeling I/H beschikt over informanten in het buitenland om informatie te verkrijgen over materies in de belangensfeer van de militaire inlichtingendienst. Daarbij werden een aantal dysfuncties aangekaart. Onder meer de opdrachtsomschrijving, het strategisch beheer, de vaardigheden en kwaliteit van het personeel, de *tradecraft* … werden daarbij kritisch bekeken.[28]

In het verlengde van dat klachtonderzoek, besloot het Vast Comité I eind april 2018 om een toezichtonderzoek te openen waarbij de werking van de Afdeling I/H werd doorgelicht. Het rapport werd in november 2019 afgerond.

I.2.1. HUMAN INTELLIGENCE

Artikel 18 W.I&V bepaalt dat '*de inlichtingen- en veiligheidsdiensten […], in het belang van de uitoefening van hun opdrachten, een beroep [kunnen] doen op menselijke bronnen voor het verzamelen van gegevens omtrent gebeurtenissen, voor-*

27 De klacht was tegelijkertijd het voorwerp van een toezichtonderzoek en van een gerechtelijk onderzoek door het federaal parket. Zie VAST COMITÉ I, *Activiteitenverslag 2017*, 4-11 ('Een klacht betreffende drie operaties van de ADIV').

28 Ook in het onderzoek naar de werking van de Directie Counterintelligence (I.6), kwam de Afdeling I/H aan bod: het was immers duidelijk dat er op zijn minst een gevaar bestond dat beide diensten omwille van het ontbreken van duidelijke afspraken en richtlijnen naast elkaar zouden gaan werken.

werpen, groeperingen en natuurlijke personen of rechtspersonen die een belang vertonen voor de uitoefening van hun opdrachten conform de richtlijnen[29] informatie leveren aan een inlichtingen- en veiligheidsdienst, ongeacht het communicatiemiddel, en ook niet binnen het toepassingsgebied vallen van andere artikels van de W.I&V[30], worden beschouwd als menselijke bronnen. Dit omvat personen met zeer uiteenlopende profielen, die zowel eenmalig voor een debriefing, als sporadisch of op zeer regelmatige basis kunnen worden gezien, gedurende korte of lange periodes, ongeacht hun informatiepositie en de gevoeligheid van de informatie die ze overdragen. Het beroep doen op dergelijke bronnen, vormt een gewone methode voor het verzamelen van gegevens.[31]

De NAVO definieerde op zijn beurt HUMINT als "*a category of intelligence derived from information collected and provided by human sources*".[32] HUMINT wordt door de NAVO opgedeeld in drie categorieën.[33] HUMINT wordt als 'open' geclassificeerd als de informatieverzameling wordt uitgevoerd via bronnen die hun ware rol niet verbergen. Als de informatieverzameling wordt uitgevoerd via menselijke bronnen die hun ware functie en doel verbergen, wordt de HUMINT als 'discreet' beschouwd. HUMINT wordt ten slotte als 'clandestien' geclassificeerd voor activiteiten die in het geheim worden uitgevoerd, met name om de bronnen te beschermen.

I.2.2. DE AFDELING I/H VAN DE ADIV DOORGELICHT

I.2.2.1. Collecte-orgaan met personeelstekort

De Afdeling I/H – die geen monopolie heeft over het beheer van menselijke bronnen binnen de militaire inlichtingendienst – vertegenwoordigt slechts een klein deel van het totale personeelsbestand van de Directie Intelligence. Het Comité kon, naast een sterk personeelsverloop (rotatie), voor de jaren 2017-'18 25% nettopersoneelsverlies (uitstroom) vaststellen. Het Comité wees er op dat omwille van de rotatie en de uitstroom bij de Afdeling I/H een aantal risico's inzake disconti-

29 In maart 2019 valideerde de Nationale Veiligheidsraad (NVR) het ontwerp van richtlijn dat door de VSSE en de ADIV gezamenlijk werd voorgesteld. Ingevolge deze validering, heeft de behandeling van menselijke bronnen nu een volledig wettelijk kader, bestaande uit vier niveaus: de organieke Wet, het Nationaal Strategisch Inlichtingenplan (NSIP), de richtlijn van de NVR en interne instructies.

30 Zoals bijv. art. 14 W.I&V waarin wordt gepreciseerd dat de diensten in het kader van hun inlichtingenopdracht een beroep kunnen doen op de gerechtelijke overheden, de ambtenaren en de agenten van de openbare diensten.

31 Dit betekent dat deze methode, op grond van de beginselen van subsidiairiteit en evenredigheid, voorrang moet krijgen op de specifieke of uitzonderlijke methoden (de zgn. BIM-methoden).

32 NATO, *Glossary of terms and definitions (AAP-6)*, ed. 2015.

33 NATO, *Allied Joint Publication (AJP) 2.3. and STANAG 2578*.

nuïteit en kennisverlies bestonden. In januari 2019 constateerde het Vast Comité I dat de Afdeling I/H met een personeelstekort van 22% kampte in vergelijking met de organieke tabel (OT). De personeelssituatie is met andere woorden precair.

Niettemin heeft de Afdeling I/H een netwerk met honderden menselijke bronnen ontwikkeld dat wereldwijd verspreid zit. Zowat de helft van deze bronnen levert inlichtingen over slechts één of twee landen, gemiddeld levert een bron inlichtingen over vijf landen.

I.2.2.2. Aansturing vanop diverse niveaus

Voor HUMINT-activiteiten in het buitenland voorziet het Nationaal Strategisch Inlichtingenplan dat de ADIV, net zoals de VSSE, lijsten opstelt van de landen waarin ze actief zijn op het vlak van HUMINT.[34] Datzelfde plan bepaalt ook hoe het beheer van hun bronnen gecommuniceerd moet worden.

De Directie Intelligence van de ADIV op zijn beurt stelt om de drie jaar een Inlichtingenstuurplan op. Dit plan moet de inlichtingencyclus aansturen en wordt elk jaar bijgewerkt.[35] Op basis hiervan worden er specifieke acties en prioriteiten voor de verzameling en analyse bepaald voor de afdelingen, en dus ook voor de Afdeling I/H. Ook wordt een *'Intel Focus'* opgesteld dat operationele doelstellingen bevat.

Ten slotte wordt elk collecte-orgaan op het terrein, inclusief de Afdeling I/H, verzocht om collecteplannen in te vullen (de zgn. '*Intelligence Collection Plan*s of ICP). De ICP's voor de Afdeling I/H-dienst bevatten concrete vragen voor de bronnen via dewelke informatie kan worden verzameld over diverse dreigingen. Het Comité stelde vast dat de ICP's tal van verschillende specifieke thema's bevatten, wat niet onlogisch is gezien de diversiteit van de geopolitieke contexten. Echter, de ICP's van de andere collecte-organen van de Directie Intelligence zijn niet op dezelfde manier gestructureerd en de periodes waarop de plannen betrekking hebben, werden niet systematisch gepreciseerd. Het Comité was van oordeel dat een standaardisatie en synchronisatie van de collecteplannen alsook het vermijden van conflicten inzake het beheer van de bronnen door de diverse diensten, aan de orde was.

Het overzicht van de bronnen toonde verder aan dat de Afdeling I/H niet volledig aansloot op bepaalde strategische doelstellingen zoals gedefinieerd in het Inlichtingenstuurplan. Ook werd over bepaalde landen informatie verzameld, terwijl ze *ab initio* niet rechtstreeks en onmiddellijk van strategisch belang zijn

---

34 Op basis van die lijsten worden vier categorieën van landen worden opgesteld: landen waarin uitsluitend de ADIV belang stelt, landen waarin uitsluitend de VSSE belang stelt, landen waarin beide belang stellen en niet-prioritaire landen.

35 Het Comité kon weinig verschillen vaststellen tussen het 'Inlichtingenstuurplan 2013-2014' en het 'Inlichtingenstuurplan 2015-2018' Slechts een aantal strategische doelstellingen werd een andere prioriteit toegekend omwille van de gewijzigde geopolitieke context.

voor de Belgische landsverdediging. Deze vaststelling moet – naar luid van de ADIV – worden gezien in het licht van de globale werking van de Directie Intelligence en de ADIV. De Afdeling I/H levert slechts een deel van de informatie voor elk van de relevante landen. Bovendien kan informatie die niet prioritair is voor de Belgische belangen, van bijzonder belang zijn voor een partnerinlichtingendienst en op die wijze de internationale uitwisseling van informatie voeden. Waar het voor België dan misschien moeilijker is om bronnen te rekruteren en beheren voor een land dat de belangstelling opwekt, kan het dan wel genieten van de wederkerigheid binnen de internationale uitwisseling.[36]

I.2.2.3. De betrouwbaarheid van de bron en de geloofwaardigheid van de aangeleverde informatie

Het beheer van de menselijke bronnen vormt een essentiële taak van de Afdeling I/H. Het betreft een reeks processen waarbij bronnen worden 'gespot', benaderd en geëvalueerd (de rekrutering), hun inlichtingen vervolgens worden verwerkt en de bronnen ten slotte worden 'gearchiveerd'. De meerderheid van deze processen maakt het voorwerp uit van interne richtlijnen. De nieuwe directie besloot in 2018 evenwel om de interne richtlijnen volledig te herzien. Het Comité kon vaststellen dat er voor bepaalde processen nog geen richtlijnen bestonden (bijv. de archivering).

Uiteraard dient de betrouwbaarheid van de bron en de geloofwaardigheid van de verkregen informatie periodiek te worden geëvalueerd. Het NAVO-systeem voor de waardering van de bronnen en informatie die ze verzamelen, is opgebouwd als volgt:

Reliability of the source		**Credibility of the information**	
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probably true
C	Fairly reliable	3	Possibly true
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged

Het Vast Comité I diende bij de aanvang van zijn onderzoek vast te stellen dat de betrouwbaarheid voor een aanzienlijk deel van de bronnen niet was bepaald.[37] In

[36] Het rekruteren en beheren van een bron is ten slotte een investering op meerdere jaren. Een bron in een land dat op dit moment slechts van beperkt strategisch belang is, kan in de toekomst cruciaal blijken.

[37] De betrouwbaarheid van de bron wordt niet alleen op basis van zijn prestaties in het verleden bepaald. Ze heeft op zich geen invloed op de geloofwaardigheid van de informatie. Een 'onbetrouwbare bron' kan informatie aanleveren waarvan de geloofwaardigheid als uitstekend wordt bevonden. De betrouwbaarheid van de bronnen in het algemeen zal echter wel de keuzes

de loop van het onderzoek heeft de Afdeling I/H, met resultaat, een proces opgestart om deze situatie recht te zetten: alle bronnen werden geëvalueerd en indien nodig geheroriënteerd, geheractiveerd of gearchiveerd.

De via menselijke bronnen verkregen informatie moet ook worden geëvalueerd. Op twee jaar tijd (2017-2018) werden meerdere duizenden informatiebulletins geproduceerd.[38] Het Comité kon vaststellen dat de analysediensten voor een groot deel van de informatiebulletins geen formele *feedback* gaven. Dat vormde een verontrustende vaststelling voor de inlichtingencyclus; het is immers cruciaal dat de analysediensten de collectediensten nuttig kunnen aansturen om de inlichtingendoelstellingen te bereiken.

I.2.2.4. Het beheer van de dossiers van de bronnen

Voor de dossiers van de bronnen is er zowel een 'papieren' administratief beheer als een elektronisch beheer. Het onderzoek heeft het mogelijk gemaakt om de problemen met het administratieve beheer te duiden en corrigerende maatregelen te bepalen om de vastgestelde tekortkomingen recht te zetten. Het Comité diende evenwel vast te stellen dat in een reeks dossiers echter nog steeds stukken ontbraken (bijv. documenten met betrekking tot het 'verzoek om een bron te benaderen', het 'verslag van de benaderingsfase' of nog, het 'rekruteringsverslag').

I.3. INTERNATIONALE GEGEVENSUITWISSELING OVER *FOREIGN TERRORIST FIGHTERS*

I.3.1. CONTEXTUALISERING

Al in 2016 werd, tijdens een internationale vergadering met verschillende Europese toezichthouders[39], 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*

beïnvloeden die worden gemaakt in het kader van het collecteplan. Daartoe dient *feedback* te worden gegeven tussen de analist en de persoon die de informatie verzamelt, om vervolgens de bron te kunnen evalueren.

38 Zowel de analyse van de inhoud van die inlichtingenbulletins als de evaluatie van hun relevantie voor de strategische doelstellingen, behoorden niet tot het voorwerp van het onderzoek.

39 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.

(FTF[40]). Het lag 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 bestudeerde.

Het opzet van het Belgische luik van het onderzoek bestond 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 was te komen tot een beoordeling over de informatie-uitwisseling en desgevallend tot aanbevelingen om deze te optimaliseren zodat de informatiepositie van de betrokken diensten kon worden verbeterd, zonder dat daarbij de fundamentele rechten van de burger worden uitgehold.

Het eigen onderzoek van het Comité werd opgeschort. Dit had deels te maken met andere, urgente opdrachten – zeker na de terreuraanslagen in Frankrijk en in België – maar eveneens omwille van de wisselwerking met het internationaal project. Hierdoor besloot het Vast Comité I in januari 2019 om het onderzoek af te sluiten met een beknopt eindverslag en niet, zoals gebruikelijk, met een uitgebreid rapport met beschrijvingen, conclusies en aanbevelingen.

I.3.2. ONDERZOEKSRESULTATEN

Het onderzoek toonde in de eerste plaats aan dat de internationale gegevensuitwisseling over *foreign terrorist fighters* tussen inlichtingendiensten zeker vanaf 2015 niet alleen sterk toenam, maar ook van aard veranderde. Waar voorafgaand aan de FTF-problematiek de gegevensuitwisseling vooral een reactief en bilateraal karakter had, won de proactieve en multilaterale uitwisseling steeds meer terrein. Voorbeeld hiervan is de samenwerking binnen de zgn. Counter terrorist Group (CTG)[41] waarin na de aanslagen in Parijs, in 2016 en onder Nederlands voorzitterschap, een permanent operationeel platform (formeel geopend begin 2017) en een gemeenschappelijke database tot stand werd gebracht waarbinnen informatie wordt uitgewisseld over (vermeende) jihadisten. Deze evolutie betekende ook de implementatie van het beginsel van '*need to share*' op internationaal vlak tussen de betrokken landen. Het belang hiervan kan niet worden overschat en deze samenwerking kan de basis vormen voor een algemene en structurele samenwerking van Europese inlichtingendiensten.

---

40 Zoals gedefinieerd in de VN Resolutie 2178 van 24 september 2014: "*Individuals who travel to a State other than their State of residence or nationality for the purpose of perpetration, planning or preparation of, or participating in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict*".

41 De CTG werd opgericht na 9/11, is een gespecialiseerde groep en geldt als informeel overlegorgaan van vnl. EU-landen.

Ook de in hoofdzaak militaire inlichtingendiensten hebben een multilateraal platform opgericht ter coördinatie van hun SIGINT-activiteiten en analyses.

De door het Comité steekproefsgewijs onderzochte uitgewisselde berichten toonden aan dat deze communicaties pertinent, proportioneel en overeenkomstig de wettelijke opdrachten van de diensten waren, maar plaatsvonden buiten het kader van internationale instellingen (EU, VN …) of van formele, juridisch bindende afspraken (zoals bijv. verdragen). Wel diende te worden vastgesteld dat de uitvoering van de Richtlijn van de Nationale Veiligheidsraad van september 2016 in verband met de relaties met buitenlandse inlichtingendiensten geruime vertraging kende.[42] Deze richtlijn geeft uitvoering aan artikel 20 W.I&V dat de internationale samenwerking met buitenlandse diensten nader regelt.

Ten slotte werd gewezen op de steeds complexer wordende regelgeving inzonderheid op internationaal niveau en de uitspraken van internationale rechtsbanken (*soft law*), maar ook op nationaal vlak. Zo dient onder meer te worden onderzocht welke collectemethoden verenigbaar zijn met het nationaal recht of internationale verdagen en dienen de evoluties op vlak van bescherming van persoonsgegevens stringent te worden opgevolgd.

I.4. DE INFORMATIEPOSITIE VAN DE INLICHTINGENDIENSTEN OVER DE PAKISTAANSE KERNWETENSCHAPPER KAHN

Halfweg januari 2018 verschijnt een persartikel[43] over het kernprogramma van Noord-Korea. Daarbij wordt onder meer verwezen naar het Pakistaanse kernwapenprogramma en worden (wijlen) professor Martin Brabers (KU Leuven) alsook Abdul Qadir Khan, de Pakistaanse wetenschapper die eind jaren '60 begin jaren '70 in België verbleef en die wordt beschouwd als de vader van de Pakistaanse kernbom, vernoemd.

Er stelde zich onder meer de vraag of de Belgische inlichtingendiensten deze problematiek destijds hadden opgevolgd. De Begeleidingscommissie van de Kamer gaf de opdracht de thematiek te bestuderen. Begin juli werd het '*toezichtonderzoek*

---

42 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.

43 M. RABAEY, *De Morgen*, 13 januari 2018 ('De Belgische bommen van Kim Jong-un'). Hierin wordt veelvuldig verwezen naar Luc BARBÉ (L. BARBÉ, *België en de bom. De rol van België in de proliferatie van kernwapens*, juni 2012), die een pleidooi houdt voor een breed onafhankelijk wetenschappelijk onderzoek binnen academische middens en bij de VSSE over de nucleaire sector in België.

naar de informatiepositie van de inlichtingendiensten over een Pakistaanse wetenschapper die actief was in het Belgisch academisch milieu, en over zijn hoogtechnologische kennis verworven inzake massavernietigingswapens, die uiteindelijk werden aangewend om nucleaire wapens in Pakistan te ontwikkelen', geïnitieerd.[44]

I.4.1. HET BELGISCHE LUIK VAN HET DOSSIER KAHN

Abdul Qadir Khan had een belangrijke rol in het uitbouwen van het Pakistaanse kernprogramma. Betrokkene studeerde en werkte tussen 1961 en 1975 in Europa waar hij heel wat kennis opdeed die later mogelijks werd aangewend voor de ontwikkeling van de Pakistaanse atoombom. Khan verbleef vooral in Nederland[45], maar studeerde vanaf 1968 in België, om in 1972 te promoveren als doctor in de natuurkunde aan de KU Leuven, en dit met als mentor Prof. Brabers.[46]

Het toezichtonderzoek spitste zich toe op het zogenaamde Belgische luik van het dossier Khan en de vraag óf de Belgische inlichtingendiensten gedurende die periode aandacht hadden geschonken aan de aanwezigheid van betrokkene in België, en aan de mogelijke bedreigingen die hij kon vertegenwoordigen inzake het verspreiden van technologie aangewend om massavernietigingswapens te ontwikkelen.

I.4.2. DE INFORMATIEPOSITIE VAN DE INLICHTINGENDIENSTEN

Voor wat de VSSE betreft, gebeurde de opvolging van Khan en de aan hem verbonden personen of entiteiten zowel vanuit de bedreiging proliferatie als spionage. In de mate waarin kerntechnologie zou (kunnen) worden gebruikt voor de aanmaak en verspreiding van kernwapens, was er op het ogenblik dat de feiten zich afspeelden tevens een voldoende bevoegdheidsgrond voor de opvolging van deze problematiek door de militaire inlichtingendienst. Het Vast Comité I kon dan ook besluiten dat zowel de VSSE als de ADIV – ook vóór de totstandkoming van de Wet van 1998 – bevoegd waren om de problematiek op te volgen.[47]

---

44 Het onderzoek werd begin 2019 afgerond.

45 In 1980 werd in de schoot van de Nederlandse Tweede Kamer een onderzoeksrapport over de affaire-Khan opgesteld (*De Zaak KHAN*, Tweede Kamer 1979-1980, Bijzondere Commissie Ter Beek, Kamerstuknummer 16082). In 1983 werd Khan in Nederland veroordeeld voor spionage (voor feiten daterend van 1974 en 1975), maar hij wordt in 1985 in graad van beroep vrijgesproken.

46 Over betrokkene(n) verscheen al heel wat nationale en internationale literatuur (L. BARBÉ, *o.c.*, 2012; F. DOUGLAS en C. COLLINS, *The Nuclear Jihadist* New York, Twelve, 2007; C. COLLINS en F. DOUGLAS, *De Khan-code. Spionage, falende inlichtingendiensten en de handel in atoomgeheimen*, Balans, 2011; …).

47 In de voorbereidende werken bij de totstandkoming van de Wet van 30 november 1998 en meer bepaald bij de discussies over het takenpakket van de inlichtingendiensten en hun rol in

I.4.2.1. De VSSE

Tijdens de periode 1979-1996 (en dus na het vertrek van Khan uit België) verzamelde de VSSE over Khan en Prof. Brabers om en bij de 100 documenten, in hoofdzaak afkomstig uit open bronnen. Daarnaast ontving de dienst ook meer dan 50 documenten van zijn correspondenten. De VSSE stelde ongeveer 40 rapporten op, naast 20 nota's voor Belgische of buitenlandse correspondenten.

Vanaf 1996 (en dus na de informatiseringsbeweging binnen de VSSE) kon worden vastgesteld dat een twintigtal onderzoeksrapporten (OR's) werden opgesteld.

Het onderzoek stelde een duidelijke toename van informatie-uitwisseling vast vanaf 2004. Het betrof informatierapporten opgesteld door de buitendiensten van de VSSE. Van belang is weliswaar dat deze rapporten vooral aandacht hadden voor de proliferatieproblematiek in Pakistan, waarbij Khan vanzelfsprekend ook prominent genoemd werd. Een twintigtal nota's werden gestuurd naar federale en/of regionale politieke overheden; een aantal synthesenota's waren bestemd voor de directie van de VSSE.[48]

De VSSE meldde dat er geen aanwijzingen waren dat Prof. Brabers een rol zou hebben gespeeld in het verwervingsnetwerk van Khan of actief zou hebben bijgedragen aan de ontwikkeling van de Pakistaanse atoombom. Een actief en regelmatig nazicht van de activiteiten of de contacten van Prof. Brabers vond echter niet plaats.

I.4.2.2. De ADIV

De ADIV beschikte over geen specifieke informatie in zijn verschillende gegevensbanken over de Pakistaanse atoomgeleerde Khan noch over Prof. Brabers-voor de jaren '60 en '70. De dienst bleek naar eigen zeggen heel wat resultaten te detecteren wanneer de naam Khan voor de daaropvolgende periode. Deze resultaten werden evenwel niet verwerkt in zijn antwoord gezien deze geen betrekking hadden op de periode dat Khan in Europa aan het werk was.

---

het kader van het WEP, werd bovendien expliciet verwezen naar het dossier-Khan: *"[…] De economische en wetenschappelijke spionage is in ontwikkeling. Het is echter niet de bedoeling ten dienste te staan van een onderneming maar men moet toch wel weten welke elementen een rol spelen in de activiteit van deze onderneming, en vooral van wie deze activiteit hinder kan ondervinden in het buitenland (zie de Pakistaanse stagiairs – bevoegdheid van de heer Khan inzake burgerlijk gebruik van kernstoffen). Het economisch en wetenschappelijk potentieel grondig kennen en de ontwikkeling ervan ondersteunen kan dus zeer nuttig zijn. Dit vormt zeker het meest moderne onderdeel van de huidige functies van de inlichtingendiensten"*. In: Wetsontwerp houdende regeling van de inlichtingen- en veiligheidsdiensten, *Parl. St.* Senaat 1997 98, nr. 1-758/10, 101.

48 Er werden slechts enkele nota's medegedeeld aan buitenlandse correspondenten gedurende de laatste tien jaar. De VSSE wees erop dat dit coherent is met de afname aan belang van Khan en zijn (toenmalig) verwervingsnetwerk.

I.4.3. CONCLUSIES

Het 'Belgische luik' van de zaak-Kahn speelde zich af in de periode 1968-1972. Beide inlichtingendiensten hadden op dat ogenblik – zij het niet steeds op expliciete wijze – een algemene opdracht inzake voorliggende thematiek.

Of de Belgische diensten een directe aanleiding hadden om Khan op te volgen, is een andere vraag. Immers, het verblijf van Khan in België was relatief kort. Hij viel blijkbaar niet op en was bovendien niet de enige Pakistaanse student die werkzaam was in het domein van kerntechnologie. Ook was het domein waarin hij zijn onderzoek voerde (metallurgie), niet direct verbonden met kernonderzoek. Het gros van zijn kennis deed Khan op in Nederland (vanaf 1972), toen hij daar na zijn doctoraat aan het werk ging bij een onderzoekslaboratorium. Uit het Nederlandse onderzoek (*supra*) bleek dat het ook daar is dat hij gegevens ontvreemde. Dat hij in de kijker van een partnerdienst liep, werd door deze laatsten pas in 1979 aan de VSSE gemeld, toen hij ondertussen reeds zeven jaar uit België weg was.

De Nederlandse Prof. Brabers, die naast aan de universiteit van Tilburg ook aan de KU Leuven doceerde, kwam pas in 1987 onder de aandacht van de VSSE. Er is ten aanzien van hem nooit enig feit inzake hulp aan proliferatie of spionage opgeworpen of hard gemaakt.

Het Vast Comité I was van mening dat, gelet op de beschikbare informatie of indicaties, Khan noch Prof. Brabers de onmiddellijke aandacht van de Belgische inlichtingendiensten hadden moeten trekken of als belangrijk, laat staan prioritair target moesten worden beschouwd. '*In hindsight*' zou weliswaar kunnen gesteld worden dat al wie met kernonderzoek te maken had, zeker de aandacht van de inlichtingendiensten waard was. Vanaf de jaren '80, zo meldde de VSSE, was er meer aandacht voor deze problematiek.

Als eindbeoordeling stelde het Vast Comité I dat het gegeven dat de Belgische inlichtingendiensten zowel Khan tijdens zijn verblijf in België als Prof. Brabers niet prioritair opvolgden niet onredelijk is, rekening houdend met het tijdskader en met de gegevens die er toen maar bekend waren.

I.5. PUIGDEMONT EN DE MOGELIJKE ACTIVITEITEN DOOR BUITENLANDSE INLICHTINGENDIENSTEN IN BELGIË

I.5.1. CONTEXTUALISERING

Op 27 oktober 2017 wordt Carles Puigdemont, voormalig president van de regionale regering van Catalonië die het Catalaanse Parlement de onafhankelijkheid liet uitroepen, ontheven van zijn functies door de Spaanse instellingen. Hij

vluchtte daarop naar België. Begin november 2017 maakt hij het voorwerp uit van een Europees aanhoudingsmandaat dat werd uitgevaardigd door de Spaanse gerechtelijke autoriteiten.

Op 9 februari 2018 diende Puigdemont klacht in bij de Belgische autoriteiten voor schending van zijn privéleven. Enkele dagen daarvoor was er immers een verborgen lokalisatiebaken aangetroffen onderaan zijn voertuig.[49] Nadat ze dit dispositief hadden gevonden, verwittigden de adviseurs van Puigdemont de lokale politiezone van Waterloo. Volgens open bronnen zouden de chauffeurs van Puigdemont, voorafgaand aan de ontdekking van de geolokalisatiebaken, gemerkt hebben dat zij werden geobserveerd. Er werden wagens met Duitse nummerplaten opgemerkt die schaduwoperaties uitvoerden.

Tijdens haar vergadering van 12 juni 2018, verzocht de Begeleidingscommissie het Vast Comité I om een toezichtonderzoek te openen naar de informatiepositie en de reactie van de Belgische inlichtingendiensten met betrekking tot eventuele activiteiten van buitenlandse inlichtingendiensten op het Belgische grondgebied op het ogenblik dat Puigdemont in België verbleef.

I.5.2. JURIDISCHE ASPECTEN

In toepassing van de artikelen 7, 1° en 8, lid 1, 1°, g) W. I&V, heeft de VSSE als opdracht het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de uitwendige veiligheid van de Staat en de internationale betrekkingen bedreigt of zou kunnen bedreigen; activiteiten die resulteren uit spionage (het verzamelen of het verstrekken van niet voor het publiek toegankelijke informatie […]) of inmenging (de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden).

Daarnaast heeft de VSSE in toepassing van de artikelen 7, 1° en 8, lid 1, 2°, a) en b) W.I&V in het bijzonder als opdracht het inwinnen, analyseren en het verwerken van inlichtingen betreffende elke activiteit die de inwendige veiligheid van de staat en het voortbestaan van de democratische en grondwettelijke orde bedreigt of zou kunnen bedreigen; activiteiten die voortkomen uit de schending van de mensenrechten en de fundamentele vrijheden, of van inbreuken op de veiligheid en de fysieke en morele integriteit van personen en op de vrijwaring van eigendom.

Bovendien heeft de VSSE, en dit in toepassing van de artikelen 7, 3°/1 en 11, § 1, 5° W.I&V, sedert januari 2016 als opdracht: het inwinnen, analyseren en ver-

[49] Zie open bronnen: Y.N. met Belga, *La Libre Belgique*, 28 maart 2018 ('Carles Puigdemont porte plainte en Belgique: sa voiture était pistée avec des balises de traçage'). Daarin onder meer: '*les responsables de la sécurité de l'ancien président catalan ont inspecté son véhicule et détecté un dispositif de suivi installé sous sa voiture*'. ('*inspecteerden de veiligheidsverantwoordelijken van de Catalaanse oud-president het voertuig en vonden ze een traceerapparaat dat was bevestigd onderaan de wagen*') *(vrije vertaling).*

werken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied. Eenzelfde opdracht werd in 2016 eveneens toegevoegd voor de ADIV (art. 11, § 1, 5° W.I&V). Het betreft een algemene bevoegdheid waar, bij de uitoefening ervan, geen sprake moet zijn van een bedreiging.

Met het oog op het regelen van de verdeling van de taken voor het inwinnen, analyseren en behandelen van inlichtingen betreffende de activiteiten van buitenlandse inlichtingendiensten op het Belgisch grondgebied, bepaalt artikel 20, § 4 W.I&V dat de VSSE en de ADIV een samenwerkingsakkoord afsluiten op basis van richtlijnen van de Nationale Veiligheidsraad (NVR). Het Vast Comité I heeft geen kennis van een richtlijn van de Nationale Veiligheidsraad noch van een samenwerkingsakkoord afgesloten in toepassing van deze beschikking (noch van een dergelijk ontwerp).[50]

Wat betreft de mededeling van gegevens aan buitenlandse inlichtingen- en veiligheidsdiensten verduidelijkt artikel 19 W.I&V het volgende: "*de inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en aan de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook aan de instanties en personen die het voor zijn van een [dreiging] bedoeld in artikelen 7 en 11*". Hierover vermelden de voorbereidende werkzaamheden inzake artikel 19 W.I&V[51] de mogelijkheid om inlichtingen aan buitenlandse inlichtingen- en veiligheidsdiensten mee te delen.

In diezelfde context stelt artikel 20, § 1 W.I&V dat de Belgische inlichtingendiensten eveneens zorgen voor een doeltreffende samenwerking met de buitenlandse inlichtingen- en veiligheidsdiensten.

Conform artikel 20, lid 3 van diezelfde wet, moeten de voorwaarden van deze samenwerking worden vastgelegd door een richtlijn van de Nationale Veiligheidsraad. Op 26 september 2016 hebben de ministers van Justitie en Defensie een dergelijke nota voorgelegd aan de Nationale Veiligheidsraad.

Om het juridisch kader volledig te schetsen (maar rekening houdend met het feit dat deze beschikkingen nog niet in werking waren getreden in oktober 2017), moet worden verwezen naar de artikelen 92 tot 94 van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Deze artikelen voorzien specifieke regelingen inzake het behandelen van persoonsgegevens door inlichtingen- en veiligheidsdiensten, onder meer op vlak van het meedelen van gegevens aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties.

---

50 Het Strategisch Inlichtingenplan, dat in 2018 werd goedgekeurd door de Nationale Veiligheidsraad, behandelt deze specifieke kwestie slechts op een beknopte wijze (via een tabel). Deze bevoegdheid komt toe aan de twee diensten.

51 *Parl. St.* Kamer, 1995-96, n°49-638/1, 19.

I.5.3. VASTSTELLINGEN

Wat betreft de bevoegdheid van de Belgische inlichtingen- en veiligheidsdiensten

De taakverdeling tussen de VSSE en de ADIV wat betreft het toezicht op buitenlandse inlichtingen- en veiligheidsdiensten op Belgisch grondgebied staat niet vermeld in het Strategisch Inlichtingenplan dat werd goedgekeurd door de Nationale Veiligheidsraad. Evenmin werd er een akkoord afgesloten tussen beide diensten in toepassing van artikel 20, § 4, W.I&V.

Daar waar de VSSE beweerde dat ze niet bevoegd was, wees het Comité er op dat de VSSE en de ADIV sedert januari 2016 als opdracht hebben inlichtingen in te winnen, te analyseren en te verwerken inzake activiteiten van buitenlandse inlichtingendiensten op het Belgisch grondgebied. Het Vast Comité I was van oordeel dat de juridische analyse van de VSSE moest worden bijgestuurd in die zin dat de bepalingen uit artikel 20, § 4, W. I&V moeten worden nageleefd.

Wat betreft de ADIV ondervroeg het Vast Comité I deze dienst over zijn informatiepositie inzake Carles Puigdemont. Had deze dienst bepaalde acties ondernomen in het kader van zijn verblijf in België en/of had de dienst zijn medewerking verleend aan een operatie uitgevoerd door de buitenlandse partnerdienst A? De ADIV antwoordde hierop dat zij over geen enkele informatie beschikte betreffende Puigdemont, dat zij niet heeft meegewerkt met de buitenlandse partnerdienst A in het kader van Puigdemonts verblijf in België en dat, vermits hij geen bedreiging vormde voor de Belgische belangen of voor de NAVO, de dienst geen enkele activiteit lastens betrokkene had ondernomen. In onderhavig geval, rekening houdend met de specifieke bevoegdheidssfeer gekoppeld aan een bedreiging van 'militaire' aard, had de ADIV, wat haar betreft – en terecht – geen redenen om interesse te tonen voor het dossier van Puigdemont.

Wat betreft de evaluatie van het risico gekoppeld aan de eventuele ontwikkeling van inlichtingenactiviteiten en van inmenging begaan door een of meerdere buitenlandse inlichtingen- of veiligheidsdiensten

Rekening houdend met het opzet van het onderzoek, besloot het Vast Comité I dat de VSSE ten onrechte niet overging tot het inwinnen, analyseren en verwerken van informatie betreffende de uitoefening van bepaalde activiteiten op het Belgisch grondgebied door een buitenlandse inlichtingen- en veiligheidsdienst betreffende het verblijf van Carles Puigdemont in België, tussen 2017 en het afsluiten van het toezichtonderzoek.

Er werd geen beroep gedaan aan de hand van een verzoek tot technische bijstand op de VSSE met het oog op het analyseren van de lokalisatie-bakens.

Met een risico dat was ingeschaald als zijnde onwaarschijnlijk en de dreigingsanalyse 'niveau 1' opgesteld door het OCAD, maakte dat Puigdemont geen voor-

werp uitmaakte van operaties van de kant van ADIV noch vanwege de VSSE. In deze context heeft het Vast Comité I vastgesteld dat doorheen de diverse dossiers met betrekking tot de dreigingsevaluatie uitgevoerd door het OCAD inzake de aanwezigheid van Puigdemont, nergens melding werd gemaakt van een risico gekoppeld aan eventuele inlichtingenactiviteiten of inmengingsactiviteiten van één of meerdere buitenlandse inlichtingen- of veiligheidsdiensten. Dit risico valt niet onder de bevoegdheid van het OCAD, maar het komt aan het Vast Comité I in ieder geval toe zich uit te spreken over de aan- of afwezigheid van dergelijke vermelding gekoppeld aan het risico.

Gevraagd naar haar eigen evaluatiemethodologie betreffende de vermelde dreiging (of afwezigheid van dreiging) heeft de VSSE sedert dit dossier de methodologie '*leadfase investigative model*' aangenomen. Dit moet toelaten te beslissen of een dossier moet worden geopend en/of maatregelen moeten worden genomen na een risicoanalyse teneinde de geloofwaardigheid, alsook de mogelijks te ondernemen acties en de proportionaliteit te bepalen. Deze methodologie zal het voorwerp uitmaken van een opvolging bij de VSSE en zal eveneens worden voorgesteld aan de ADIV.

Het Vast Comité I concludeerde dat de aanwezigheid van een dergelijke persoonlijkheid op het Belgisch grondgebied een specifieke formele analyse en evaluatie vereiste door de diensten van de VSSE, in het licht van de specifieke dreigingen die tot haar bevoegdheden behoren en dus niet louter in het licht van dreigingsevaluaties opgesteld door het OCAD, die niet aan dezelfde finaliteit een beantwoorden.

Wat betreft de uitwisseling van informatie

De VSSE heeft persoonsgegevens (die weliswaar hoofdzakelijk afkomstig waren uit open bronnen en/of niet vertrouwelijk waren) meegedeeld aan een buitenlandse Europese inlichtingendienst die als 'betrouwbare' partner werd gekwalificeerd.[52]

Er liepen inderdaad verzoeken tot het meedelen van informatie bij de VSSE binnen, geformuleerd door de buitenlandse partnerdienst A betreffende de verblijfplaats van Puigdemont. Daarop verstrekte de VSSE antwoorden op basis van open bronnen en niet-geclassificeerde politie-informatie. De VSSE heeft de partnerdienst A geen vragen gesteld over de directe aanleiding van deze verzoeken en heeft geen afweging gemaakt tussen het belang van de dienst enerzijds en de belangen van de betrokkenen anderzijds (bijv. het fundamenteel recht op privacy of het recht op vereniging). Deze casus toont voor het Vast Comité I het belang aan van duidelijke regels inzake de informatie-uitwisseling tussen Belgische en buitenlandse inlichtingendiensten.

[52] Hoewel de richtlijn van de Nationale Veiligheidsraad dateert van september 2016, verrichtte de VSSE op 25 november 2015 reeds een analyse (hierbij rekening houdend met de principes zoals uiteengezet in een ontwerp van richtlijn die zij zelf had opgesteld) betreffende haar relaties met de buitenlandse partnerdienst A. Deze dienst werd gekwalificeerd als zijnde een betrouwbare partner. De ADIV had deze richtlijn nog niet geïmplementeerd.

Het Comité betreurde tevens dat de bevoegde minister niet op de hoogte werd gebracht van het verzoek van de buitenlandse partnerdienst A.

Wat betreft de formele overlegmodaliteiten tussen de Belgische inlichtingendiensten en de buitenlandse inlichtingen- en veiligheidsdiensten

Het Vast Comité I stelde vast dat geen formele overlegmodaliteiten werden voorzien tussen de Belgische inlichtingendiensten met één of meerdere buitenlandse inlichtingen- of veiligheidsdiensten of veiligheidsdiensten betreffende Carles Puigdemont. Informele contacten werden opgestart door de buitenlandse partnerdienst A, maar de VSSE heeft daaraan geen gevolg gegeven. Het Vast Comité I onthield zich, wat dit onderdeel betreft, van commentaar.

Wat betreft de reactie van de VSSE betreffende de buitenlandse partnerdienst A en de buitenlandse politiedienst

Het Vast Comité I stelde vast dat op een bepaald ogenblik, de Administrateur-generaal de bilaterale samenwerking met de buitenlandse partnerdienst A – die bepaalde grieven had gericht aan de VSSE – tijdelijk bevroor. De relaties tussen de VSSE en de buitenlandse partnerdienst A zijn kort daarna genormaliseerd, na een onderhoud tussen beide diensthoofden. Uit het dossier bleek niet dat de bevoegde minister werd geïnformeerd over het tijdelijk bevriezen van deze relatie.

Na het ontdekken van de bakens heeft de VSSE ten onrechte geoordeeld dat de politie-informatie – die stelde dat een buitenlandse politiedienst het dossier van Puigdemont opvolgde en dat deze dienst bepaalde vragen formuleerde aan het adres van de Belgische politie betreffende de verplaatsingen van betrokkene – geen bedreiging inhield op het vlak van de uitoefening van inlichtingenactiviteiten van buitenlandse inlichtingen- of veiligheidsdiensten op het Belgisch grondgebied. Het Comité was ook van oordeel dat de informatie, stellende dat een buitenlandse politiedienst het dossier van Carles Puigdemont opvolgde, een formele analyse en specifieke evaluatie door de diensten binnen de VSSE verdiende.

I.6. DE WERKING VAN DE DIRECTIE COUNTERINTELLIGENCE (CI) VAN DE ADIV: OPVOLGING VAN DE AANBEVELINGEN

I.6.1. CONTEXTUALISERING EN OPZET

In uitvoering van artikel 32 W.Toezicht verzocht de minister van Defensie eind december 2016 het Vast Comité I een onderzoek te voeren naar de werking van de Directie Counterintelligence (CI), één van de vier toenmalige directies van de ADIV. Rechtstreekse aanleiding hiervoor was een brief van een belangrijk deel

van het personeel van CI waarin hun bezorgdheid werd geuit over het functioneren van de dienst en de omstandigheden waarin ze hun wettelijke opdrachten dienden te vervullen.

In januari 2017 opende het Vast Comité I zijn toezichtonderzoek[53]; het werd afgerond in februari 2018.[54] Het onderzoek gaf een inkijk in de ernst, de complexiteit en de pluriformiteit van de tekortkomingen binnen de Directie CI. Het Comité stelde voorop dat de nationale veiligheid een sterke en betrouwbare militaire inlichtingendienst vergt. Daarom ook was het Comité ervan overtuigd dat de Directie CI belang had bij een organisatie en sturing die beantwoordt aan de standaarden van een doelmatige (effectieve) en doeltreffende (efficiënte) overheidsdienst. Uit het onderzoek bleek dat aan deze standaarden niet was voldaan.

Het onderzoek naar de werking van de Directie CI gaf aanleiding tot omstandige aanbevelingen.[55] Wat de uitvoeringsdata betreft, werden prioriteiten aangegeven van 'zeer hoog' (te realiseren tegen eind 2018), over 'hoog' (te realiseren tegen eind juni 2019) tot 'gemiddeld' (te realiseren tegen eind december 2019).

Het Vast Comité I opende eind januari 2019 al een opvolgingsonderzoek naar de mate van uitvoering van het geheel van de aanbevelingen zoals geformuleerd in bovenvermelde audit. Eind februari 2019 werd het Vast Comité I door zijn parlementaire Begeleidingscommissie uitgenodigd om hierover van gedachten te wisselen. Dit gebeurde ter voorbereiding van de hoorzitting[56] achter gesloten deuren met het Hoofd van ADIV, de Chef Defensie en toenmalig minister van Defensie, nu bleek dat de problemen bij de militaire inlichtingendienst bleven aanslepen.

I.6.2. OPSTART VAN EEN BUSINESS PROCESS RE-ENGINEERING (BPR)

Als reactie op de audit van de Directie CI, besliste de Chef ADIV begin juni 2018 een *Business Process Re-engineering* (BPR) op te starten.[57] Deze management-

---

53 Eerder voerde het Comité een gelijkaardige audit uit: VAST COMITE I, *Activiteitenverslag 2011*, 7-14 ('II.1. Een audit bij de militaire inlichtingendienst') en 104-107 ('IX.2.1. Aanbevelingen met betrekking tot de audit bij de ADIV').

54 VAST COMITÉ I, *Activiteitenverslag 2018*, 2-17 ('I.1. De werking van de Directie Counterintelligence (CI) van de ADIV').

55 VAST COMITÉ I, *Activiteitenverslag 2018*, 130-134 ('XII.2.1. Diverse aanbevelingen voor de ADIV naar aanleiding van het toezichtonderzoek naar de werking van de Directie Counterintelligence').

56 Bijzondere Commissie belast met de parlementaire begeleiding van de Vaste Comités P en I, Gedachtewisseling met Luitenant-generaal Claude Van de Voorde, Chef ADIV, Generaal Marc Compernol, Chef Defensie, en de vice-eersteminister en minister van Buitenlandse Zaken en Europese Zaken, en van Defensie, belat met Beliris en de Federale Culturele Instellingen, over de toestand bij de Directie Counterintelligence (CI) van ADIV, 18 maart 2019 (vergadering met gesloten deuren).

57 Om deze BPR in goede banen te leiden, werd een 'core team' samengesteld, bestaande uit de Deputy Assistant Chief of Staff, de Civilian en Military Advisors van het Commando van de

techniek moest toelaten de bedrijfsprocessen fundamenteel te herstructureren. Een dergelijke methodologie beoogt, naast een effect op de organisatiestructuur, ook een wijziging van de managementstijl en de organisatiecultuur. Daarbij werd de strategische optie genomen om een reflectie over de antwoorden op de aanbevelingen inzake de werking van de Directie CI, te kaderen in een ruimere oefening met betrekking tot de gehele werking van de ADIV. Het Commando van de ADIV wou immers tegelijkertijd ook rekening houden met de conclusies zoals geformuleerd door de Parlementaire Commissie terroristische aanslagen. Hoewel het Comité de mening was toegedaan dat dit het hervormingsproces van de Directie CI zwaarder zou maken, werd dit als een valabele keuze beschouwd.

Eind oktober 2018 deed zich evenwel een conflict voor tussen het commando van de ADIV en de leidinggevende van de Directie CI. De voorstellen die waren uitgewerkt naar aanleiding van de aanbevelingen in het Auditrapport CI 2018, konden niet verder in de BPR worden geïntegreerd. Daardoor ontstond een situatie waarin de synchronisatie tussen beide verbeteringstrajecten verloren ging (oktober 2018 – januari 2019). Begin februari 2019 werd het commando van CI overgenomen en werd terug aansluiting gezocht bij het algemene BPR-traject.

I.6.3. DE UITVOERING VAN DE AANBEVELINGEN VAN AUDIT 2018: STAND VAN ZAKEN

Het Comité trachtte zich – onder meer op basis van documentair onderzoek en interviews – een beeld te vormen in hoeverre er inzake de aanbevelingen een significante vooruitgang werd gerealiseerd. Uit het onderzoek bleek dat er begin maart 2019 in één derde van de aanbevelingen met zeer hoge prioriteit, een significante vooruitgang werd geboekt; voor de helft van de aanbevelingen was vooruitgang zichtbaar maar onvoldoende om de operationaliteit volledig te herstellen; enkele aanbevelingen werden nog helemaal niet gerealiseerd.

Het Comité kon vaststellen dat:

– de rol van de Directie CI in het kader van de strijd tegen het terrorisme werd uitgeklaard: bij terrorisme van 'burgerlijke' aard neemt de VSSE de leiding. In het kader van een protocol zijn het personeel én de bronnen overgeheveld naar een gemeenschappelijk CounterTerro-platform gehuisvest bij de VSSE. Bij de ADIV werd een 'horizontale' CounterTerro-coördinator aangeduid (afkomstig uit CI) wiens taak werd ingebed in de DISCC, wat de samenwerking intra-ADIV moet verbeteren;
– inzake infrastructuur de zeer penibele toestand van de Directie CI werd opgelost; de dienst kon in maart 2019 verhuizen naar een gerenoveerd gebouw, uitgerust met alle nodige veiligheidsvoorzieningen;

ADIV, twee vertegenwoordigers van de stafdiensten, en de hoofden van de (toenmalige) vijf directies (CI, I, S, Cy, ERO, DISCC) van de ADIV.

– er een betere coördinatie tot stand werd gebracht tussen de Directie CI en de stafdienst 'J6', de ICT-verantwoordelijke van de ADIV. Er kwam een duidelijk aanspreekpunt en er werd een inventaris van de ICT-behoeften opgemaakt.
– er conceptueel werk werd verricht inzake missie en visie, hoewel dit nog moest worden gevalideerd en finaal geformaliseerd. Eenmaal dit gerealiseerd, kunnen op alle niveaus de *intelligence requirements* en *intelligence collection-plans* worden opgemaakt;
– inzake organigram en bepaling van de behoeften aan middelen (personeel) er voorstellen voorlagen, die ook nog moeten worden gevalideerd en geformaliseerd (voorzien in het tweede kwartaal 2019);
– wat betreft de samenwerking tussen de analyse- en collectediensten ook stappen werden gezet; de situatie waarbij er voor bepaalde materies wel collectoren waren maar geen analisten, of omgekeerd, moet daarmee tot het verleden behoren.

Belangrijk is echter wel dat voor sommige aanbevelingen gebleken is dat de Directie CI zelf weinig of geen 'greep' heeft om de zaak vooruit te helpen (en soms de ADIV evenmin) en waarbij de oplossing vooral in handen ligt van andere echelons (bijv. de realisatie van een specialisatie 'inlichtingen').

Het Vast Comité I nam zich voor de uitvoering van de aanbevelingen verder nauwgezet op te volgen.

I.7. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2019 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2019 WERDEN OPGESTART

I.7.1. DE ONDERSTEUNENDE DIENSTEN VAN HET OCAD

Met de Wet van 10 juli 2006 betreffende de analyse van de dreiging werd het Coördinatieorgaan voor de dreigingsanalyse (OCAD) opgericht. Het doel van dit orgaan is de politieke, bestuurlijke en gerechtelijke overheden een zo accuraat mogelijk beeld te geven van de terroristische of extremistische dreiging in of tegen België en hen toe te laten op gepaste wijze te reageren. De kerntaak bestaat er in punctuele of strategische evaluaties te maken. Deze taak berust bij analisten en bij – vanuit de zogenaamde 'ondersteunende diensten' gedetacheerde – experten (art. 2, 2° W.OCAD). De ondersteunende diensten vormen voor het coördinatieorgaan de belangrijkste informatiebron. Het betreft zeer uiteenlopende diensten, elk met een eigen cultuur en grootte.

Eerder, in 2010, voerde het Vast Comité I samen met het Vast Comité P een gemeenschappelijk toezichtonderzoek naar de informatiestromen tussen het OCAD en de ondersteunende diensten, met bijzondere aandacht voor de twee inlichtingendiensten en de Federale en Lokale Politie.[58]

Op de gemeenschappelijke plenaire vergadering van december 2017 werd besloten een toezichtonderzoek te openen naar de 'andere' ondersteunende diensten, te weten de Dienst Vreemdelingenzaken (FOD Binnenlandse Zaken), de FOD Mobiliteit, de FOD Buitenlandse Zaken alsook de Administratie der Douane en Accijnzen (FOD Financiën). Met dit gemeenschappelijk onderzoek wensen de Vaste Comités I en P een *status quaestionis* op te maken van de informatiestroom tussen het OCAD en de overige ondersteunende diensten.

In de loop van 2019 werden diverse onderzoeksverrichtingen uitgevoerd. Eind 2019 werd de laatste hand gelegd aan de rapportage. De parlementaire Begeleidingscommissie, die akte nam van het verslag in 2020, verzocht meteen om een opvolgonderzoek alsook een uitbreiding van de *scope* met de in 2018 toegevoegde steundiensten (de Algemene Directie Crisiscentrum (FOD BIZA), het Directoraat-generaal Penitentiaire Instellingen (FOD JUS), de Dienst Erediensten en Vrijzinnigheid (FOD JUS) en de Algemene Administratie van de Thesaurie (FOD Financiën).[59]

I.7.2. DE TOEPASSING VAN NIEUWE (BIJZONDERE) INLICHTINGENMETHODEN

Met de inwerkingtreding van de Wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (BIM-Wet) in 2010 werden de mogelijkheden voor de ADIV en de VSSE om informatie te verzamelen, aanzienlijk uitgebreid. Sindsdien kunnen de diensten een beroep doen op gewone, specifieke en uitzonderlijke methoden, die een weerspiegeling zou zijn van de mate van intrusiviteit van de maatregelen.[60] Gelet op de tussengekomen wetswijzigingen, werd ondertussen de draagwijdte van een aantal methoden gewijzigd – lees verruimd –, werden sommige 'bijzondere' methoden 'gewone' methoden en werden nieuwe gewone methoden toegevoegd.

Recent kreeg het Comité een aantal controlemogelijkheden bij voor wat betreft sommige 'gewone' methoden, weliswaar voor omzeggens elke methode verschillend geregeld. Het betreft onder meer het toezicht op de identificatie van de

---

58 Hierover VAST COMITÉ I, *Activiteitenverslag 2010*, 46 ('II.12.6. Mededeling van inlichtingen aan het OCAD door de ondersteunende diensten) en meer uitgebreid *Activiteitenverslag 2011*, 25-32 ('II.4. De informatiestromen tussen het OCAD en zijn ondersteunende diensten').

59 KB van 17 augustus 2018 tot uitvoering van art. 2, eerste lid, 2°, g) van de wet van 10 juli 2006 betreffende de analyse van de dreiging, *BS* 12 september 2018.

60 De logica en de gradatie van de methoden staat evenwel onder druk. Hierover: W. VAN LAETHEM, 'Enkele reflecties over tien jaar BIM-controle door het Vast Comité I', in J. VANDERBORGHT, (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, Antwerpen, Intersentia, 2020, 70 e.v..

gebruiker van telecommunicatie (art. 16/2 W.I&V), de toegang tot PNR-gegevens (art. 16/3 W.I&V), de toegang tot politionele camerabeelden (art. 16/4 W.I&V), of nog, de controle voorafgaand aan intercepties, intrusies in een informaticasysteem en de opname van bewegende beelden (art. 44/3 W.I&V).

Het Comité besliste om deze thematiek te bestuderen in zijn in 2019 geopende '*toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten de recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld*'. Het onderzoek wordt in het tweede semester van 2020 afgerond.

I.7.3. BREXIT EN DE RELATIE TUSSEN BELGISCHE EN BRITSE INLICHTINGENDIENSTEN

In juni 2016 werd in het Verenigd Koninkrijk een referendum georganiseerd over de uittreding uit de Europese Unie. Een kleine meerderheid stemde voor de uittreding; enige tijd later startten aanslepende uittredingsonderhandelingen. Uiteindelijk trad het Verenigd Koninkrijk uit de Europese Unie op 31 januari 2020.

Dit proces, dat gemeenzaam bekend geraakte als de 'Brexit', wierp zekere vragen op over de mogelijke gevolgen van de Britse terugtrekking uit de Europese Unie op het vlak van de samenwerking tussen de twee Belgische (en andere Europese) inlichtingendiensten en de drie Britse (burgerlijke) inlichtingendiensten, te weten de *British Security Service* (BSS, ook gekend als MI5), de *Secret Intelligence Service* (SIS, ook gekend als MI6) en het *Government Communications Headquarters* (GCHQ).

Het Vast Comité I opende in mei 2019 een toezichtonderzoek naar de effecten van de Brexit voor de samenwerking tussen de Belgische (VSSE en ADIV) en de Britse inlichtingendiensten. In het bijzonder wenste het Comité na te gaan of er een risico bestond dat de Brexit deze samenwerking in het gedrang zou kunnen brengen. Ook aan de orde was de wijze waarop de Belgische inlichtingendiensten zich hierop voorbereidden.

Op het tijdstip van het voeren van het toezichtonderzoek (oktober – november 2019) was er – omwille van de conflictueuze en onduidelijke situatie in het Verenigd Koninkrijk – geen zekerheid over de *timing* noch over de precieze omstandigheden van de uittreding.[61] Het Comité besteedde aandacht aan de wettelijk basis voor de internationale samenwerking, toetste een aantal hypotheses over de impact van de Brexit en bestudeerde de inschatting door de Belgische inlichtingendiensten over de gevolgen van de Brexit. Het rapport werd gefinaliseerd in de eerste trimester van 2020.

---

61 Verschillende scenario's bleven gedurende een lange tijd mogelijk: een Brexit op basis van het in oktober 2019 onderhandelde akkoord tussen de EU en de Britse regering, een Brexit op basis van een nog te wijzigen akkoord, een Brexit zonder akkoord (de zogenaamde 'no deal'), of zelfs een annulatie van de Brexit na eventuele verkiezingen (of een nieuw referendum) in het Verenigd Koninkrijk.

I.7.4. DE MOGELIJKE INMENGING DOOR BUITENLANDSE DIENSTEN /STATEN BIJ BELGISCHE VERKIEZINGEN

Hoewel in de Verenigde Staten de resultaten van het onderzoek daaromtrent niet volledig publiek werden gemaakt, rezen er sterke vermoedens dat buitenlandse diensten/Staten (meer bepaald de Russische) tijdens de Amerikaanse presidentsverkiezingen van 2016 gepoogd hebben deze verkiezingen te beïnvloeden via cybermiddelen. Ook in Europa, en dus in België, is dit denkbaar.

Met het zicht op de verkiezingen van 26 mei 2019 was dit thema bijzonder actueel.[62] Het houden van open en faire verkiezingen behoort tot de kern van de democratie. Het is de taak van de VSSE om bepaalde bedreigingen tegen de Belgische instellingen in kaart te brengen en de bevoegde autoriteiten hiervan in kennis te stellen. *In casu* kan bijvoorbeeld verwezen worden naar 'inmenging' als bedreiging (artikel 8, 2de lid, g) W.I&V), dit wil zeggen "*de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden*". Inmenging kan verschillende vormen aannemen: desinformatie, gerichte publiciteit via *social media*, maar ook regelrechte cyberaanvallen. Maar ook voor de ADIV, wiens bevoegdheid in onderhavige materie op het eerste zicht minder evident is, bestaan er in deze aanknopingspunten.

Het Comité besloot dan ook begin 2019 een toezichtonderzoek[63] te openen naar de wijze waarop de Belgische inlichtingendiensten reageren (inlichtingen verzamelen, waarschuwingen uitzenden, internationaal samenwerken, eventueel verstoren[64] …) op de mogelijke cyberinmenging door buitenlandse diensten/Staten bij Belgische verkiezingen. De onderzoeksvragen waren daarbij de volgende:

- Hoe kan de bedreiging gekarakteriseerd worden (welke vormen neemt ze aan en welke instrumenten worden gebruikt) en welke zijn de recente precedenten?
- Wat is de juridische context (zowel van het optreden van de Belgische diensten, als de mogelijke internationaalrechtelijke aspecten)?

---

62 Midden oktober 2018 werd over het thema in de aanloop naar de Europese verkiezingen van mei 2019 onder de patronage van de EU een *high—level* conferentie gehouden door de European Political Strategy Center ("Election Interference in the Digital age: building resilience to cyber-enabled Threats"). Zie https://eceuropa.eu/epsc/events/election-interference-digital-age-building-resilience-cyber-enabled-threats-en.

63 Voluit 'Toezichtonderzoek naar de wijze waarop de inlichtingendiensten een mogelijke inmenging van buitenlandse diensten in Belgische verkiezingen opvolgen, de eventuele bedreigingen tegen trachten te gaan, er over rapporteren aan de autoriteiten, en in het bijzonder wat betreft het gevaar van cyberinmenging of cyberaanvallen op dit vlak'.

64 De VSSE ziet ook verstoring ('disruption') als deel van haar takenpakket. Verstoring betekent dat een inlichtingendienst niet alleen discreet inlichtingenoperaties uitvoert, maar eventueel ook poogt de bedreigingen die ze op het spoor zijn actief tegen te gaan via allerlei middelen (bijv. in het openbaar brengen ervan; cf. de reactie van de Nederlandse AIVD nadat bleek dat de Russische GRU gepoogd had een internationale instelling in Den Haag te *hacken*).

– Welke zijn de verschillende actoren in België die bij deze problematiek betrokken zijn (inlichtingendiensten, OCAD, Cybersecuritycenter …) en wat is de bevoegdheidsverdeling?

Het onderzoeksrapport werd begin 2020 goedgekeurd.

I.7.5. DE OPVOLGING VAN EXTREEMRECHTS DOOR DE BELGISCHE INLICHTINGENDIENSTEN

Uit diverse bronnen blijkt dat extreemrechtse groepen en bewegingen in Europa een stevige voet aan de grond hebben en hun invloed aan het uitbreiden zijn. De voorbije jaren vonden er ook een aantal aanslagen, aanvallen en (geplande) gewelddaden plaats, die aan rechts-extremisten werden toegeschreven. Ook in België vonden enkele dergelijke gebeurtenissen plaats. Het Vast Comité I besloot dan ook in mei 2019 om een toezichtonderzoek te openen naar de wijze waarop de inlichtingendiensten de bedreiging die uitgaat van het fenomeen extreemrechts heden ten dage in België opvolgen en erover rapporteren aan de autoriteiten. Het Comité wenst te onderzoeken of en hoe de inlichtingendiensten werk maken van hun wettelijke opdracht om het extremisme, en meer bepaald het extreemrechts extremisme in België, op te volgen. De onderzoeksvragen werden als volgt omschreven:

– Hoe definiëren de inlichtingendiensten het fenomeen 'extreemrechts': hanteren de VSSE en de ADIV een definitie om extreemrechts af te bakenen en er hun aandacht op te richten? Wordt er door de Belgische inlichtingen- en veiligheidsdiensten een gemeenschappelijke definitie gehanteerd in het kader van het Plan Radicalisme? Kaderen deze definities in de wettelijke context?
– Wat is de juridische context? Welke zijn de instructies van de bevoegde ministers, de Nationale Veiligheidsraad of andere instanties?
– Kunnen de inlichtingendiensten het fenomeen contextualiseren en kwantificeren? Welke vorm en plaats neemt extreemrechts in België?
– Hoe volgen de diensten het fenomeen op? Hoe wordt bepaald welke groeperingen en situaties het voorwerp uitmaken van actieve opvolging? Hoe zijn de diensten georganiseerd om deze opvolging uit te voeren? Welke prioriteiten werden er gelegd? Welke middelen worden ingezet (personeel, methoden …) en methoden worden gebruikt (gewone methoden, bijzondere inlichtingenmethoden …)? Welke inschattingen worden er gedaan (analyse), hoe wordt daarover gerapporteerd naar de autoriteiten en wat is de *feedback* hierover?

In de loop van 2019 werden diverse onderzoeksdaden gesteld. Het onderzoek wordt verder gezet in 2020.

I.7.6. INFORMATIE- EN COMMUNICATIE-TECHNOLOGIE IN HET INLICHTINGENPROCES

Informatie- en communicatietechnologieën (ICT) spelen een steeds belangrijkere rol in de inlichtingenprocessen, zowel bij het verzamelen en de analyse van de basisinformatie als bij de verspreiding van de inlichtingen. Informatie kan afkomstig zijn van menselijke bronnen (HUMINT), van partners of van digitale bronnen zoals '*open sources*' (OSINT), afluisteroperaties (SIGINT), beeldmateriaal (GEOINT) … De constante groei van de gegevensstromen vereist passende systemen die geschikt zijn om die stromen te absorberen en om een correcte, snelle en doeltreffende analyse mogelijk maken. De informatica-omgeving moet dus een stabiele en toekomstgerichte *tool* zijn die ondersteuning kan bieden aan de verschillende actoren die een rol spelen in de inlichtingencyclus. Deze omgeving, zowel de *hardware* als de *software*, moet beantwoorden aan de normen ter zake en de goede ICT-praktijken, en moet tegelijk rekening houden met de nieuwe en toekomstige technologische ontwikkelingen[65], zoals bijv. '*big data*'.[66]

In eerdere onderzoeken stelde het Vast Comité I vast dat de inlichtingendiensten het hoofd moeten bieden aan grote uitdagingen in dit domein. Vooral wat betreft de ADIV is in het verleden al gebleken dat ICT een teer punt is. Het Comité stelde vast dat de inlichtingenactiviteiten niet (langer) voldoende werden ondersteund door ICT. De voorwaarden voor een goed beheer van de informatie werden niet (langer) volledig vervuld.[67, 68]

In mei 2019 deelde het Vast Comité I aan de Kamervoorzitter de opstart van het '*Toezichtonderzoek betreffende de informaticamiddelen die de Belgische inlichtingendiensten gebruiken om informatie te verzamelen, te analyseren en te communiceren in het kader van de inlichtingencyclus*' mee. De draagwijdte van het onderzoek werd bij de start duidelijk afgebakend. Het onderzoek spitst zich toe op de informaticamiddelen die specifiek worden gebruikt ter ondersteuning van de elementen van de inlichtingencyclus. Het gaat om de systemen die bijvoorbeeld

---

65 De toezichtsorganen vervullen in dit verband ook een belangrijke rol. Zie in dit verband: K. VIETH en T. WETZLING, *Data-driven Intelligence Oversight. Recommendations for a System Update*, StiftungNeueVerantwortung, november 2019, 63 p.

66 Het begrip '*big data*' verwijst naar de wetenschap van het verzamelen en analyseren van grote volumes gegevens met als doel bepaalde interessante '*patterns*' te ontdekken op basis van een rangschikking ('*clustering*') en statistische analyses die zo hulp kunnen bieden bij de besluitvorming. Deze gegevens worden gewoonlijk gekenmerkt door een grote verscheidenheid, een grote snelheid en een groot volume.

67 VAST COMITÉ I, *Activiteitenverslag 2011*, 7-14 ('II.1. Een audit bij de militaire inlichtingendienst'); *Activiteitenverslag 2018*, 2-18 ('I.1. De werking van de Directie Counterintelligence (CI) van de ADIV').

68 Ook werd in het verslag van de parlementaire onderzoekscommissie naar de aanslagen in Zaventem en Maalbeek de aanbeveling geformuleerd om het informatiebeheer van de diensten te verbeteren om meer bepaald de 'infobesitas' onder controle te houden. Zie 'Onderzoekscommissie naar de terroristische aanslagen van 22 maart 2016. *Parl. St.* Kamer, 2016-2017, nr. 54-1752/008, 15 juni 2017, p. 53 en 180 e.v.

worden gebruikt om gegevens te verzamelen of ook om specifieke analysetools en databanken.[69] Het Vast Comité I voert geen onderzoek naar de (generieke/standaard) faciliteiten inzake kantoorautomatisering die de diensten gebruiken (bijv. Windows, Word, Excel …), voor zover ze niet specifiek zijn voor de inlichtingendiensten. Het Comité voert evenmin een gedetailleerd onderzoek naar het informaticamateriaal (*hardware*) waarover de diensten beschikken, tenzij het specifiek is voor de inlichtingendiensten. Het onderzoek heeft tot doel de risico's te identificeren waarmee de diensten te maken krijgen en die risico's te verminderen door gepaste aanbevelingen te formuleren.

Een eerste module (ADIV) werd halfweg 2020 afgewerkt. De resultaten van het onderzoek bij de VSSE worden ingewacht begin 2021.

I.7.7. DE OPVOLGING VAN VRIJGELATEN TERRO-VEROORDEELDEN DOOR DE VSSE

In België zijn er sinds 2015 zowat 400 personen veroordeeld voor terroristische misdrijven.[70] Sommigen onder hen werden veroordeeld bij verstek, en konden dus ook niet in hechtenis worden genomen. Een aantal van die veroordeelden hebben inmiddels hun straf in de gevangenis uitgezeten of werden, na beslissing van de strafuitvoeringsrechtbank, voorwaardelijk (voor het strafeinde) vrijgelaten.

Een informaticasysteem (SIDIS Suite[71]) van het gevangeniswezen zorgt ervoor dat telkens een geradicaliseerde gedetineerde de gevangenis verlaat, een aantal instanties (VSSE, Federale Politie …) hiervan op de hoogte worden gebracht. Halfweg 2019 besliste het Comité een toezichtonderzoek te openen naar '*de wijze waarop de Belgische inlichtingen- en veiligheidsdiensten de opvolging verzekeren van enerzijds personen die in België verdacht worden van terroristische misdrijven die in België of elders zijn gepleegd en die genieten van een maatregel bedoeld in de Wet van 20 juli 1990 en anderzijds personen, die in België veroordeeld zijn voor terroristische misdrijven en die de Belgische gevangenis verlaten in het kader van één van de maatregelen bedoeld in de Wet van 17 mei 2006, hetzij die definitief vrijgelaten werden (art. 71 van genoemde wet)*'.

---

69 Bij de ADIV worden deze systemen *'weapon systems'* genoemd – naar analogie met bijvoorbeeld systemen die zijn geïntegreerd in de defensieplatformen bij Landsverdediging (bv. de software voor de radarsystemen of '*battle management'*).

70 Samengevoegde vragen aan de minister van Justitie over 'de vrijlating van terroristen' (*Hand.* Kamer 2019-20, 4 juni 2020, CRIV55COM043, 16, VR. nr 550000781P en 550000786P).

71 De databank SIDIS Suite verwerkt de gegevens van personen aan wie een vrijheidsstraf, een vrijheidsbenemende maatregel (voorlopige hechtenis) of een internering werd opgelegd en die daartoe in een gevangenis, een inrichting of een afdeling tot bescherming van de maatschappij (internering) of een gemeenschapscentrum voor minderjarigen verblijven. SDIS Suite maakt de noodzakelijke informatie-uitwisseling en gegevensstromen tussen die overheden mogelijk.

I.7.8. HET RISICO OP INFILTRATIE BIJ DE TWEE INLICHTINGENDIENSTEN

Afgelopen jaren werd de internationale inlichtingenwereld opgeschrikt door een aantal cases van infiltratie (en *insider threat*). Het Comité nam in 2019 het initiatief een toezichtonderzoek op te starten naar de wijze waarop de twee inlichtingendiensten met het risico op infiltratie omgaan: welke risico's worden onderkend, welke tegenmaatregelen worden genomen om ze te beheersen en om er op te reageren indien ze zich voordoen.

Er vonden diverse werkvergaderingen met de ADIV en de VSSE plaats over de thematiek 'cartografie en risico-evaluatie van infiltratie in de schoot van de inlichtingendiensten'. Het proces van risicomanagement zoals hernomen in de ISO 31000-norm vormde daarbij de vertrekbasis.[72]

[72] www.iso.org:fr/iso-31000-risk-management.html.

HOOFDSTUK II
DE CONTROLE OP DE BIJZONDERE EN BEPAALDE GEWONE INLICHTINGENMETHODEN

Dit hoofdstuk bevat cijfermateriaal over de inzet door enerzijds de Veiligheid van de Staat (VSSE) en anderzijds de Algemene Dienst Inlichting en Veiligheid (ADIV) van de specifieke en de uitzonderlijke methoden (de zgn. 'bijzondere methoden') en van de gewone methoden waarin aan het Comité een specifieke opdracht werd toegekend. Tevens wordt verslag gedaan over de wijze waarop het Vast Comité I zijn jurisdictionele controletaak op deze methoden heeft waargenomen. Naast een aantal cijfers over het aantal beslissingen en de wijze waarop het Comité werd gevat, wordt de essentie weergegeven van de jurisprudentie van het Vast Comité I. De rechtspraak werd ontdaan van operationele gegevens; alleen die elementen die van belang zijn voor het juridische vraagstuk, worden opgenomen.

II.1. CIJFERS MET BETREKKING TOT DE BIJZONDERE EN BEPAALDE GEWONE METHODEN

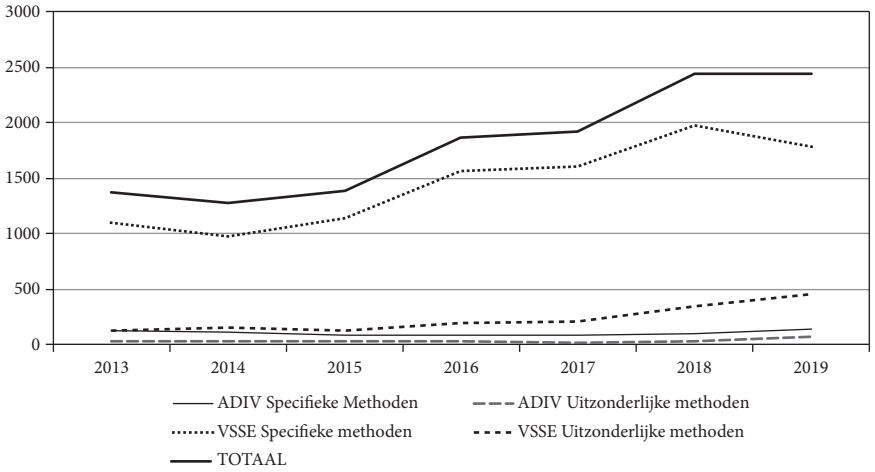
Tussen 1 januari en 31 december 2019 werden door de twee inlichtingendiensten samen 2444 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 2230 door de VSSE (waarvan 1781 specifieke en 449 uitzonderlijke) en 214 door de ADIV (waarvan 138 specifieke en 76 uitzonderlijke).

Onderstaande tabel maakt een vergelijking met de cijfers van de afgelopen jaren.

	ADIV		VSSE		TOTAAL
	Specifieke Methoden	**Uitzonderlijke methoden**	**Specifieke methoden**	**Uitzonderlijke methoden**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445
2019	138	76	1781	449	2444

Dit kan als volgt grafisch worden weergegeven:

Overzicht aantal ingezette BIM's doorheen de jaren (2013-2019)



Na een constante stijging van het aantal ingezette BIM's de afgelopen jaren, kan voor het eerst een stagnatie worden opgetekend: het totale aantal ingezette methoden bleef in 2019 stabiel tegenover 2018. Let wel, per toegelaten methode kunnen wel meerdere targets (zoals personen, organisaties, plaatsen, voorwerpen, communicatie-middelen …) worden geviseerd.

De VSSE blijft het leeuwendeel van de ingezette methoden voor zijn rekening nemen (91,2%).

Als deze cijfers evenwel worden uitgesplitst, kan een opmerkelijke stijging bij de ADIV worden opgetekend van zowel specifieke (van 102 naar 138) als uitzonderlijke (van 28 naar een meer dan verdubbeling 76) ingezette methoden. De VSSE laat een opmerkelijke stijging optekenen van het aantal ingezette uitzonderlijke methoden (van 344 naar 449). Dat ondanks al deze stijgingen een stagnatie in het geheel werd waargenomen, is te wijten aan het sterk gedaalde aantal (van 1971 naar 1781) ingezette specifieke methoden voor de jaargang 2019. Het Comité

beperkt zich in deze tot de weergave van brute cijfergegevens en onthoudt zich van commentaren. Het Comité beoogt om de diensten hieromtrent te bevragen teneinde de weergegeven cijfers op verantwoorde wijze te kunnen duiden.

Wat betreft de gewone methoden van vorderingen gericht aan operatoren om bepaalde communicatiemiddelen te identificeren betreft, wordt – in tegenstelling tot de afgelopen jaren – een daling van ca. 12% opgetekend (60 vorderingen minder bij de ADIV in vergelijking met 2018, tegenover meer dan 800 vorderingen minder door de VSSE).

	Vorderingen door ADIV	**Vorderingen door VSSE**
2016	216	2203
2017	257	4327
2018	502	6482
2019	442	5674

Het Comité stelde reeds eerder[73] dat het "*niet om de vaststelling heen [kon] dat er sinds de invoering van de versoepelde procedure ex artikel 16/2 W.I&V veel meer identificaties worden verricht*". Hoewel het aantal vorderingen afnam in 2019, blijft dit een vrij omvangrijk aantal. Vanuit zijn algemene toezichtsbevoegdheid onderzocht het Comité de redenen hiertoe; de resultaten werden opgenomen in zijn in 2019 geopende *'toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten die recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld'* (cf. I.7.2).

II.1.1. METHODEN AANGEWEND DOOR DE ADIV

II.1.1.1. Gewone methoden

Identificatie van de gebruiker van telecommunicatie

De identificatie van de gebruiker van telecommunicatie (bijv. gsm-nummer of IP-adres) of van een gebruikt communicatiemiddel wordt 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.[74] De regeling voorziet in een verplichting voor de VSSE en de ADIV om een register bij te hou-

73 VAST COMITÉ I, *Activiteitenverslag 2017*, 42.

74 Voorheen vormde dit een specifieke methode. De wijziging gebeurde door de invoeging van een nieuw artikel 16/2 in de Wet van 30 november 1998. Wanneer de identificatie met behulp van een technisch middel verloopt (en dus niet via de vordering aan een operator) blijft de collecte een specifieke methode (art. 18/7 § 1 W.I&V).

den van alle gevorderde identificaties en van alle via rechtstreekse toegang verkregen identificaties. Er werd ook bepaald dat het Comité maandelijks een lijst van de gevorderde identificaties en van elke toegang moet ontvangen. In de praktijk kreeg het Comité maandelijks alleen het aantal vorderingen.[75] Deze thematiek vormde ook het voorwerp van het in 2019 geopende toezichtonderzoek (*supra*).

Identificatie van prepaid-kaarthouder

De VSSE en de ADIV moeten – net zoals bij de identificatie van de gebruiker van telecommunicatie of van een gebruikt communicatiemiddel – een register bijhouden van alle gevorderde identificaties van een andere, sinds 2016, ingevoerde gewone methode. Artikel 16/2 W.I&V vermeldt immers: '§ 2. *De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een bank of financiële instelling om over te gaan tot het identificeren van de eindgebruiker van de in artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie bedoelde voorafbetaalde kaart, op basis van de referentie van een elektronische banktransactie die verband houdt met de voorafbetaalde kaart en die voorafgaand meegedeeld is door een operator of verstrekker in toepassing van paragraaf 1.*' Net als in 2018 werd hier door de beide inlichtingendiensten geen gebruik van gemaakt.

Toegang tot PNR-gegevens

Begin 2017[76] werd de mogelijkheid ingebouwd voor de inlichtingendiensten om toegang te krijgen tot informatie die berust bij de Passagiersinformatie-eenheid en dit bij wijze van gerichte opzoekingen (art. 16/3 W.I&V en art. 27 PNR-wet van 25 december 2016). Het Comité wordt in kennis gesteld van de aanwending van deze methode en kan ze desgevallend verbieden.[77]

De PNR-regeling laat ook toe een zgn. 'voorafgaande beoordeling' te doen waarbij ingevoerde PNR-gegevens automatisch afgetoetst worden aan namenlijsten of bestanden van de inlichtingendiensten en waarbij informatie op basis van gevalideerde hits wordt doorgezonden (art. 24 PNR-wet).

75 In de loop van 2020 werd deze situatie geregulariseerd.

76 Wet van 25 december 2016 (*BS* 25 januari 2017).

77 Anders dan voor de methoden opgenomen in artikel 16/2 W.I&V werd niet voorzien in een verplichte verslaggeving aan het Parlement; artikel 35 § 2 W.Toezicht werd immers niet aangepast. Op suggestie van de Begeleidingscommissie besliste het Comité om deze cijfers mee op te nemen in zijn jaarlijkse verslaggeving en niet te wachten op een eventuele wetswijziging. Pas in 2020 werden de eerste twee stopzettingen bevolen.

Gebruik van politionele camerabeelden

Bij Wet van 21 maart 2018 (*BS* 16 april 2018) werd de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten aangepast om de inlichtingendiensten toe te laten gebruik te maken van politionele camerabeelden. Daartoe werd er een nieuwe gewone observatiemethode ingevoerd (art. 16/4 W.I&V).[78] Bij gebrek aan een uitvoeringsbesluit is deze bepaling nog niet in werking getreden.[79]

De cijfers

Gewone methoden (ADIV)	**Aantal toelatingen**
Identificatie van de gebruiker van telecommunicatie	442
Identificatie van prepaid-kaarthouder	0
Gerichte opzoekingen PNR-gegevens	In 2018 18 nu 38
Doorgifte PNR-gegevens o.b.v. hits	Niet aangeleverd
Gebruik van politionele camerabeelden	Niet in werking

II.1.1.2. De specifieke methoden

Onderstaande tabel geeft de cijfers weer over de toepassing van de specifieke methoden door de ADIV. Er worden daarbij zeven specifieke methoden onderscheiden.

Specifieke methoden (ADIV)	**Aantal toelatingen**
Observeren in publiek toegankelijke plaatsen met een technisch middel of al dan niet met behulp van een technisch middel observeren in een niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is (art. 18/4 W.I&V)[80]	12
Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (art. 18/5 W.I&V)	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	0
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	0

78 Bij dezelfde wet werd de bestaande specifieke en uitzonderlijke observatiemogelijkheid uitgebreid (artt. 18/4 § 3 en 18/11 § 3 W.I&V).

79 Begin 2019 keurde de Ministerraad ter zake een ontwerp van koninklijk besluit goed. Het werd aan het advies van het Vast Comité I voorgelegd. Dit advies 002/VCI-BTA/2019 van 9 april 2019 is te consulteren op de website van het Comité (www.comiteri.be).

80 Bij Wet van 21 maart 2018 (*BS* 16 april 2018) werd een nieuwe paragraaf toegevoegd aan art. 18/4 W.I&V om de inlichtingendiensten toe te laten gebruik te maken van politionele camerabeelden om *real time*-observaties uit te voeren. Deze methode, die een rechtstreekse toegang vereist tot de bedoelde informatie, werd nog niet geoperationaliseerd.

Specifieke methoden (ADIV)	Aantal toelatingen
Identificatie met behulp van een technisch middel, van de elektronische communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt en de vordering van de operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst tot het bekomen van de gegevens betreffende de betalingswijze, de identificatie van het betalingsmiddel en het tijdstip van betaling voor het abonnement of voor het gebruik van de elektronische communicatiedienst (art. 18/7 W.I&V;)	0
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8 W.I&V)	63
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator (art. 18/8 W.I&V)	63
TOTAAL	**138**

II.1.1.3. De uitzonderlijke methoden

De ADIV kan in het kader van zijn opdrachten bedoeld in de artikelen 11, § 1, 1° tot 3° en 5°, en § 2 W.I&V diverse uitzonderlijke methoden machtigen:

Uitzonderlijke methoden (ADIV)	Aantal toelatingen
Al dan niet met behulp van technische middelen, observeren in niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en betreden van al dan niet aan het zicht onttrokken niet voor het publiek toegankelijke plaatsen om te observeren, een technisch middel te installeren, een voorwerp te openen of mee te nemen (art. 18/11 W.I&V)[81]	3
Al dan niet met behulp van technische middelen niet voor het publiek toegankelijke plaatsen doorzoeken, evenals al dan niet vergrendelde voorwerpen die zich daar bevinden (art. 18/12 W.I&V)	3
Een rechtspersoon als bedoeld in art. 13/3 § 1 W.I&V inzetten om gegevens te verzamelen (art. 18/13 W.I&V)	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	2
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	20
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	8
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	40
TOTAAL	**76**

[81] Bij Wet van 21 maart 2018 (*BS* 16 april 2018) werd een nieuwe paragraaf toegevoegd aan art. 18/11 W.I&V om de inlichtingendiensten toe te laten gebruik te maken van politionele camerabeelden om real time-observaties uit te voeren. Deze methode, die een rechtstreekse toegang vereist tot de bedoelde informatie, werd nog niet geoperationaliseerd.

II.1.1.4. De opdrachten en de dreigingen die de inzet van de gewone en bijzondere methoden rechtvaardigen[82]

De ADIV mag de specifieke en uitzonderlijke methoden aanwenden in het kader van vier opdrachten daarbij rekening houdend met verschillende dreigingen.

1. **De inlichtingenopdracht (art. 11, 1° W.I&V)**
   Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties.
   Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die volgende belangen bedreigt of zou kunnen bedreigen:
   - de onschendbaarheid van het nationaal grondgebied of het voortbestaan van de gehele of een deel van de bevolking;
   - de militaire defensieplannen;
   - het wetenschappelijk en economisch potentieel op vlak van defensie;
   - de vervulling van de opdrachten van de strijdkrachten;
   - de veiligheid van de Belgische onderdanen in het buitenland.
2. **De zorg voor het behoud van de militaire veiligheid (art. 11, 2° W.I&V)**
   - de militaire veiligheid van het personeel dat onder de minister van Landsverdediging ressorteert;
   - de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen;
   - in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten.
3. **De bescherming van geheimen (art. 11, 3° W.I&V)**
   Het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de minister van Landsverdediging beheert.
4. **Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied (art. 11, 5° W.I&V).**

---

82 Per toelating kunnen meerdere opdrachten en dreigingen aan de orde zijn.

Deze methoden kunnen dus niet ingezet worden in het kader van veiligheidsonderzoeken of andere door bijzondere wetten aan de ADIV toevertrouwde opdrachten (bijv. het verrichten van veiligheidsverificaties voor kandidaat-militairen). Wel is de inzet van bijzondere methoden sinds de inwerkingtreding van de Wet van 30 maart 2017 niet meer beperkt tot het Belgische grondgebied (art. 18/1, 2° W.I&V). De praktijk wijst uit dat per toelating verschillende dreigingen aan de orde kunnen zijn.

Twee derden van de specifieke en uitzonderlijke methoden worden door de ADIV aangewend in het kader van de opdracht 'inwinnen, analyseren en verwerken van inlichtingen van activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied' (art. 11, 5° W.I&V). Toch mag hier niet uit worden afgeleid dat de ADIV sinds 2017 een 'nieuwe soort' dreiging opvolgt; de opvolging van buitenlandse diensten werd voorheen immers sneller aangeknoopt bij de 'inlichtingenopdracht' in het kader van de strijd tegen 'spionage'.

AARD DREIGING	AANTAL 2019
Spionage	165
Terrorisme en radicaliseringsproces)	6
Extremisme	5
Inmenging	38
Criminele organisatie	–
Andere	–
Totaal	214

Anders dan voor de inzet van bijzondere methoden, beschikt het Comité niet over de cijfers met betrekking tot de geviseerde dreiging en de te verdedigen belangen wat betreft de in dit hoofdstuk bedoelde gewone methoden. In zijn vorig activiteitenverslag beveelde het Comité de diensten aan ook deze gegevens te registreren en ter beschikking te stellen.[83] Dit gebeurde vooralsnog niet; het Comité herhaalt in dat kader dan ook zijn eerder geformuleerde aanbeveling.

II.1.2. METHODEN AANGEWEND DOOR DE VSSE

II.1.2.1. De gewone methoden

Gewone methoden (VSSE)	Aantal toelatingen
Identificatie van de gebruiker van telecommunicatie	5674
Identificatie van prepaid-kaarthouder	0
Gerichte opzoekingen PNR-gegevens)	27
Doorgifte PNR-gegevens o.b.v. hits	Niet aangeleverd
Gebruik van politionele camerabeelden	Niet in werking

[83] VAST COMITÉ I, *Activiteitenverslag 2017*, 43.

Zoals gezegd, zal het Comité de wijze waarop deze methode wordt ingezet, nader onderzoeken in zijn in 2019 opgestart toezichtonderzoek.

II.1.2.2. De specifieke methoden

Specifieke methoden (VSSE)	**Aantal toelatingen**
Observeren in publiek toegankelijke plaatsen met een technisch middel of al dan niet met behulp van een technisch middel observeren in een niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is (art. 18/4 W.I&V)	311
Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (art. 18/5 W.I&V)	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	0
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	48
Identificatie met behulp van een technisch middel, van de elektronische communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt en de vordering van de operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst tot het bekomen van de gegevens betreffende de betalingswijze, de identificatie van het betalingsmiddel en het tijdstip van betaling voor het abonnement of voor het gebruik van de elektronische communicatiedienst (art. 18/7 W.I&V;)	50
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8 W.I&V)	700
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator (art. 18/8 W.I&V)	672
TOTAAL	**1781**

II.1.2.3. De uitzonderlijke methoden

Uitzonderlijke methoden (VSSE)	**Aantal toelatingen**
Al dan niet met behulp van technische middelen, observeren in niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en betreden van al dan niet aan het zicht onttrokken niet voor het publiek toegankelijke plaatsen om te observeren, een technisch middel te installeren, een voorwerp te openen of mee te nemen (art. 18/11 W.I&V)	26
Al dan niet met behulp van technische middelen niet voor het publiek toegankelijke plaatsen doorzoeken, evenals al dan niet vergrendelde voorwerpen die zich daar bevinden (art. 18/12 W.I&V)	13
Een rechtspersoon als bedoeld in art. 13/3 § 1 W.I&V inzetten om gegevens te verzamelen (art. 18/13 W.I&V)	0

Uitzonderlijke methoden (VSSE)	Aantal toelatingen
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	12
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	95
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	48
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	255
TOTAAL	**449**

II.1.2.4. De opdrachten en de dreigingen die de inzet van de gewone en 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 wet hanteert volgende definities:

1. Spionage: het opzoeken of het verstrekken van inlichtingen die voor het publiek niet toegankelijk zijn en het onderhouden van geheime verstandhoudingen die deze handelingen kunnen voorbereiden of vergemakkelijken;
2. Terrorisme: het gebruik van geweld tegen personen of materiële belangen om ideologische of politieke redenen met het doel zijn doelstellingen door middel van terreur, intimidatie of bedreigingen te bereiken;
   Radicaliseringproces: een proces waarbij een individu of een groep van individuen op dusdanige wijze wordt beïnvloed dat dit individu of deze groep van individuen mentaal gevormd wordt of bereid is tot het plegen van terroristische handelingen
3. Extremisme: racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat;
4. Proliferatie: de handel of de transacties betreffende materialen, producten, goederen of knowhow die kunnen bijdragen tot de productie of de ontwikkeling van non-conventionele of zeer geavanceerde wapensystemen. In dit verband worden onder meer bedoeld de ontwikkeling van nucleaire, chemische en biologische wapenprogramma's, de daaraan verbonden transmissiesystemen, alsook de personen, structuren of landen die daarbij betrokken zijn;
5. Schadelijke sektarische organisaties: elke groep met filosofische of religieuze inslag of die voorwendt dat te zijn en die qua organisatie of in haar praktijk schadelijke onwettige activiteiten uitoefent, individuen of de maatschappij nadeel berokkent of de menselijke waardigheid schendt;

6. Inmenging: de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden;
7. Criminele organisaties: iedere gestructureerde vereniging van meer dan twee personen die duurt in de tijd, met als oogmerk het in onderling overleg plegen van misdaden en wanbedrijven, om direct of indirect vermogensvoordelen te verkrijgen, waarbij gebruik gemaakt wordt van intimidatie, bedreiging, geweld, listige kunstgrepen of corruptie, of waarbij commerciële of andere structuren worden aangewend om het plegen van misdrijven te verbergen of te vergemakkelijken. In dit kader worden bedoeld de vormen en structuren van de criminele organisaties die wezenlijk betrekking hebben op de activiteiten bedoeld in voorgaande dreigingen of die destabiliserende gevolgen kunnen hebben op het politieke of sociaaleconomische vlak.

Sinds de inwerkingtreding van de Wet van 30 maart 2017 mogen de bijzondere methoden ook worden ingezet '*vanaf het grondgebied van het Rijk*' en dus niet alleen meer '*op*' het grondgebied (art. 18/1, 1° W.I&V).

In acht genomen dat per toelating verschillende dreigingen aan de orde kunnen zijn, kunnen volgende cijfers worden opgetekend:

AARD DREIGING	AANTAL 2019
Spionage	777
Terrorisme (en radicaliseringsproces)	1118
Extremisme	291
Proliferatie	2
Schadelijke sektarische organisaties	0
Inmenging	87
Criminele organisaties	0
Activiteiten buitenlandse diensten in België opvolgen	(inbegrepen in bovenstaande cijfers)
TOTAAL	**2230**

Bovenstaande cijfers tonen aan dat 'terrorisme (en het radicaliseringsproces)', wat betreft de inzet van BIM-methoden in 2019, de absolute prioriteit blijft voor van de VSSE.

De bevoegdheid van de VSSE wordt niet alleen bepaald door de aard van de dreiging. De dienst mag slechts optreden ter vrijwaring van welbepaalde belangen:

1. De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde zijnde,
   a) de veiligheid van de instellingen van de Staat en het vrijwaren van de 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
2. De uitwendige veiligheid van de Staat en de internationale betrekkingen: het vrijwaren van de onschendbaarheid van het nationaal grondgebied, van de soevereiniteit en de onafhankelijkheid van de Staat, van de belangen van de landen waarmee België gemeenschappelijke doeleinden nastreeft, alsook van de internationale en andere betrekkingen die België met vreemde Staten en internationale of supranationale instellingen onderhoudt;
3. De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

Net als bij de ADIV, wordt door de VSSE verschillende belangen gecombineerd. Wel kan worden vermeld dat de 'vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel' in de cijfergegevens niet voorkwam als belang.

Zoals gezegd (zie II.1.1.4.), beschikt het Comité niet over de cijfers met betrekking tot de geviseerde dreiging en de te verdedigen belangen wat betreft de in dit hoofdstuk bedoelde gewone methoden.

II.2. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS (JURISDICTIONEEL) CONTROLEORGAAN EN ALS PREJUDICIEEL ADVIESVERLENER

II.2.1. CONTROLE OP BEPAALDE GEWONE METHODEN

De controle op bepaalde gewone methoden is voor elk van die methoden anders geregeld.

Wat betreft de identificatie van de gebruiker van telecommunicatie (of de identificatie van de gebruiker van een prepaid-kaart), voerde de wet geen specifieke controle in. In artikel 16/2 § 4 W.I&V werd alleen bepaald dat het Comité maandelijks in het bezit wordt gesteld van de lijst van de gevorderde identificaties en van de rechtstreekse toegang. Zoals hoger gesteld, ontvangt het Comité in dit kader alleen het aantal vorderingen. Het Comité nam zich echter voor om jaarlijks steekproefsgewijs een aantal vorderingen te controleren.[84] Hiermee werd een aanvang genomen in 2020. Het Comité besliste deze thematiek mee op te nemen in zijn in 2019 geopende *'toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten die recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld.'*

84 VAST COMITÉ I, *Activiteitenverslag 2017*, 25 voetnoot 40.

Wat betreft de toegang tot PNR-gegevens die berusten bij de Passagiersinformatie-eenheid, bepaalt artikel 16/3 W.I&V dat die toegang alleen kan na beslissing van het diensthoofd en '*mits afdoende motivering*'. Het Comité moet hiervan in kennis worden gesteld en '*verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen*'. In 2019 werd door het Comité geen dergelijk verbod uitgesproken.

Ten slotte werden aan het Comité bijzondere controlemodaliteiten toegekend in het kader van de mogelijkheid voor de inlichtingendiensten om toegang te krijgen tot informatie afkomstig van politionele camerabeelden (artikel 16/4 W.I&V): een *a priori*-controle[85] en een *a posteriori*-controle.[86] Aangezien de inlichtingendiensten nog geen gebruik konden maken van deze methode, diende het Comité in deze niet op te treden.

II.2.2. CONTROLE OP BIJZONDERE METHODEN

II.2.2.1. De cijfers

In dit onderdeel wordt ingegaan op de activiteiten van het Vast Comité I met betrekking tot de specifieke en uitzonderlijke inlichtingenmethoden. Daarbij zal uitsluitend aandacht besteed worden aan de ter zake genomen jurisdictionele beslissingen en niet aan de operationele gegevens. Vooraf dient evenwel te worden onderlijnd dat het Comité *alle* toelatingen tot de inzet van bijzondere methoden aan een *prima facie*-onderzoek onderwerpt, en dit met het oog op de al dan niet vatting. Tevens woont een lid van de Dienst Enquêtes de (tweewekelijkse) vergaderingen bij waarop de betrokken inlichtingendienst de BIM-Commissie inlicht over de uitvoering van de uitzonderlijke methoden. Hierover wordt een verslag opgemaakt ten behoeve van het Vast Comité I, dat op deze wijze een beter zicht heeft op deze methoden.[87]

---

85 '*De beoordelingscriteria bedoeld in het eerste lid, 2°, worden voorafgaandelijk aan het Vast Comité I voorgeleg*d.'

86 *'De beslissing van het diensthoofd of zijn gedelegeerde wordt met de motivering van deze beslissing zo spoedig mogelijk aan het Vast Comité I betekend. De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingen onderzoek. In dit geval wordt een lijst van de gerichte toegangen eenmaal per maand aan het Vast Comité I doorgegeven. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.*' en '*Elke lijst aan de hand waarvan de correlatie bedoeld in het eerste lid, 1°, wordt uitgevoerd, wordt zo spoedig mogelijk doorgegeven aan het Vast Comité I. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.*'

87 Het Comité beval in 2017 de ADIV aan ook dergelijke tweewekelijkse vergaderingen te organiseren. Het betreft immers een wettelijke verplichting (art. 18/10 § 1, derde lid, W.I&V en

Artikel 43/4 W.I&V stelt dat het Vast Comité I op vijf manieren kan worden gevat:

1. Op eigen initiatief;
2. Op verzoek van de Gegevensbeschermingsautoriteit;
3. Op klacht van een burger;
4. Van rechtswege als de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden;
5. Van rechtswege als de bevoegde minister een toelating heeft verleend op basis van artikel 18/10 § 3 W.I&V.

Daarnaast kan het Comité ook gevat worden in zijn hoedanigheid van 'prejudicieel adviesverlener' (art. 131*bis*, 189*quater* en 279*bis* Sv.). In dat geval geeft het Comité een advies over de al dan niet rechtmatigheid van de specifieke of uitzonderlijke methoden die inlichtingen hebben opgeleverd die in een strafzaak worden gebruikt. De beslissing om een advies te vragen berust bij de onderzoeksgerechten of de strafrechters. Strikt genomen treedt het Comité alsdan niet op als jurisdictioneel orgaan.

WIJZE VAN VATTING	2013	2014	2015	2016	2017	2018	2019
1. Op eigen initiatief	16	12	16	3	1	1	4
2. Gegevensbeschermingsautoriteit	0	0	0	0	0	0	0
3. Klacht	0	0	0	1	0	0	0
4. Schorsing door BIM-Commissie	5	5	11	19	15	10	12
5. Toelating minister	2	1	0	0	0	0	0
6. Prejudicieel adviesverlener	0	0	0	0	0	0	0
TOTAAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**

Het aantal door het Comité genomen beslissingen blijft dalen, en dit ondanks de significante stijging (+27%) van het aantal ingezette BIM-methoden. Bovendien zijn – op één na – alle vattingen het gevolg van een schorsing door de BIM-Commissie.

Eens gevat, kan het Comité verschillende soorten (tussen)beslissingen nemen.

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);

art. 9 KB 12 oktober 2010). Sinds eind januari 2018 wordt – gezien het geringe aantal ingezette BIM-methoden – maandelijks vergaderd, en (in principe) tweewekelijks gerapporteerd.

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.).

AARD VAN DE BESLISSING	2014	2015	2016	2017	2018	2019
Beslissingen voorafgaand aan de vatting						
1. Nietige klacht	0	0	0	0	0	0
2. Kennelijk ongegronde klacht	0	0	0	0	0	0
Tussenbeslissingen						
3. Schorsing methode	3	2	1	0	0	0
4. Bijkomende informatie van BIM-Commissie	0	0	0	0	0	0
5. Bijkomende informatie van inlichtingendienst	1	1	4	0	0	0
6. Onderzoeksopdracht Dienst Enquêtes	54	48	60	35	52	52
7. Horen BIM-Commissieleden	0	2	0	0	0	0
8. Horen leden inlichtingendiensten	0	2	0	0	0	1
9. Beslissing m.b.t. geheim van onderzoek	0	0	0	0	0	0
10. Gevoelige informatie tijdens verhoor	0	0	0	0	0	0
Eindbeslissingen						
11. Stopzetting methode	3	3	6	9	4	11
12. Gedeeltelijke stopzetting methode	10	13	4	6	6	4
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	0	4	11	0	0	0
14. Onbevoegd	0	0	0	0	0	0
15. Wettige toelating / Geen stopzetting methode / Ongegrond	4	6	2	1	1	0
Prejudicieel advies						
16. Prejudicieel advies	0	0	0	0	0	0

II.2.2.2. De rechtspraak

Hieronder wordt de essentie weergegeven van de eindbeslissingen die het Vast Comité I in 2019 nam. De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk worden opgenomen.

De beslissingen werden gegroepeerd onder vier rubrieken:

– Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode;
– De proportionaliteit en de subsidiariteit;
– Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging;
– De wettelijkheid van de uitvoering van een wettige methode.

Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode

Vorderingen tot buitenlandse verstrekkers van communicatiediensten

Dossier 2019/8254 had betrekking op de vraag van een inlichtingendienst aan een sociaal mediaplatform om de inhoud van de communicatie van twee profielen te kennen. Omdat het betrokken mediaplatform niet antwoordde, richtte de dienst een vordering tot een buitenlandse inlichtingendienst met de vraag zich tot het platform te richten. De *démarche* van de dienst kaderde in een imminente dreiging; daar was geen discussie over. Maar aangezien de dienst dit als een gewone methode beschouwde, was er geen BIM-beslissing opgesteld. Zowel de BIM-Commissie, die via een ander dossier kennis had gekregen van de vordering aan de buitenlandse inlichtingendienst, als het Vast Comité I, waren van oordeel dat het een uitzonderlijke methode betrof. Omwille van het belang van deze uitspraak wordt de essentie van de beslissing van het Comité *in extenso* weergegeven: *'Overwegende dat de wet van 13 juni 2005 betreffende de elektronische communicaties en meer in het bijzonder de artikelen 9 en 122 tot 127 de procedures vastlegt waarin de politiediensten en de inlichtingen- en veiligheidsdiensten toegang hebben tot elektronische communicaties. Dat het Koninklijk Besluit van 12 oktober 2010, en meer in het bijzonder artikel 5, de modaliteiten vastlegt inzake de verzoeken betreffende elektronische communicaties door de inlichtingen-en veiligheidsdiensten. Overwegende dat het Arrest van het Hof van Cassatie van 1 december 2015 (zaak Yahoo, P.13.2082.N) bevestigt dat een maatregel die bestaat in de verplichting om gevorderde gegevens te verstrekken wordt genomen op het Belgisch grondgebied ten aanzien van elke operator of verstrekker die zijn economische activiteiten actief op consumenten in België richt. Overwegende dat overigens artikel 3, 11/1 in die zin werd gewijzigd, waarbij het begrip 'verstrekker van communicatiedienst' nader werd gedefinieerd. Overwegende dat […[in die optiek aan de Belgische wet is onderworpen en op basis van de Belgische wet door de [betrokken inlichtingendienst] kan worden aangesproken. Overwegende dat de [betrokken inlichtingendienst] bij haar vordering […] bij […], herhaald via haar vordering […] bij de [buitenlandse inlichtingendienst], dienvolgens de Belgische wet diende na te leven. Overwegende dat in voorliggend geval art. 18/17 W.I&V diende te worden nageleefd. Dat inderdaad voornoemd artikel 18/17 van toepassing is en niet art. 18/16 W. I&V, nu art. 18/17 W.I&V spreekt van "communicaties onderscheppen" en "er kennis van te nemen", terwijl art. 18/16 integendeel spreekt van het "toegang krijgen tot een informaticasysteem" (…) Overwegende dat het Vast Comité I overigens benadrukt dat, anders dan de [betrokken inlichtingendienst] voorhoudt in haar brief van […] aan de BIM-commissie, de bevraging bij de [buitenlandse inlichtingendienst] niet kan gezien worden als een gewone methode. Dat integendeel deze bevraging moet worden gezien als een tweede poging (na de vordering aan[…]) om alsnog de inhoud van communicatie te bekomen.'*

Onvoldoende motivering

In het kader van een specifieke methode die door de BIM-Commissie was geschorst, vroeg het Comité bijkomende informatie aan de inlichtingendienst. Deze verschafte slechts een summier antwoord; zij beriep zich daarbij onder meer op de regel van de derde dienst. Ze voegde echter toe dat ze de beslissing van de BIM-Commissie tot schorsing aanvaardde. Het Comité oordeelde '*dat onder deze omstandigheden de beoogde methode dient te worden gestaakt en dat alle door de methode bekomen inlichtingen dienen te verdwijnen*' (dossier 2019/8418).

Ook in een ander dossier was het gebrek aan een gedegen motivering van de beslissing aan de orde. In dossier 2019/8768 wenste de inlichtingendienst gegevens te bekomen over telefonische communicaties van een bepaald persoon voor een periode van twaalf maanden voorafgaand aan de datum van de beslissing van het diensthoofd. Het Comité oordeelde echter dat de in de BIM-beslissing opgegeven motivering het niet mogelijk maakte '*te beslissen of de in toepassing gebrachte BIM voldoet aan de door de wet gestelde vereisten, inzake bevoegdheid van de dienst en proportionaliteit van de methode*'. Daarenboven bleek onder meer dat:

- '*in de BIM-beslissing nergens sprake is van de twee wettelijk op te volgen dreigingen waarnaar wordt verwezen*';
- '*de werkelijke activiteit die door de dienst als een op te volgen dreiging wordt beschouwd en waarvoor een specifieke methode wordt aangevraagd, niet duidelijk of eenduidig omschreven is, evenmin onderbouwd is met feitelijke elementen en op bepaalde vlakken de bevoegdheid van een inlichtingendienst te buiten gaat. Dat onvoldoende wordt aangetoond of en hoe de voorziene methode een reële bijdrage kan leveren aan bepaalde van de in de beslissing vooropgesteld finaliteiten*';
- '*het Comité er op wijst dat 'pacifisme' op zich geen op te volgen dreiging kan uitmaken. Het is immers niet meer dan een wereldbeschouwing die duurzame vrede nastreeft en in die optiek volkomen legitiem is in een democratische samenleving*';
- '*de definitie van extremisme strikt genomen niet van toepassing is op de ADIV aangezien ze is opgenomen in de artikelen 7 en 8 W.I&V die alleen van toepassing zijn op de Veiligheid van de Staat. Echter, aangezien de toepassing van de methode zoals omschreven in artikel 18/8 W.I&V een verwijzing naar een van de dreigingen uit de artikelen 7 en 8 W.I&V vereist om de maximale duur van de methode te rechtvaardigen, is deze definitie in deze ook van toepassing op de ADIV*';
- '*uit de feiten zoals die in de BIM-beslissing zijn hernomen, evenmin blijkt dat de betrokkene of een (extremistische) dreiging vormt*'; '*het Vast Comité I op artikel 2 § 1 tweede lid IW.I&V wijst: 'Bij het vervullen van hun opdrachten zorgen die diensten voor de naleving van, en dragen bij tot de bescherming van de individuele rechten en vrijheden alsook tot de democratische ontwikkeling van de maatschappij.' Het Comité benadrukt in dit kader het belang van de vrijheid*

van vereniging en de vrijheid van meningsuiting als fundamentele waarden van onze Westerse maatschappij. Het wijst er op dat een inmenging van de overheid in deze rechten en vrijheden alleen kan in uitzonderlijke omstandigheden. Dat deze omstandigheden allerminst blijken uit voorliggend dossier. In die optiek zijn de gehanteerde bewoordingen, de gemaakte redeneringen waarbij men vanuit zeer onzekere feiten nog meer onzekere hypothese opbouwt (als A waar zou zijn – maar hiervoor zijn omzeggens geen aanwijzingen – dan is B eventueel mogelijk …) en de niet-onderbouwde verdachtmakingen en doemscenario's (de term terrorisme wordt zelfs gebruikt), onaanvaardbaar.'

– '*de BIM-beslissing tot slot op sommige plaatsen melding maakt van de of een finaliteit van de methode terwijl deze finaliteit niet aantoonbaar kan gerealiseerd worden via de geviseerde methoden*.'

Het Comité vatte zichzelf en stelde een aantal bijkomende vragen aan de betrokken inlichtingendienst. De navolgende beslissing van het Comité werd genomen in het werkingsjaar 2020.

Verschil tussen de periode in het ontwerp van machtiging en in de uiteindelijke machtiging

De BIM-Commissie verleende haar eensluidend advies bij een ontwerp van machtiging tot het uitvoeren van een uitzonderlijke methode voor '*une période de deux semaines, à partir de mon autorisation*.'[88] In de uiteindelijke machtiging wordt echter gewag gemaakt van een periode van twee maanden. Daarop schorst de BIM-Commissie de machtiging voor een periode die de twee weken te rekenen vanaf de machtiging van het diensthoofd, te boven gaat. Het Vast Comité I sloot zich bij die schorsing aan (dossier 2019/8421).

Niet-tijdige verwittiging van de BIM-Commissie

In twee dossiers wenste een inlichtingendienst een lopende methode te verlengen (dossiers 2019/8788 en 2019/8968). De BIM-Commissie werd echter pas enkele dagen na de afloop van de initiële beslissing op de hoogte gebracht van de verlenging. In die tussentijd was de nieuwe methode dan ook niet gedekt door een geldige beslissing. Immers, '*pas vanaf het moment van betekening de verlenging van de methode kon worden opgestart*'. In dossier 2019/8788 had de inlichtingendienst deze onwettig verkregen gegevens zelf '*in quarantaine […] gehouden*'. Het Comité benadrukte echter dat '*het feit dat de gegevens "in quarantaine worden gehouden" en niet beschikbaar zijn voor exploitatie niets verandert aan de wettelijke bepalingen ter zake. Overwegende dat de BIM-Commissie dan ook een exploitatieverbod uitsprak krachtens artikel 18/3 § 6 W. I&V.*'

88 '*een periode van twee weken, vanaf mijn machtiging*' (vrije vertaling).

De proportionaliteit en de subsidiariteit[89]

Een inlichtingendienst wenste over te gaan tot de kennisname van oproep- en lokalisatiegegevens van de communicatiemiddelen van drie targets (dossier 2019/8150). Voor een van hen stelde zich geen enkel probleem: '*Attendu qu'en ce qui concerne le "target" principal dans le dossier, la décision du dirigeant du service est suffisamment motivée et la mesure est proportionnelle à la menace*'.[90] Maar voor de twee andere personen was dat niet het geval. Het bleken familieleden van de eerste target die zelfs niet op hetzelfde adres gedomicilieerd waren. Daarenboven bleek op geen enkele wijze dat deze personen betrokken zouden zijn bij de activiteiten van hun familielid, noch dat de target de communicatiemiddelen van de twee andere personen zou gebruiken. '*Attendu que le simple fait qu'un lien familial existe entre ces personnes n'est en soi pas suffisant pour justifier une intrusion dans la vie privée*'.[91] De methode was op dit vlak dan ook onwettig.

Wanneer een inlichtingendienst gedurende twee maanden een plaats wil observeren, waar op één welbepaalde dag een extremistische bijeenkomst zal plaatsvinden, komt eerst de BIM-Commissie en nadien het Vast Comité I tussen: '*Attendu que la décision de méthode spécifique est disproportionnée en ce qu'elle ne mentionne pas en quoi l'observation peut être réalisée pendant deux mois, alors que la menace avancée porte sur un événement à date fixe, sur un seul jour*'.[92] Wat betreft de dag van de bijeenkomst zelf, was de genomen maatregel niet disproportioneel: '*Attendu que la décision est motivée par la nécessité d'identifier des personnes issues [d'un milieu extrémiste] et participant à un meeting, dont le lieu et la date sont précisés, et au cours duquel des orateurs [extrémistes] prendront la parole; que ces informations ne peuvent être recueillies par méthode ordinaire; que l'utilisation de moyens techniques est justifiée par la difficulté d'observer les lieux visés*'[93] (dossier 2019/8224). De conclusie luidde dan ook dat de methode alleen legaal was op de dag van de bijeenkomst.

In het kader van een controle van een specifieke methode vroeg de BIM-Commissie meer informatie over de vermelde dreiging van spionage en de beweerde

89 Er was één dossier, dat evenwel geen aanleiding gaf tot een jurisdictionele beslissing, waarin de nadruk kwam te liggen op het subsidiairiteitsbeginsel.

90 *'overwegende dat wat betreft het hoofdtarget in dit dossier, de beslissing van het diensthoofd voldoende gemotiveerd is en dat de maatregel proportioneel is ten aanzien van de dreiging'.* (vrije vertaling)

91 '*Overwegende dat het eenvoudige feit dat er een familiale band bestaat tussen deze personen onvoldoende is om een intrusie in de private levenssfeer te rechtvaardige.'* (vrije vertaling).

92 *'Overwegende dat de beslissing tot specifieke methode disproportioneel is gezien deze niet vermeldt hoe de observatie kan worden uitgevoerd gedurende twee maanden, terwijl de vooropgestelde dreiging betrekking heeft op een gebeurtenis met een vaste datum, op één dag'.* (vrije vertaling).

93 *'Overwegende dat de beslissing werd gemotiveerd door de noodzaak om personen te identificeren uit [een extremistisch milieu] dewelke deelnamen aan een meeting, waarvan de plaats en de datum worden vermeld, en tijdens dewelke [extremistische] sprekers het woord zullen nemen; dat de informatie niet kan worden verzameld via een gewone methode, dat de inzet van technische middelen gerechtvaardigd is omwille van de moeilijkheid om de geviseerde plaats te observeren'.* (vrije vertaling).

link tussen het target en die mogelijke dreiging (dossiers 2019/8377). Wanneer de dienst antwoordt dat ze niet over de gevraagde informatie beschikte, schorste de BIM-Commissie de methode. Ook op het verzoek van het Vast Comité I '*om bepaalde aspecten van de specifieke methode nader te motiveren aangezien de wijze waarop de beslissing was gemotiveerd, niet toeliet te bevestigen dat de methode beantwoordde aan de wettelijke vereisten van legaliteit, proportionaliteit en subsidiariteit*', herhaalde de betrokken inlichtingendienst in essentie wat in de oorspronkelijke toelating was opgenomen. De dienst erkende zelf dat de enkele bijkomende gegevens '*de ontoereikende proportionaliteit niet corrigeren*' en dat ze de schorsing door de BIM-Commissie zondermeer aanvaardt. Het Comité besloot dan ook dat de methode niet op wettige wijze was gemachtigd.

Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging

Onduidelijk voorwerp

De betrokken inlichtingendienst wenste een aantal targets van vreemde origine te observeren op '*niet voor het publiek toegankelijke plaatsen, die niet aan het zicht onttrokken zijn*', zonder die plaatsen te betreden (art. 18/4 § 2 W.I&V). Het was de bedoeling om daarbij technische middelen te gebruiken. In het dossier was sprake van (mobiele) camera's en CCTV, terwijl de beslissing van het diensthoofd gewag maakte van het plaatsen van een baken. Daarenboven bleek slechts van één target geweten met welke wagen hij zich verplaatste. De BIM-Commissie vroeg nadere uitleg aan de betrokken dienst. Daaruit bleek nog steeds niet voldoende duidelijk op welke voertuigen bakens zouden worden geplaatst. Daarom werd de stopzetting bevolen van het plaatsen van een baken onder de voertuigen van de overige targets (dossier 2019/8109).

Een uitzonderlijke in plaats van een specifieke methode

Een inlichtingendienst vordert via een specifieke methode de technische medewerking van een operator om verkeersgegevens te bekomen van een bepaalde persoon. Het Vast Comité I merkt echter dat de operator die gegevens niet via haar eigen bestanden kan opvragen, maar wel via een bestand dat gelokaliseerd is bij de betrokkene: '*Considérant que les données […] ne sont disponibles que par le biais d'une intrusion dans le système informatique où elles sont stockées, à savoir [chez] la personne faisant l'objet des méthodes de recueil de données. Considérant qu'une telle intrusion constitue une méthode exceptionnelle de recueil des données prévue à l'article 18/16 L.R&S.*'[94] De methode werd dan ook vernietigd (dossier 2019/8446).

[94] *'Gelet dat de gegevens […] enkel beschikbaar zijn via een intrusie in het informaticasysteem waarin ze zijn opgeslagen, te weten [bij] de persoon die het voorwerp uitmaakt van bijzondere*

Diplomatieke immuniteiten

De in dossier 2019/8483 beoogde methode bestond erin om gedurende twee maanden vanaf de datum van de machtiging van het diensthoofd (en na eensluidend advies van de Commissie) communicaties af te luisteren. De methode bleek echter betrekking te hebben op telefoonnummers die geregistreerd waren op naam van een permanente missie bij een internationale instelling die in België gevestigd is.

De bescherming die door het Verdrag van Wenen van 18 april 1961 inzake diplomatiek verkeer geboden wordt, was hierop niet van toepassing. Dit verdrag handelt immers over de traditionele diplomatieke bilaterale missies. Maar de internationale instelling is onderhevig aan een eigen regeling die België verplicht de gebruikelijke diplomatieke immuniteiten te respecteren. Hiermee wordt verwezen naar de immuniteiten en voorrechten uit het verdrag van Wenen.

De inlichtingendienst meende hiermee geen rekening te moeten houden omdat de nummers waarop zij een methode wou toepassen, exclusief door de target zouden worden gebruikt. Na een eerste analyse bleek echter dat de nummers gedeeld werden met andere personen dan de target. '*Overwegende dienvolgens dat de omstandigheden en het feitelijk relaas zoals medegedeeld via het ontwerp van machtiging aan de BIM-Commissie […] op die manier niet overeenstemt met de realiteit.*' De dienst stelde zelf vast dat hierdoor de voorwaarden waarvan sprake in het eensluidend advies niet meer waren voldaan en besloot om de methode stop te zetten. Het Comité stelde dan ook '*dat aldus de beoogde methode dient te worden gestaakt en dat alle door de methode bekomen inlichtingen dienen te verdwijnen.*'

Berekening periode 'voorafgaand aan de beslissing'

Een inlichtingendienst besliste om over te gaan tot het opsporen van elektronische communicatiemiddelen en lokaliseren van elektronische communicaties voor de periode van twaalf maanden voorafgaand aan de beslissing (dossier 2019/8794). Deze beslissing werd genomen op dag 29 van maand X. Het Comité stelde dat '*de "periode voorafgaand aan de beslissing" zich in casu noodzakelijkerwijs dient te situeren tussen 28 X 2018 en 29 X 2019.*' De dienst vroeg evenwel gegevens op voor de periode van 20 X 2018 tot 19 X 2019. '*Dat aldus moet worden vastgesteld dat gedurende de periode 20 X 2018 tot en met 27 X 2018 verkeerdelijk gegevens werden opgevraagd, wat niet conform is met artikel 18/8 § 2 W. I&V.*'

Dezelfde problematiek was aan de orde in dossier 2019/9024. '*Qu'en l'espèce, les méthodes de repérage et de localisation de communications électroniques décidées concernent une menace potentielle liée au domaine du terrorisme; Attendu que dans le cadre d'une menace potentielle de terrorisme, et en vertu de l'article*

inlichtingenmethoden. Gelet dat een dergelijke intrusie een uitderlijke inlichtingenmethode betreft voorzien in artikel 18/16 W.I&V'. (vrije vertaling).

précité, le dirigeant d'un service peut uniquement requérir le repérage et la localisation de données liées à des communications électroniques pour une période de 12 mois préalables à la décision; Que le terme préalable doit être compris comme instituant la date de la décision comme un point de départ non inclus dans le calcul du délai légal visé; Que la décision dont question étant datée du 18 X 2019, la récolte des données ne pouvait donc pas excéder une période de 12 mois précédant le jour de la décision; Qu'en l'espèce la période maximale de récolte rétroactive de données pouvait donc uniquement s'étendre [jusqu'au] 17 X 2018.'[95]

De wettelijkheid van de uitvoering van een wettige methode

Uitvoering van een specifieke methode voorafgaand aan de kennisgeving van de BIM-commissie

In dossier 2019/9097 had de inlichtingendienst zijn vordering aan de operator gezonden de dag voorafgaand aan de in kennisstelling van de BIM-Commissie. Deze '*mise en œuvre […] ne respecte pas les prescrits de l'article 18/3, § 1er de la L R&S; Qu'en conséquence, le réquisitoire adressé à l'opérateur en date du 4 X 2019 à 16h49 et les résultats obtenus sur la base de celui-ci doivent être considérées comme obtenu illégalement*.'[96]

II.3. CONCLUSIES

Het Vast Comité I formuleert volgende algemene conclusies:

– Tussen 1 januari en 31 december 2019 werden door de twee inlichtingendiensten samen 2444 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 2230 door de VSSE (waarvan 1781 specifieke en 449 uitzonderlijke) en 214 door de ADIV (waarvan 138 specifieke en 76 uitzonderlijke). Na een constante stijging van het aantal ingezette BIM's de afgelopen jaren, kan voor het eerst een stagnatie worden opgetekend.

---

95 '*Dat in dit geval, de methoden tot opsporen en lokaliseren van elektronische communicaties een potentiële dreiging uitmaken gelieerd aan terrorisme; Overwegende dat in het kader van een potentiële terrorismedreiging, en krachtens het geciteerde artikel, het hoofd van een dienst alleen de opsporing en lokalisatie kan vorderen van elektronische communicaties voor een periode van 12 maanden voorafgaand aan de beslissing; Dat de term voorafgaand dient te worden begrepen als een datum waarbij de datum van de beslissing niet inbegrepen is bij de berekening van de wettelijk bedoelde termijn; Dat de beslissing waarvan sprake gedateerd was op 18 X 2019, en dat de collecte van de gegevens dus geen periode van 12 maanden kon overstijgen voorafgaand aan de dag van de beslissing; Dat in voorkomend geval de maximale periode tot retroactieve gegevensverzameling zich slechts uitstrekt (tot) 17 X 2018*.' (vrije vertaling).

96 'indeplaatstelling *[…] de voorwaarden uit artikel 18/3, § 1er van de W.I&V niet respecteert; Dat bijgevolg, de vordering aan het adres van de operator van 4 X 2019 om 16u49 en de op deze basis verkregen resultaten moeten worden beschouwd als zijnde illegaal verkegen*.' (vrije vertaling).

- De VSSE blijft het leeuwendeel van de ingezette methoden voor zijn rekening nemen (91,2%).
- Als de globale cijfers worden uitgesplitst, kan een opmerkelijke stijging bij de ADIV worden opgetekend van zowel specifieke (van 102 naar 138) als uitzonderlijke (van 28 naar een meer dan verdubbeling 76) ingezette methoden. De VSSE laat een opmerkelijke stijging optekenen van het aantal ingezette uitzonderlijke methoden (van 344 naar 449). Dat ondanks al deze stijgingen een stagnatie in het geheel werd waargenomen, is te wijten aan sterk gedaalde aantal (van 1971 naar 1781) door de VSSE ingezette specifieke methoden.
- Wat betreft de gewone methoden van vorderingen gericht aan operatoren om bepaalde communicatiemiddelen te identificeren betreft, wordt – in tegenstelling tot de afgelopen jaren – een daling van ca. 12% opgetekend.
- De ADIV richtte zich bij de inzet van BIM-methoden zoals steeds meer op de dreiging van 'spionage', gevolgd door 'inmenging'; voor de VSSE was de aard van de dreiging hoofdzakelijk 'terrorisme (en het radicaliseringsproces)', gevolgd door 'spionage'.
- Het Comité werd gevat in zestien dossiers, waarvan vier vattingen op eigen initiatief en twaalf van rechtswege nadat de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid had geschorst (art. 43/4 W.I&V). Onwettigheden betroffen onder meer een onvoldoende motivering, de niet-tijdige verwittiging van de BIM-Commissie, een onduidelijk voorwerp, of nog, een te lange collecteperiode.

HOOFDSTUK III
HET TOEZICHT OP BUITENLANDSE INTERCEPTIES, BEELDOPNAMEN EN IT-INTRUSIES

III.1. DE BEVOEGDHEDEN VAN DE ADIV EN DE CONTROLETAAK VAN HET VAST COMITÉ I[97]

Al in 2017 werd de bevoegdheid van de ADIV in het kader van de veiligheidsintercepties uitgebreid².[98] De intercepties konden sindsdien voor communicaties '*uitgezonden of ontvangen in het buitenland*'. Deze mogelijkheid geldt voor *quasi* alle opdrachten van de ADIV. Daarbij is het niet onbelangrijk te vermelden dat de opdrachtomschrijvingen zelf, ook werden verruimd. Tegelijkertijd voerde de wetgever twee andere methoden in, te weten de 'intrusie in een informaticasysteem' (art. 44/1 W.I&V) en de 'opname van bewegende beelden' (art. 44/2 W.I&V). En ook de wijze waarop het Comité deze methoden kan controleren, werd gewijzigd.

De controle *voorafgaand* aan de intercepties, intrusies of beeldopnames gebeurt op basis van jaarlijks opgestelde lijsten.[99] Dit betekent dat er naast een jaarlijks interceptieplan, ook een intrusie- en beeldplan dient te worden opgesteld door de ADIV.[100] De ADIV moet die lijsten in de maand december voor toelating aan de minister van Defensie zenden. Deze heeft tien werkdagen om zijn beslissing mee te delen aan de ADIV[101] die op zijn beurt de lijsten, voorzien van de toelating van de minister, overzendt aan het Vast Comité I.[102]

---

97 Zie artt. 44 t.e.m. 44/5 W.I&V.

98 Over de opeenvolgende wetswijzigingen inzake de interceptiebevoegdheid van de ADIV, zie VAST COMITÉ I, *Activiteitenverslag 2018*, 61 e.v.

99 Dit impliceert niet dat het Vast Comité I de bevoegdheid heeft om de door de minister goedgekeurde lijst al dan niet goed te keuren.

100 In deze plannen stelt de ADIV een lijst op van '*organisaties of instellingen die het voorwerp zullen uitmaken van interceptie van hun communicaties, intrusies in hun informaticasystemen of opnames van vaste of bewegende beelden tijdens het komende jaar. Deze lijsten verantwoorden voor iedere organisatie of instelling de reden waarom zij het voorwerp is van een interceptie, intrusie of opname van vaste of bewegende beelden in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°, en vermelden de voorziene duur*' (art. 44/3 W.I&V).

101 Indien de minister geen beslissing heeft genomen of deze niet heeft meegedeeld aan de ADIV vóór 1 januari, mogen de voorziene intercepties, intrusies en opnames aanvangen, onverminderd iedere latere beslissing van de minister.

102 Voor intercepties, intrusies of opnames die niet opgenomen zijn in de jaarlijkse lijsten, maar die '*onontbeerlijk en dringend blijken te zijn*', wordt de minister zo spoedig mogelijk en uiterlijk

Het toezicht *tijdens* de interceptie, intrusie of opname gebeurt '*op elk ogenblik door middel van bezoeken aan de installaties waar de Algemene Dienst Inlichting en Veiligheid deze intercepties, intrusies en opnames van vaste of bewegende beelden uitvoert*'.

Het toezicht *na* de uitvoering van de methode gebeurt '*aan de hand van maandelijkse lijsten van landen of van organisaties of instellingen die effectief het onderwerp hebben uitgemaakt van een afluistering, intrusie of opname van beelden gedurende de voorafgaande maand*' en die '*de reden verantwoorden waarom de interceptie, intrusie of opname van beelden werd uitgevoerd in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°*'. Deze lijsten moeten ter kennis van het Vast Comité I worden gebracht. De *ex post*-controle gebeurt ook aan de hand van '*het nazicht van logboeken die permanent op de plaats van de interceptie, de intrusie of de opname van vaste of bewegende beelden door de Algemene Dienst Inlichting en Veiligheid worden bijgehouden*'. Deze logboeken moeten steeds toegankelijk zijn voor het Vast Comité I.

Wat kan het Vast Comité I nu ondernemen indien het een onregelmatigheid vaststelt? Artikel 44/4 W.I&V bepaalt dat het Comité, '*[o]ngeacht de andere bevoegdheden aan dit Comité toegekend op basis van de wet van 18 juli 1991, het recht [heeft] de aan de gang zijnde intercepties, intrusies of beeldopnames te doen stopzetten wanneer blijkt dat ze de wettelijke bepalingen of de [ministeriële] toelating niet respecteren. Het beveelt dat de gegevens die onwettig werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd, volgens de door de Koning te bepalen nadere regels*.' Ondanks de dringende aanbeveling van het Comité[103], werd evenwel nog steeds geen dergelijk interceptie-KB getroffen.[104] Het Comité beveelt dan ook opnieuw aan om dit zo spoedig mogelijk te doen.[105]

III.2. HET IN 2019 VERRICHTE TOEZICHT

III.2.1. HET TOEZICHT VOORAFGAAND AAN DE INTERCEPTIE, INTRUSIE OF OPNAME

Eerder formuleerde het Vast Comité I een aantal belangrijke opmerkingen bij de zogenaamde 'interceptieplannen'. De belangrijkste opmerkingen betroffen de pri-

op de eerste werkdag die volgt op de aanvang van de methode ingelicht. Indien de minister niet akkoord gaat, kan hij deze methode laten stopzetten. Deze beslissing wordt door de ADIV zo spoedig mogelijk meegedeeld aan het Vast Comité I.

103 VAST COMITÉ I, *Activiteitenverslag 2018*, 129.

104 Het Comité moet zijn beslissing alleszins omstandig motiveren en meedelen aan de minister en aan de ADIV.

105 In dezelfde zin dient ook nog een KB getroffen te worden voor wat betreft de nadere regels voor de medewerking van operatoren van een netwerk of verstrekkers van een elektronische communicatiedienst (art. 44/5 W.I&V).

oriteitsverschillen tussen enerzijds het Inlichtingenstuurplan[106] en anderzijds de voorgenomen SIGINT-intercepties alsook het gegeven dat de omschrijving van de organisaties en instellingen die het voorwerp zullen uitmaken van intercepties, te algemeen was. In het 'Interceptieplan 2019', dat eind januari 2019 aan het Comité werd bezorgd, heeft de ADIV de organisaties die het voorwerp kunnen uitmaken van intercepties, gedetailleerd omschreven. Het Comité diende slechts enkele kleine opmerkingen te formuleren bij het plan.

De beeld- en intrusieplannen daarentegen waren opnieuw eerder summier. Ze vormden het onderwerp van bespreking tijdens een werkvergadering tussen het Vast Comité I en de ADIV in maart 2019. Er werd door het Comité besloten deze thematiek op te nemen in zijn in 2019 geopende *'toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten die recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld.*'

III.2.2. HET TOEZICHT TIJDENS DE INTERCEPTIE, INTRUSIE OF OPNAME

In 2019 heeft het Comité de installaties van waaruit de intercepties gebeuren niet bezocht; dit werd uitgesteld naar het tweede semester van 2020. Deze bezoeken waren nochtans ingepland in het kader van boven vernoemd toezichtonderzoek. Meerdere redenen lagen aan de opschorting ten grondslag. Vooreerst vergde de eerste modules van het toezichtonderzoek – te weten de studie van de artikelen 16/2 en 16/3 W.I&V – meer tijd en middelen dan initieel verwacht. Ook werd het Comité geconfronteerd met andere prioriteiten en bleek voor sommige aspecten deze controle technisch onmogelijk (bijv. bij opnames).

III.2.3. HET TOEZICHT NA DE UITVOERING VAN DE METHODE

Het Comité ontving elf '*maandelijkse lijsten*[107] *van landen of van organisaties of instellingen die effectief het onderwerp hebben uitgemaakt van een afluistering, intrusies of opname van beelden gedurende de voorafgaande maand*' en die '*de reden verantwoorden waarom de interceptie, intrusie of opname van beelden werd uitgevoerd in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°*'.

Wat betreft de intrusies, moest het Comité de ADIV herhaaldelijk aan zijn verplichtingen herinneren en preciseren dat het Comité maandelijks bestemme-

106 Een plan opgesteld door de voorheen Directie Intelligence van de ADIV met daarin de op te volgen landen en de prioritisering.

107 De lijst van november 2019 voor wat betreft de intercepties en opnames ontbrak.

ling moet zijn van een verslag, ook als er geen intrusies werden uitgevoerd. In oktober 2019 mocht het Comité een schrijven ontvangen van de ADIV met de melding dat er geen intrusies plaatsvonden in 2019. Ingevolge de brief werd het Comité tevens bestemmeling van de maandelijkse lijst van intrusies. In totaal werden drie lijsten ontvangen. De controle van de maandelijkse intrusie- en beeldopnamelijsten werd opgenomen in het kader van het in hierboven vermelde toezichtonderzoek.

HOOFDSTUK IV
BIJZONDERE OPDRACHTEN

In de loop der jaren kreeg het Vast Comité I een aantal specifieke opdrachten toegekend dewelke hun oorsprong niet vinden in een wettelijke bepaling, maar een antwoord bieden op een concrete nood. Deze bijkomende opdrachten werden in nauw overleg met het Comité aan hem toegewezen.

IV.1. TOEZICHT OP DE ACTIVITEITEN VAN HET ISTAR-BATALJON

Eerder nam het Vast Comité I al een standpunt in met betrekking tot de inlichtingenactiviteiten die worden uitgeoefend door het ISTAR-bataljon *(Intelligence Surveillance Target Acquisition and Reconnaissance)* in het kader van buitenlandse operaties. Daarin werd door het Comité benadrukt dat de oprichting van het bataljon tegemoet kwam aan een toenemende behoefte aan *battlefield intelligence*, en dit gelet op het feit dat het aantal buitenlandse opdrachten steeds groeide. Maar het Comité herhaalde ook dat de organieke Wet van 30 november 1998 slechts twee inlichtingendiensten erkent (art. 2 W.I&V). Het wees daarbij zowel het Parlement, de minister van Defensie als de CHOD op het feit dat dit bataljon – zij het gedeeltelijk – inlichtingenactiviteiten ontwikkelt.

Aangezien er op korte termijn geen wettelijke of structurele oplossingen voorhanden bleken, werd eind april 2018 een voorlopige oplossing uitgewerkt door middel van een protocolakkoord tussen de ADIV en de CHOD.[108] Hierin worden onder meer de taken en opdrachten van het ISTAR-bataljon inzake HUMINT- en analysecapaciteiten vastgelegd. Daarnaast wordt ook de organisatie van een technische en juridische controle uitgewerkt. Technische controle is de controle op de

[108] Protocolakkoord van 24 mei 2018 tussen de CHOD en de ADIV betreffende de HUMINT- en de analysecapaciteiten van het ISTAR Bn. Hierop werd eerder aangedrongen door de Parlementaire Onderzoekscommissie Aanslagen: '*De onderzoekscommissie acht de opdrachten van ISTAR belangrijk voor de veiligheid van onze militairen, doch meent dat de verhouding tussen dit bataljon en de ADIV formeel geregeld moet worden middels een samenwerkingsprotocol, waarin duidelijk wordt omschreven op welke wijze en onder welke voorwaarden ISTAR kan bijdragen aan de versterking van de informatiepositie van de ADIV. In dat kader lijkt het tevens aangewezen om het Vast Comité I te belasten met het toezicht op deze ondersteunende taak van ISTAR*', in *Parl. St.* Kamer, 2016-17, nrs. 54K1752/008, 306.

correcte toepassing van de richtlijnen inzake analyse en van de HUMINT-richtlijnen en van de bijzondere akkoorden tussen de CHOD en de ADIV. Onder juridische controle wordt de controle op de correcte toepassing van het protocol verstaan. Deze taken berusten bij de ADIV.

Het ISTAR-bataljon bezorgt de ADIV daartoe uit eigen beweging de interne reglementen en richtlijnen. De controle vindt plaats door middel van bezoeken aan de installaties van het ISTAR-bataljon en aan de zones waar het zijn operaties en activiteiten uitvoert. De controle wordt ook uitgevoerd op basis van een analyse van documenten en van verhoren.

Het Vast Comité I werd in het protocol aangewezen om een – zij het onrechtstreeks – toezicht uit te oefenen over de activiteiten van het bataljon. Daartoe overhandigt de ADIV aan de minister van Defensie, de CHOD en het Vast Comité I een trimesterieel verslag betreffende iedere onderzoeksopdracht.

Het Comité ontving in 2019 effectief vier controlerapporten. Uit de rapporten bleek dat het ISTAR-bataljon weinig activiteiten ontvouwde die onder toepassing van het bovenvermelde protocolakkoord vielen. De door het ISTAR-bataljon ontwikkelde inlichtingenactiviteiten, beantwoordden volgens de ADIV aan de opgelegde voorschriften en richtlijnen.

De analyse van deze verslagen zal het voorwerp uitmaken van verder onderzoek. Gelet op het feit dat ISTAR weinig HUMINT-activiteiten ontwikkelt, heeft het Comité hiervan geen prioriteit gemaakt.

IV.2. CONTROLE OP DE SPECIALE FONDSEN

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 werd 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 werd de controle van deze specifieke uitgaven alleen verricht door de directeur algemeen beleid van de minister van Justitie. Halfweg 2018 uitte het Rekenhof het voornemen om vanaf het afsluiten van de rekening van 2018 eveneens een periodieke controle te doen van deze fondsen. Het Comité kreeg in 2020 kopie van de in 2019 door het Rekenhof uitgevoerde controle voor het boekjaar 2018.[109]

De controle van de speciale fondsen van de ADIV wordt uitgevoerd door een vertegenwoordiger van het kabinet van de minister van Defensie en dit viermaal per jaar. Dit gebeurde sinds 2010 – op voorstel van het Rekenhof – in aanwezigheid van de voorzitter van het Vast Comité I. Het was een gevolg van de wens

[109] COUR DES COMPTES, *Sûreté de l'Etat. Contrôle 2019 des fonds spéciaux. Rapport adressé au ministre de la Justice*, 20 mai 2020.

uitgedrukt door de toenmalige minister van Defensie om niet langer zelf de controle uit te voeren zoals geïnstaureerd sinds 1962. In februari 2019 was de voorzitter effectief aanwezig bij één van deze controles. In mei 2019 werd evenwel een schrijven gericht aan de toenmalige vice-premier en minister van Buitenlandse en Europese Zaken en Defensie dat het Comité deze opdracht niet langer zou uitvoeren. Immers, "*nous estimons que le contrôle actuel basé sur un échantillonnage limité ne correspond pas aux exigences d'un contrôle réellement effectif et pourrait, en outre, engager tant la responsabilité ministérielle que celle du Comité permanent R*". Er werd tevens gesuggereerd dat, conform het toezicht op de fondsen van de VSSE, hier een opdracht voor het Rekenhof was weggelegd. In februari 2020 schaarde het Rekenhof zich achter dit initiatief en bracht het de minister van Buitenlandse Zaken en Defensie op de hoogte van zijn bereidheid om een formele controle op de rekeningen uit te voeren, waarbij ze beroep kon doen op de technische ondersteuning zoals voorgeteld door het Vast Comité I.[110] Daardoor kon het Comité "*exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds*". Er werd in 2019 beslist om in 2020 een opvolgonderzoek op te starten naar het beheer, het gebruik en de controle van de speciale fondsen.[111]

IV.3. TOEZICHT OP DE OPVOLGING VAN POLITIEKE MANDATARISSEN

In (parlementaire) debatten werd reeds veelvuldig de vraag gesteld of en in welke mate de Belgische inlichtingendiensten politieke mandatarissen (mogen) opvolgen en welke regels ze daarbij in acht moeten nemen.[112]

Vanaf begin 2018 wordt in deze binnen de VSSE de als 'vertrouwelijk' geclassificeerde dienstnota van 13 december 2017 toegepast.[113] De VSSE zendt twee types van rapporten naar de minister van Justitie en de Premier, met kopie naar het Vast Comité I. Het betreft enerzijds punctuele rapporten over politieke man-

110 *Ce contrôle sera périodique et comportera, outre un examen des processus et un contrôle de caisse, un contrôle formel réalisé par sondage et portant sur l'existence des pièces justificatives conformes aux instructions et approuvées par les fonctionnaires compétents. Le contrôle ne portera pas sur le bien-fondé ou la bonne gestion des opérations sous-jacentes et sera mis en œuvre, dans le respect des missions du SGRS, par des auditeurs disposant de l'habilitation de sécurité requise*".

111 VAST COMITE I, *Activiteitenverslag 2015*, 12-15 ('Het beheer, het gebruik en de controle van de speciale fondsen').

112 VAST COMITE I, *Activiteitenverslag 2008*, 22-33 (II.2. 'Gereserveerde dossiers' bij de Veiligheid van de Staat). Het was overigens niet voor het eerst dat het Comité de activiteiten van de inlichtingendiensten ten aanzien van politieke mandatarissen onderzocht (VAST COMITÉ I, *Activiteitenverslag 1998*; 67 e.v.; *Activiteitenverslag 1999*, 12 e.v. Zie hierover ook *Activiteitenverslag 2013*, 37 e.v. ('II.4. De opvolging van politieke mandatarissen door de inlichtingendiensten').

113 Om de rapportage ten aanzien van de directie inzake disruptieve activiteiten te verbeteren, werd de dienstnota in juni 2020 geactualiseerd.

datarissen die bijdragen aan de totstandkoming van een dreiging alsook een trimestrieel overzicht van het geheel van documenten waarin melding wordt gemaakt van deze mandatarissen.[114] De minister van Justitie stemde daarbij in met het *'principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991'*.[115]

In uitvoering van de principes vermeld in bovenstaande dienstnota, werd het Comité in 2019 effectief door de VSSE van beide types van rapporten op de hoogte gesteld. Omwille van het feit dat er in 2018 gemeenteraadsverkiezingen en in 2019 regionale, federale en Europese verkiezingen plaatsvonden, kon een toenemende aandacht vastgesteld voor politici worden vastgesteld. Immers, in de directe periode voor of na de verkiezingen ziet de VSSE voor zichzelf een rol weggelegd om het goede verloop van deze verkiezingen mee te bewaken, althans wat betreft de dreigingen waarop de VSSE volgens de wet dient toe te zien (bijv. inmenging). Specifiek rond de mogelijke Russische online dreigingen (cyber, desinformatie) ten aanzien van de verkiezingen van mei 2019 werd daarenboven een gezamenlijk project opgezet met de militaire inlichtingendienst en werd daarnaast regelmatig overleg gepleegd met het Belgische cybersecurity Center (BCC) en het Federaal Crisicentrum (ADCC).[116]

Ondanks herhaaldelijk verzoek mocht het Comité van de ADIV – die net zoals de VSSE werd aangespoord tot aanname van een uniforme richtlijn met klare en eenduidige regels met betrekking tot de inwinning, verwerking, raadpleging, opslag en archivering aangaande politieke mandatarissen – in 2019 geen informatie in die zin ontvangen. De ADIV beschikte niet over een specifieke procedure (SOP) om met deze informatie om te gaan noch werd bepaald hoe het Vast Comité I hiervan op de hoogte te brengen.

Gezien nergens wordt vermeld wat het Comité wordt geacht aan te vangen met voormelde informatie, nam het zelf het initiatief een methodologie uit te werken omtrent de 'problematiek van de opvolging van de politieke mandatarissen door de inlichtingendiensten en de rol van het Vast Comité I'. Deze methodologie werd in 2020 door de parlementaire Begeleidingscommissie goedgekeurd.

---

114 De bedoelde politieke mandatarissen zijn de ministers van de diverse regeringen, de Belgische commissaris in de Europese Commissie en de leden van de verschillende Parlementen, inclusief de Belgische leden van het Europees Parlement. Het gaat niet om andere verkozenen of aangeduide mandatarissen (bijv. op gemeentelijk vlak, zoals schepenen, of op provinciaal vlak, bijv. de gouverneurs).

115 *'met het toezichtsbeginsel/beginsel van verificatie/ dat noodzakelijk blijkt conform de organieke wet van 18 juli 1991'* (vrije vertaling) In: Brief van de minister van Justitie gericht aan het Vast Comité I d.d. 26 juli 2018 over 'Le recueil d'informations par un service de renseignement concernant une persone exerçant un mandat politique'.

116 In de loop van 2019 werd door het Vast Comité I omtrent deze materie het 'Toezichtonderzoek naar de wijze waarop de inlichtingendiensten een mogelijke inmenging van buitenlandse diensten in Belgische verkiezingen opvolgen, de eventuele bedreigingen tegen trachten te gaan, er over rapporteren aan de autoriteiten, en in het bijzonder wat betreft het gevaar van cyberinmenging of cyberaanvallen op dit vlak' opgestart (cf. I.7.4).

IV.4. DAG HAMMARSKJÖLD EN DE BELGISCHE INLICHTINGENARCHIEVEN

In de nacht van 17 op 18 september 1961 kwam de toenmalige Secretaris-generaal van de Verenigde Naties, Dag Hammarskjöld, om het leven bij een vliegtuigongeluk tijdens een vredesmissie in Congo. Hoewel er vermoedens waren dat het om een aanslag ging, werd de oorzaak van de vliegtuigcrash nooit opgehelderd.

Voormalig secretaris-generaal van de VN Ban Ki-Moon stelde in 2017 een onderzoek in, onder leiding van *Eminent Person* Mohamed Chande Othman.[117] Daarin werden lidstaten die relevante informatie over het dossier hebben, gevraagd om een onafhankelijke persoon aan te duiden om hun archieven te (laten) onderzoeken en de resultaten hiervan aan de VN te bezorgen. Op 16 april 2018 duidden de ministers van Justitie en Defensie toenmalig voorzitter van het Vast Comité I, Guy Rapaille[118] en Professor Kris Quanten, Luitenant-kolonel en docent aan de Koninklijke Militaire School aan als '*independent and high-ranking officials*' om de VN bij te staan in het onderzoek naar de dood van de Secretaris-generaal. Eind september 2018 legden zij hun verslag neer bij de VN. Begin november 2018 kreeg de Algemene Vergadering van de Verenigde Naties van Othman een eerste tussentijdse verslag, een eindverslag volgde in 2019.[119, 120]

Eind januari 2019 werd België door Judge Othman gevraagd om de reikwijdte van het onderzoek uit te breiden. Deze vraag kwam er als gevolg van bepaalde informatie die in de onderzoeken in andere landen aan het licht kwam.[121] Meer bepaald werd gevraagd om na te gaan over welke informatie de Belgische inlichtingendiensten beschikten met betrekking tot de aanwezigheid en/of activiteiten van inlichtingen- en defensiepersoneel van ander landen in Katanga in september 1961. In juni 2019 werd de VN hierover een rapport toegestuurd.[122] Het Comité kwam, samen met Luitenant-Kolonel Quanten van de Koninklijke Militaire

---

117 UNITED NATIONS, General Assembly, *71/260 Investigation into the conditions and circumstances resulting in the tragic death of Dag Hammerskjöld and of the members of the party accompanying him*, Resolution adapted on 23 December 2016, 31 January 2017, A/RES/71/260 (en A/C.5/72/19).

118 Ingevolge de oprusttelling van Guy Rapaille verzochten de ministers van Justitie en Buitenlandse Zaken halfweg maart 2019 dat het Vast Comité I een van zijn leden zou aanstellen om het onderzoek verder te voeren. Het Comité besliste deze opdracht toe te vertrouwen aan zijn voorzitter Serge Lipszyc.

119 De thematiek vormde opnieuw het onderwerp van een film (*Cold Case Hammerskjöld* van M. BRÜGGER) en diverse publicaties (H. MELBER, *Dag Hammerskjöld, the United Nations and the decolonisation of Africa*, Hurst Publishers, Londen, 2019; M. PICARD, *Ils ont tué Monsieur H. Congo 1961. Le complot des mercenaires français contre l'ONU*, Seuil, 2019).

120 Zie: www.hammarskjoldinquiry.info/pdf/ham_263_UN_Final_Report_complete.pdf.

121 In dat kader verzochten de Franse, Zweedse en Duitse *Independent Appointees* om een wederzijdse uitwisseling van de interim-rapporten.

122 BELGIAN STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE, Review investigation of the information available to the intelligence services regarding the death of Dag Hammarskjôld. Final Report, June 2019, 29.

School tot de conclusie dat *"the research carried out […] within the framework of this investigation, did not reveal any information that sheds new light on the precise circumstances that led tot he death of Mr. Dag Hammarskjöld and his company in September 1961"*.[123] Begin 2020 kon op basis van nieuwe inlichtingen bijkomende verduidelijkingen worden aangebracht.

123 '*De studie die in het kader van dit onderzoek werd uitgevoerd, heeft geen informatie opgeleverd die een nieuw licht werpt op de precieze omstandigheden die hebben geleid tot de dood van Mr. Dag Hammarskjöld en zijn gezelschap in september 1961' (vrije vertaling).*

HOOFDSTUK V
HET VAST COMITÉ I ALS BEVOEGDE TOEZICHTHOUDENDE AUTORITEIT IN HET KADER VAN DE VERWERKING VAN PERSOONSGEGEVENS

V.1. INLEIDEND

De Algemene Verordening Gegevensbescherming 2016/679 (AVG)[124] en de Richtlijn 2016/680 (Richtlijn)[125] regelen de wijze waarop publieke en private actoren dienen te handelen wanneer zij persoonsgegevens verzamelen, opslaan, bewaren en doorgeven. Beide Europese instrumenten gaven aanleiding tot enkele belangrijke wetswijzigingen op nationaal vlak: in december 2017 werd de Gegevensbeschermingsautoriteit (GBA)[126] – de opvolger van de Privacycommissie – opgericht en in juli 2019 werd een nieuwe Gegevensbeschermingswet (GBW) gestemd.[127] Deze wet wijzigde op zijn beurt de Toezichtwet van 18 juli 1991. Het Vast Comité I werd immers als gegevensbeschermingsautoriteit aangeduid voor verwerkingen van persoonsgegevens die kaderen binnen het domein van de 'nationale veiligheid'.

De rol van het Comité in deze staat omschreven in de Wet tot oprichting van de Gegevensbeschermingsautoriteit (GBA-Wet), in de Gegevensbeschermingswet (GBW) en in de Toezichtwet (W.Toezicht).[128]

---

124 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (AVG), *PB L* 2 mei 2016.

125 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en het vrije verkeer van die gegevens en tot intrekking van het Kaderbesluit 2008/977/JBZ van de Raad, *PB L* 4 mei 2016, afl. 119/89.

126 Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (GBA-Wet), *BS* 10 januari 2018.

127 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (GBW), *BS* 5 september 2018.

128 Hierover uitvoerig: VAST COMITÉ I, *Activiteitenverslag 2018*, 73-84.

In 2019 heeft het Comité diverse activiteiten ontwikkeld om deze bijkomende taak en verplichtingen waar te kunnen nemen. Reeds in 2018 werd een *Data Protection Officer* (DPO) voor alle verwerkingen van het Comité die buiten de 'nationale veiligheid' vallen (bijv. verwerkingen in het kader van het personeelsbeheer en logistiek) aangesteld. Verder werden diverse vergaderingen gehouden met de drie andere bevoegde toezichthoudende overheden (*infra, V.2*). Met het Vast Comité P werden afspraken gemaakt om een voorstel tot wijziging van de Toezichtwet uit te werken. Diverse bepalingen zijn immers niet aangepast aan de nieuwe bevoegdheid van de twee Comités. Ten slotte heeft het Comité een aantal interne werkprocessen uitgewerkt voor de adviesfunctie en de onderzoeken op klacht van burgers.

In wat volgt wordt gerapporteerd over deze bijzondere rol van het Comité: achtereenvolgens wordt de samenwerking tussen de diverse bevoegde toezichthoudende autoriteiten besproken, is er aandacht voor de controle op persoonsgegevensverwerkingen door BELPIU, voor de juridische adviesverlening van het Comité alsook voor de behandeling van individuele klachten. Dit alles past in het kader van artikel 35 § 3 W.Toezicht, dat stelt dat het Vast Comité I '*jaarlijks verslag uit[brengt] bij de Kamer van volksvertegenwoordigers omtrent de gegeven adviezen in zijn hoedanigheid van gegevensbeschermingsautoriteit, omtrent de onderzoeken die werden uitgevoerd en de maatregelen die werden genomen in dezelfde hoedanigheid alsook omtrent haar samenwerking met de andere gegevensbeschermingsautoriteiten*'.

V.2. SAMENWERKING TUSSSEN DE BEVOEGDE TOEZICHTHOUDENDE AUTORITEITEN

België telt op federaal niveau vier bevoegde toezichthoudende autoriteiten. Naast het Vast Comité I, zijn er de Gegevensbeschermingsautoriteit (GBA) die een algemene en residuaire bevoegdheid heeft, het Controleorgaan op de politionele informatie (COC), die vnl. verwerkingen controleert die kaderen binnen Titel 2 van de Gegevensbeschermingswet, en het Vast Comité P dat samen met het Vast Comité I controle uitvoert op verwerkingen van het OCAD (art. 161 GBW).

Behoudens dit laatste geval, handelt het Vast Comité I dus autonoom. Dit betekent niet dat er geen overleg of samenwerking is tussen de vier instanties, integendeel. De wet stelt bijvoorbeeld dat er in bepaalde gevallen moet of kan worden samengewerkt of dat er informatie moet worden uitgewisseld (artt. 98 en 131 GBW).

Belangrijker is de verplichting om nauw samen te werken, onder meer voor wat betreft de verwerking van klachten, adviezen en aanbevelingen die raken aan de bevoegdheden van twee of meerdere BTA's en dit met het oog op de consequente toepassing van de nationale, Europese en internationale regelgeving

inzake dataprotectie (art. 54/1 § 1 GBA-Wet). Deze bepaling stelt ook dat de gezamenlijke behandeling van klachten, adviezen en aanbevelingen aan de hand van het 'één-loketmechanisme' moet gebeuren. Deze functie wordt waargenomen door de Gegevensbeschermingsautoriteit. Tevens moeten de BTA's een protocol afsluiten met het oog op de verwezenlijking van de vereiste samenwerking; in 2019 werd een dergelijk samenwerkingsprotocol voorbereid en onderhandeld door de verschillende diensten.[129] Het protocol werd gefinaliseerd halfweg 2020.

V.3. DE CONTROLE OP PERSOONSGEGEVENSVERWERKINGEN DOOR BELPIU[130]

V.3.1. CONTROLE OP BELPIU GEKADERD

Met de Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens (PNR-Wet), wordt uitvoering gegeven aan de Europese doelstellingen om tegelijk terrorisme en samenhangende ernstige misdrijven te voorkomen en te bestrijden.[131] Daarvoor werd binnen de FOD Binnenlandse Zaken een zogenaamde 'passagiersinformatie-eenheid' (PIE) opgericht die de passagiersgegevens in een gegevensbank bijhoudt met het oog op het voorkomen en bestrijden van de in de PNR-Wet vastgelegde misdrijven of dreigingen.

Op grond van ondertitel 5 van Titel 3 van de GBW is het Vast Comité I de bevoegde toezichthoudende autoriteit ten aanzien van "*elke verwerking van persoonsgegevens door de PIE in het kader van de finaliteiten bedoeld in artikel 8, § 1, 4°, van de wet van 25 december 2016*" (art. 169 GBW) of met andere woorden verwerkingen die kaderen "*in de artikelen 7, 1° en 3°/1 en 11, § 1, 1° tot 3° en 5° van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst*" (art. 8, § 1, 4° PNR-Wet). Bedoeld wordt met andere woorden verwerkingen die door de VSSE en de ADIV gebeuren in het kader van hun reguliere inlichtingenopdracht. Het Comité is alleen bevoegd om de werking van de PIE te controleren in de mate waarin ze haar medewerking verleent aan de vragen om informatie en inlichtingen komende van een van de twee inlichtingendiensten, ongeacht of dit gebeurt onder de vorm van gerichte zoekingen, *watchlists* of profielen.

---

129 De wetgever voorziet trouwens in een evaluatie van de Gegevensbeschermingswet drie jaar na de inwerkingtreding (art. 283 GBW). Een van de aspecten die daarbij aan bod zal moeten komen is de samenwerking tussen de verschillende BTA's.

130 BELPIU staat voor *Belgian Passenger Information Unit*.

131 De PNR-Wet is de omzetting van de Richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van passagiersgegevens voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (PNR-richtlijn) en de Richtlijn 2004/82/EG van de Raad van 29 april 2004 betreffende de verplichting voor vervoerders van passagiersgegevens door te geven (API-richtlijn).

V.3.2. EEN GELIJKTIJDIGE (BEPERKTE) VISITATIE

Gelet op hun respectieve bevoegdheden als bevoegde toezichthoudende autoriteiten ten aanzien van de gegevensverwerkingen door de passagiersinformatie-eenheid, beslisten het Controleorgaan op de politionele informatie (COC) en het Vast Comité I op eigen initiatief gelijktijdig een (beperkte) visitatie te verrichten bij deze dienst.[132] Immers, de bevoegdheden van beide diensten ten aanzien van de PIE zijn dan wel niet volledig identiek, maar minstens overlappend.[133] De visitatie was niet het gevolg van een (individuele) klacht of het bestaan van (concrete) aanwijzingen over het niet naleven van de wet- en regelgeving.

De invalshoek van de visitatie was opgezet met de nadruk op *compliance based*: gebeurt de verwerking van passagiersgegevens in overeenstemming met de wet en wordt daarbij een hoge veiligheidsstandaard gehanteerd? De visitatie was meer gericht op informatieveiligheid dan op juridische aspecten.[134]

De reden voor een beperkte visitatie was eenvoudig. Om te beginnen was de PIE pas operationeel sinds begin 2018. Daarnaast waren nog niet alle geviseerde passagiersvervoerders en reisoperatoren technisch geconnecteerd met de PIE. De visitatie was beperkt tot twee domeinen, te weten enerzijds de ICT-beveiliging en informatieveiligheid en anderzijds de proportionaliteit van de gegevensverwerking. Het onderzoeksrapport werd in juni 2020 gefinaliseerd en voorgesteld aan de parlementaire Begeleidingscommissie.

V.4. ADVIESVERLENING

Het Comité kan in twee gevallen een advies verlenen '*over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin de beleidslijnen van de bevoegde ministers worden geformuleerd*': wanneer de wet zijn advies oplegt of op verzoek van de Kamer van Volksvertegenwoordigers of van de bevoegde minister (art. 33, zesde lid W.Toezicht). Dergelijk advies heeft specifiek betrekking op de problematiek van de gegevensverwerkingen en moet dus onderscheiden worden van de algemene adviesbevoegdheid die bijvoorbeeld ook betrekking kan hebben op de efficiëntie en de coördinatie. Deze algemene adviesbevoegdheid is in die zin ruimer, maar ze is ook enger aangezien ze beperkt is tot de werking van de inlichtingendiensten en het OCAD.

In deze hoedanigheid verleende het Comité in 2019 alleen of éénmaal samen met het Vast Comité P, negen adviezen bij ontwerpen van wet of ontwerpbeslui-

132 De visitatie vond plaats op 27 november 2019.

133 Deze visitatie had geen betrekking op de wijze waarop de twee Belgische inlichtingendiensten hun bevoegdheden in dit kader hanteren. Dit aspect werd door het Comité behandeld in een apart toezichtonderzoek dat in 2019 werd opgestart (cf. I.7.2).

134 Deze invalshoek stond er niet aan in de weg dat het COC of het Vast Comité I gepaste maatregelen neemt wanneer evidente wettelijke tekortkomingen worden vastgesteld.

ten. De voorbereiding van deze adviezen impliceerde een omvangrijke bijkomende werklast voor het Comité. De adviezen zelf zijn integraal te raadplegen op de website van het Comité (www.comiteri.be/adviezen). Hier wordt volstaan met een opsomming van de verleende adviezen:

- Advies 001/VCI-BTA/2019 van 5 februari 2019 met betrekking tot '*een voorontwerp van wet tot wijziging van de Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens*';
- Advies 002/VCI-BTA/2019 van 9 april 2019 met betrekking tot het '*voorontwerp van koninklijk besluit tot wijziging van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten*';
- Advies 003/VCI-BTA/2019 van 27 juni 2019 met betrekking tot '*het voorontwerp van wet houdende wijziging aan de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen*';
- Advies 004/VCI-VCP-BTA/2019 van 27 juni 2019 aangaande een vraag tot advies van de minister van Binnenlandse Zaken met betrekking tot '*het voorontwerp van wet betreffende de gemeentelijke bestuurlijke handhaving en houdende oprichting van een Directie Integriteitsbeoordeling voor Openbare besturen (OCAD)*';
- Advies 005/VCI-BTA/2019 van 3 juli 2019 aangaande een vraag tot advies van de minister van Binnenlandse Zaken met betrekking tot '*het voorontwerp van wet betreffende de gemeentelijke bestuurlijke handhaving en houdende oprichting van een Directie Integriteitsbeoordeling voor Openbare besturen (VSSE – ADIV)*';
- Advies 006/VCI-BTA/2019 van 23 augustus 2019 aangaande een vraag tot advies van de minister van Buitenlandse Zaken met betrekking tot het '*Wetsontwerp houdende instemming met de Overeenkomst tussen het Koninkrijk België en de Republiek Cyprus inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 20 juli 2015*';
- Advies 007/VCI-BTA/2019 van 23 augustus 2019 aangaande een vraag tot advies van de minister van Buitenlandse Zaken met betrekking tot het '*Wetsontwerp houdende instemming met de Overeenkomst tussen het Koninkrijk België en Hongarije inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Budapest op 21 september 2015*';
- Advies 008/VCI-BTA/2019 van 23 augustus 2019 aangaande een vraag tot advies van de minister van Buitenlandse Zaken met betrekking tot het '*Wetsontwerp houdende instemming met de Overeenkomst tussen het Koninkrijk België en de Republiek Finland inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Helsinki op 20 juli 2016*';

– Advies 009/VCI-BTA/2019 van 23 augustus 2019 aangaande een vraag tot advies van de minister van Buitenlandse Zaken met betrekking tot het '*Wetsontwerp houdende instemming met de Overeenkomst tussen het Koninkrijk België en het Koninkrijk Spanje inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 15 oktober 2015*'.

In februari 2019 werd de Voorzitter van het Vast Comité I uitgenodigd voor een hoorzitting in de Commissie voor de Justitie om toelichting te geven bij het in 2018 geformuleerde advies[135] inzake het wetsvoorstel houdende diverse bepalingen in strafzaken en inzake erediensten.[136]

V.5. INFORMATIE VAN DE GECONTROLEERDE DIENSTEN

De door het Comité gecontroleerde diensten moeten een aantal gegevens ter beschikking houden of stellen van het Vast Comité I.[137] Het betreft:
– indien een inbreuk op de beveiliging een hoog risico voor de rechten en vrijheden van natuurlijke personen inhoudt, meldt de verwerkingsverantwoordelijke deze inbreuk binnen de kortste termijn aan het Vast Comité I en indien mogelijk, 72 uur nadat hij er kennis van heeft gekregen (artt. 89, 122, 155 en 180 GBW);
– een register met informatie over de gehanteerde gegevensbanken of verwerkingsactiviteiten (artt. 90, 123, 156 en 181 GBW);
– de aanstelling van een functionaris voor gegevensbescherming (of *Data Protection Officer* (DPO)) door de verwerkingsverantwoordelijke of de verwerker (artt. 91, 124 en 127 GBW).

Er werden in 2019 geen *data breaches*[138] gemeld aan het Comité. Het Comité mocht ook geen registers ontvangen met informatie over gegevensbanken of verwerkingsactiviteiten. De autoriteiten waarvoor bevoegd, werden door het Comité aangeschreven met oog op de samenstelling van een overzicht van de aangestelde functionarissen voor gegevensbescherming.

---

135 Advies 008/VCI-BTA/2018, beschikbaar op www.comiteri.be/advies (Nieuwe inlichtingenmethoden en beschermings- en ondersteuningsmaatregelen (2018)).

136 *Parl. St.* Kamer, 2018-19, 54K3515/001.

137 Niet elke dienst moet alle hier vermelde gegevens bijhouden of ter beschikking stellen. Dit geldt bijvoorbeeld zeker wat betreft de BIM-Commissie die geen informatie moet meedelen aan het Vast Comité I.

138 Een *personal data breach* of 'inbreuk in verband met persoonsgegevens' wordt gedefinieerd als *'een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens*' (art. 4 AVG).

Het Comité zal, gezien de vooralsnog te beperkte kennis van deze complexe wetgeving door de gecontroleerde diensten, verder waken over de correcte toepassing ervan.

V.6. BEHANDELING VAN INDIVIDUELE DPA-KLACHTEN

Het Vast Comité I behandelt eveneens individuele verzoeken met betrekking tot de verwerkingen van persoonsgegevens door de hogervermelde personen en diensten en hun verwerkers (art. 34 W.Toezicht en artt. 79, 113, 145 en 173 GBW). De verzoeker heeft daarbij het recht te vragen om zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen en om te laten verifiëren of de toepasselijke regels inzake dataprotectie werden nageleefd. Om ontvankelijk te zijn, moet het verzoek geschreven, gedateerd, ondertekend en met redenen omkleed zijn (art. 51/2 W.Toezicht).[139] Indien het verzoek kennelijk niet gegrond is, kan het Comité besluiten geen gevolg te geven aan het verzoek. Deze beslissing moet worden gemotiveerd en schriftelijk ter kennis gebracht van de verzoeker.[140]

In 2018 ontving het Vast Comité vijf DPA-klachten van burgers die betrekking hadden op eventuele verwerkingen van persoonsgegevens door de VSSE en de ADIV, waarvan er vier werden afgehandeld in 2019. In 2019 kreeg het Comité veertien klachten, waarvan drie niet tot de bevoegdheid van het Comité behoorden (maar wel tot deze van het COC) en één klacht als ontvankelijk maar kennelijk niet gegrond werd beoordeeld. Acht van deze nieuwe klachten konden nog in 2019 worden afgehandeld.[141] In deze dossiers werden de vereiste verificaties uitgevoerd. De klagers werden hiervan in kennis gesteld.[142] De leidinggevende ambtenaar van de inlichtingendienst of de directeur van het OCAD – en naar het Comité aanneemt, ook een andere instantie of persoon – krijgt '*de besluiten van het onderzoek*' (art. 34, laatste lid W.Toezicht). De drie nog openstaande DPA-klachten (waarvan één uit 2018 en twee uit 2019), konden in 2020 worden afgehandeld.

---

139 Deze bepaling stelt ook dat het verzoek '*de identiteit van de betrokkene [moet] rechtvaardigen*.' Het is niet meteen duidelijk wat hiermee wordt bedoeld. Waarschijnlijk wordt bedoeld dat hij zijn identiteit moet bewijzen. Die verplichting is namelijk opgenomen in de betrokken bepalingen van de Gegevensbeschermingswet (zie artt. 80, 114, 146 en 174 GBW).

140 Deze verificaties gebeuren kosteloos (artt. 80, 114, 146 en 174 GBW).

141 Eén klacht werd samen afgehandeld met het Vast Comité P.

142 *'De betrokkene heeft het recht om zijn onjuiste persoonsgegevens te laten verbeteren of verwijderen'* (art. 79 GBW). *'Het Vast Comité I voert de verificatie uit en deelt uitsluitend aan de betrokkene mee dat de nodige verificaties werden verricht'* (art. 80 GBW), en dus zonder dat hierover nadere toelichting kan worden verstrekt.

HOOFDSTUK VI
DE CONTROLE VAN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN

In 2016 werd door de ministers van Binnenlandse Zaken en Justitie de gemeenschappelijke gegevensbank '*foreign terrorist fighters*' (GGB FTF) opgericht. De doelstelling ervan was bij te dragen tot de analyse, de evaluatie en de opvolging van personen met banden met deze problematiek. Deze gemeenschappelijke gegevensbank (GGB) werd in 2018 omgevormd: ze heet voortaan gemeenschappelijke gegevensbank '*terrorist fighters*' (GGB TF) en omvat naast de (bestaande) algemene categorie van de '*foreign terrorist fighters*' tevens een nieuwe categorie van '*homegrown terrorist fighters*'. Daarnaast werd in 2018 ook een aparte gemeenschappelijke gegevensbank opgericht voor '*haatpropagandisten*' (GGB HP).[143]

Bij Koninklijk besluit van eind 2019[144] ten slotte, werden nog twee bijkomende categoriën van personen in de GGB TF opgenomen, zijnde de 'potentieel gewelddadige extremisten' (PGE) en 'terrorisme-veroordeelden' (TV).

VI.1. DE BELANGRIJKSTE WIJZIGINGEN AAN DE REGELGEVING

VI.1.1. DE FUNCTIONARIS VOOR GEGEVENSBESCHERMING

De Wet van 22 mei 2019[145] wijzigde de WPA om deze in overeenstemming te brengen met de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke

143 Artikel 44/6 WPA wijst de controle op de verwerking van de in de GGB vervatte informatie en persoonsgegevens toe aan het Controleorgaan op de politionele informatie (COC) en aan het Vast Comité I (verder 'de toezichthoudende autoriteiten').

144 KB van 20 december 2019 tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank terrorist fighters en van het Koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de wet op het politieambt, *BS* 27 januari 2020.

145 Wet van 22 mei 2019 tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft, *BS* 19 juni 2019.

personen met betrekkking tot de verwerking van persoonsgegevens (Gegevensbeschermingswet). De functie 'consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer' werd vervangen door 'de functionaris voor gegevensbescherming' (art. 44/11/3*quinquies*/1 WPA). Deze functionaris wordt belast met:
- het verstrekken van deskundige adviezen inzake informatieveiligheid, inzake bescherming van gegevens en inzake hun verwerking. In het bijzonder waakt hij over de eerbiediging van de algemene voorwaarden voor de rechtmatigheid van de verwerking met betrekking tot verwerkingen van persoonsgegevens;
- het toepassen, het bijwerken en het controleren van een beleid inzake beveiliging en bescherming van gegevens;
- het uitvoeren van andere opdrachten inzake bescherming van gegevens en de beveiliging die bepaald worden door de Koning of die hem door de ministers van Binnnenlandse Zaken en Justitie worden toevertrouwd.

Deze opdracht wordt uitgevoerd aanvullend met de in de Gegevensbeschermingswet voorziene opdrachten als functionaris voor gegevensbescherming.

VI.1.2. KONINKLIJK BESLUIT VAN 20 DECEMBER 2019

Het Koninklijk besluit van 20 december 2019 (*supra*) beoogt een drieledig doel. Vooreerst worden nieuwe categorieën toegevoegd aan de gemeenschappelijke gegevensbank TF, te weten de 'potentieel gewelddadige extremisten' en de 'terrorisme-veroordeelden'. Daarnaast worden een aantal zogenaamde 'technische wijzigingen' aangebracht aan de KB's TF en HP tengevolge de wijziging van de Wet van 5 augustus 1992 door de Wet van 22 mei 2019. Ten slotte was het opzet te voorzien in een directe toegang voor de Algemene administratie van de Thesaurie van de FOD Financiën tot de gegevensbanken TF en HP.

VI.1.2.1. De toevoeging van potentieel gewelddadige extremisten (PGE) in de GGB TF

De 'potentieel gewelddadige extremist' wordt gedefinieerd als elke natuurlijke persoon die een aanknopingspunt heeft met België en voldoet aan onderstaande, cumulative criteria:
a) ze hebben extremistische opvattingen die het gebruik van geweld of dwang als actiemethode in België legitimeren;
b) er zijn betrouwbare aanwijzingen dat ze de intentie hebben om geweld te gebruiken, en dit in verband met de opvattingen vermeld in a);
c) en daarenboven, dient te PGE te voldoen aan ministens één van de volgende criteria die het risico op geweldpleging verhogen:
   - ze hebben systematische sociale contacten binnen extremistische milieus;

- ze hebben een psychische problematiek, vastgesteld door een daartoe gekwalificeerde deskundige;
- ze pleegden daden of stelden antecedenten die beschouwd kunnen worden als a) een misdaad of wanbedrijf die de fysieke of psychische integriteit van derden aantast of bedreigt; ofwel b) onderrichtingen of een opleiding voor de vervaardiging of het gebruik van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, dan wel voor andere specifieke methoden en technieken nuttig voor het plegen van terroristische misdrijven; ofwel c) bewuste handelingen die als materiële steun voor een terroristische/extremistische organisatie of netwerk gelden; ofwel d) feiten die door hun aard wijzen op een verontrustend veiligheidsbewustzijn in hoofde van de betrokkene.

VI.1.2.2. De toevoeging van terrorisme-vervoordeelden (TV) in de GGB TF

Het betreft personen die voldoen aan onderstaande cumulatieve voorwaarden:
- ze hebben een aanknopingspunt met België;
- ze werden veroordeeld of kregen een gerechtelijke beslissing tot internering, of in het geval van minderjarigen, die een beschermingsmaatregel kregen voor terroristische misdrijven zoals bepaald in Boek 2, Titel I Ter van het Strafwetboek (in België), of voor gelijkaardige inbreuken in het buitenland;
- en waarvan het niveau van dreiging dat van hen uitgaat door het OCAD wordt ingeschaald als gemiddeld (niveau 2), ernstig (niveau 3) of zeer ernstig (niveau 4).

Door de invoering van deze nieuwe categorie in de gegevensbank TF, worden alle actoren die een opvolging moeten verzekeren van terrorisme-veroordeelden (zoals DG EPI, Justitiehuizen, Politie, gesloten asielcentra, de VSSE, de Lokale Task Forces …) proactief, op tijd en volledig geïnformeerd over de betrokkenen.

VI.1.2.3. Rechtstreekse toegang tot de GGB TF en HP voor een nieuwe dienst

Middels het KB van 20 december 2019 zag ook de Algemene administratie van de Thesaurie zich een rechtstreekse toegang toegekend tot de GGB TF en HP.[146] Het betreft *in casu* de bevoegde overheid op het vlak van financiële sancties door het bevriezen van tegoeden en economische middelen van personen of entiteiten die terroristische misdrijven plegen of pogen te plegen, ze vergemakkelijken of eraan meewerken.

[146] Er dient te worden opgemerkt dat de toegang voor de Algemene adminstratie van de Thesaurie niet figureerde in het ontwerp KB noch in de bijkomende voorafgaandelijke aangifte dewelke werd voorgelegd aan het COC en het Vast Comité I.

VI.2. DE CONTROLEOPDRACHT

VI.2.1. HET VOORWERP VAN CONTROLE

Voor wat betreft 2019, beslisten het COC en het Vast Comité I om de gezamenlijke controle te focussen op enerzijds de opvolging van bepaalde aanbevelingen die in de rapporten van de afgelopen jaren werden geformuleerd en anderzijds op de bevraging van een aantal basis- en partnerdiensten inzake rechtmatigheidscontroles en de interne procedures om de gegevensverwerking van informatie in de GGB TF en HP vlot te laten verlopen.[147]

Daarnaast werd eveneens ingezoomd op de coördinatie van de gegevensverwerking van informatie in de GGB TF en HP, onder meer met aandacht voor de rol van de *data protection officer* (DPO). Het stijgend aantal diensten dat een toegang heeft tot de GGB TF en HP werd daarbij eveneens in rekening genomen.

VI.2.2. OPVOLGING VAN DE AANBEVELINGEN

VI.2.2.1. De aanwijzing van de functionaris van de gegevensbescherming

Begin september 2019 werd door de ministers van Justitie en Binnenlandse Zaken gezamenlijk een DPO aangesteld voor de GGB TF en HP.[148] Deze functionaris is de bevoorrechte gesprekspartner van het COC en het Vast Comité I.

VI.2.2.2. De indeplaatsstelling van een mechanimse voor het melden van veiligheidsincidenten

Om een veiligheidsincident te melden, is er een tabblad beschikbaar op het toepassingsscherm.[149] De gebruiker van de toepassing kan aldus een rapport opmaken over het vastgestelde probleem en de DPO van de betreffende dienst(en) heeft toegang tot een overzicht van alle incidenten die met betrekking tot de GGB TF en HP werden opgeslagen. Voor een goed begrip van de gebruiker worden de beheersvoorschriften voor veiligheidsincidenten omschreven op het scherm.

---

147 De nieuwe categorieën PGE en TV werden ingevoerd middels het KB van 20 december 2019, dat verscheen in het Belgisch Staatsblad op 27 januari 2020. Ze maakten aldus geen voorwerp van controle uit in 2019.

148 Het COC en het Vast Comité I namen nota van het feit dat deze functie gecumuleerd wordt met enerzijds de functie van DPO bij het OCAD, en anderzijds met materiële werkzaamheden bij datzelfde OCAD. Er kon nog niet worden beoordeeld of de materiële tijdsbesteding voorzien voor deze functie volstaat alsook welke wending het risico op de belangenconflicten neemt.

149 Dewelke toegang verleent tot de gemeenschappelijke gegevensbank TF en PH.

De te volgen procedure werd gedefinieerd in de handleiding. Hoewel dit eerder al werd aangekaart, blijkt dat de handleiding geen gewag maakt van een extern datalek dat routinematig aan het COC en het Vast Comité I dient te worden gemeld, en dit terwijl deze werkwijze een aanbeveling uitmaakte aan de Federale Politie in de zin van artikel 44/11/3*quinquies*/2 laatste lid WPA.

VI.2.2.3. De uitvoering van aanvullende informatica-ontwikkelingen

Eerder werd vastgesteld dat het OCAD niet over een informaticatool beschikte dat de opvolging mogelijk maakte van de bewaringstermijnen en de verwijdering van gegevens van personen die voorkomen (of voorkwamen) in één van de vijf FTF categorieën. Deze vastsstelling bracht de toezichthoudende autoriteiten er toe om hun aanbeveling inzake de ontwikkeling een informatiecatool te herhalen.

In 2019 werd een controle uitgevoerd aangaande 487 entiteiten dewelke minstens drie jaar voorkwamen in de GGB FTF. Voor 485 van deze entiteiten verwees het OCAD naar *'de logische workflow waarbij geen anomalieën werden vastgesteld'*. Het OCAD verstrekte daarbij een nuttige toelichting. Niettemin werd de aanbeveling om een informaticatool te ontwikkelen die het mogelijk maakt de bewaringstermijnen van gegevens die worden bedoeld in artikel 44/11/3*bis* § 5 WPA op te volgen, herhaald.

VI.2.2.4. Een spontane controle van de loggings

Wat betreft de spontane controle van de loggings, dient blijkens informatie van de Federale Politie, een onderscheid te worden gemaakt tussen een 'kleine logging'[150], een 'grote logging'[151] en een 'rechtmatigheidscontrole'. Het loggingsverzoek kan worden gedaan via de gebruikers-ID.

De Federale Politie meldde binnen hun eigen diensten in 2019 73 verzoeken om loggings te hebben ontvangen, waaronder 71 kleine loggings en twee via het tabblad 'rechtmatigheidscontrole'. Er werd geen 'grote logging' aangevraagd.

Het COC en het Vast Comité I wezen op het belang om eveneens een grote loggingscontrole uit te voeren. Binnen de partnerdiensten was het noodzakelijk om het bewustzijn te verhogen omtrent deze rechtmatigheidscontroles, die systematisch dienen te worden uitgevoerd.

---

150 Een 'kleine logging' is een logging met betrekking tot de verwerking die wordt uitgevoerd op een entiteit van de gemeenschappelijke database en is toegankelijk voor alle gebruikers met lees- en schrijfrechten.

151 Een 'grote logging' is een logging met betrekking tot de verwerking door de gebruikers van de gemeenchappelijke database en kan enkel worden uitgevoerd door de Federale Politie als beheerder.

VI.2.2.5. De uitzondering op de verplichting om politionele informatie op te nemen in de GGB

Er bestaan twee afwijkingen op de verplichting om de gemeenschapplijke gegevensbanken te voeden (art. 44/11/3*ter* § 5 WPA). In de eerste plaats kan de verplichting tot voeding worden uitgesteld zolang de bevoegde magistraat, met instemming van de federale procureur, meent dat deze voeding de uitoefening van de strafvordering of de veiligheid van een persoon in het gedrang kan brengen. Daarnaast kan de leidinggevende van een inlichtingendienst de doorgifte van gegevens uitstellen, wanneer en zolang hij van oordeel is dat de voeding de veiligheid van een persoon of de regel van de derde dienst in gevaar kan brengen.

In een voorgaand toezichtsrapport werd vastgesteld dat de politionele informatie uit informatierapporten (RIR) met de code 00 of 01, niet opgenomen werd in de GGB TF en HP. Deze codes resulteren uit de Omzendbrief MFO3 en betreffen de voeding van de Algemene Nationale Gegevensbank (ANG), maar de uitzondering is niet weerhouden in de reglementering betrefffende de GGB TF en HP. *De lege lata,* staat de wet en het uitvoeringsbesluit niet toe dat deze gegevens niet in de gemeenschappelijke gegevensbank zouden opgenomen worden.

De Federale Politie deelde de toezichthoudende autoriteiten mee dat een werkgroep LTF besloot om enkel de RIR 01 in de gemeenschappelijke gegevensbank op te nemen. Desgevallend kan de betrokken gebruiker verzoeken dat een RIR 01 waarnaar in de GGB TF en HP wordt verwezen, hem worden meegedeeld. Dit verzoek wordt dan geval per geval beoordeeld.

Het COC en het Vast Comité I merkten op dat deze praktijk louter gestoeld is op de (niet gepubliceerde) Omzendbrief van 14 juni 2002, dewelke op gespannen voet staat met de wettelijke bepalingen betreffende de voeding van de GGB TF en HP.

VI.2.2.6. Doorgifte van lijsten

In hun voorgaand toezichtsrapport, werd door het COC en het Vast Comité I de regelgeving en de voorwaarden om de doorgifte van lijsten legitiem te laten plaatsvinden, opgesomd. Daarbij werd herinnerd aan de eerder geformuleerde vaststelling over de noodzakelijk technische beveiliging van de doorgifte indien deze via e-mail gebeurt. Bovendien achtten ze het gepast dat de basisdienst die de doorgifte uitvoert, de ontvanger van de lijst naar behoren informeert.[152] Tot slot stelden de toezichthoudende autoriteiten zich vragen over de overheid/overheden die belast zijn met het controleren van de ontvangers betreffende het gebruik van de lijst en over de manier waarop een controle uitgevoerd zou kunnen worden.

Blijkens de controle uitgevoerd in 2019, bestond de praktijk er in dat een lijst van de persoonsgegevens en informatie in de GGB TF en HP per e-mail maande-

[152] Bijvoorbeeld door het sluiten van een vooragaand protocol tussen de diensten.

lijks wordt doorgegeven aan onder meer de FOD Werkgelegenheid, het FANC en Brussel Preventie & Veiligheid. Het COC en het Vast Comité I konden geen door de Federale Politie, het OCAD en de inlichtingen- en veiligheidsdiensten gezamenlijk opgestelde evaluatie terugvinden.[153] Ook de aanbeveling om de ontvangende diensten te informeren over de voorwaarden waaronder de lijst kan worden meegedeeld, bleek dode letter te zijn gebleven. In dat kader werden door het COC en het Vast Comité I in het bijzonder vragen gesteld over het feit dat de instelling Brussel Preventie & Veiligheid bestemmeling kon zijn van de lijsten, temeer daar deze instelling niet als nieuwe partnerdienst werd toegevoegd bij de wijziging van de regelgeving.[154]

Het COC en het Vast Comité I onderstreepten dat de mededeling van persoonsgegevens en informatie afkomstig van de gemeenschappelijke gegevensbank aan derde instanties aan strikte en cumulatieve wettelijke bepalingen is onderworpen. Voor wat betreft de noodzakelijke technische beveiliging van de doorgifte van lijsten, resulteerde de in 2019 uitgevoerde controle tot een herhaling van de aanbeveling tot het afsluiten van protocolakkkoorden met de diensten die bestemmeling zijn van de lijsten.

VI.2.3. HET GEBRUIK VAN DE GEMEENSCHAPPELIJKE GEGEVENSBANK TF EN HP DOOR DE PARTNERDIENSTEN

VI.2.3.1. Verificatie van de toegang tot de gegevensbank TF en HP door de partnerdiensten en de voeding ervan

Er werd nagegaan hoeveel gebruikers er per partnerdienst actief zijn, en hoeveel keren deze partnerdienst de toegang tot de gemeenschappelijke gegevensbank heeft gebruikt. Daaruit kon worden afgeleid dat in december 2019 zeventien van een lijst van zevenveertig partnerdiensten géén gebruik voorzagen voor de GGB TF en HP.

Met betrekking tot de partnerdiensten die voor meerdere jaren géén gebruiker en géén logins hebben aangeduid voor de GGB TF en HP, wezen het COC en het Vast Comité I op een mogelijk gebrek aan de 'behoefte om te kennen' en dient er te worden opgevolgd in welke mate (nog) aan de voorwaarden van artikel 44/11/3*ter* § 2 WPA is voldaan. Logischerwijze dient de al dan niet rechtstreekse toegang van bepaalde partnerdiensten in het kader van dat gebrek aan noodzaak te worden herzien.

---

153 Deze wordt opglegd door art.44/11/3 *quater* WPA en er wordt naar vewezen in art. 11 § 2 KB TF en HP.

154 Een juridische analyse betreffende Brussel Preventie & Veiligheid en de toegang tot de gemeenschappelijke gegevensbank Terrorist Fighters werd in september 2020 voorgelegd aan de Begeleidingscommissie.

VI.2.3.2. Beleid inzake beveiliging en bescherming van gegevens

Het COC en het Vast Comité I konden vaststellen dat de rol van functionaris voor de gegevensbescherming als een adviserende en coördinerende functie wordt gezien, waarbij de zoektocht naar een gemeenschappelijke visie gedragen door alle betrokken partnerdiensten, centraal staat. Hoewel het inderdaad niet de bedoeling kan zijn om beslissingen te nemen in de plaats van de verwerkingsverantwoordelijken, onderstreepten de toezichthoudende autoriteiten het initiatief dat van de functionaris van de gegevensbescherming voor de GGB TF en HP kan uitgaan om een eerste voorstel te voorzien. Immers, de ontwikkeling van een gemeenschappelijke benadering zou nodeloos vertraging kunnen oplopen indien het initiatief van de partnerdiensten zou worden afgewacht om (uiteenlopende) voorstellen te presenteren.

Het COC en het Vast Comité I deden de aanbeveling om hen een kopie te bezorgen van de beleidsnota's die de functionaris van de gegevensbescherming van de GGB TF en HP zal opmaken in het licht van de beleidskeuzes inzake beveiliging en bescherming van gegevens, meer specifiek in het kader van de toegang tot en de voeding van de GGB TF en HP. Trouwens, de DPO van de gemeenschappelijke gegevensbank beoogt een 'dynamisch' register van de verwerkingsactiviteiten op te stellen in de loop van het eerste kwartaal van 2020. In algemene bewoordingen werd toegelicht dat het dynamische karakter betrekking heeft op een oplossing die geïntegreerd is in elk van de gemeenschappelijke databanken en die zowel aan de wettelijke vereisten kan voldoen als gemakkelijk kan worden geactualiseerd. In afwachting zal in een 'gewoon' register van verwerkingsactiviteiten worden voorzien, dat algemeen blijft. Overigens zal de DPO in een eerste fase voorzien in een presentatiemodule[155] omvattende de principes van verwerking, de verplichtingen van de verschllende actoren betrokken bij de verwerking van persoonsgegevens en de rol van de DPO.

VI.2.3.3. Twee vaststellingen

Een eerste vaststelling betreft de Algemene administratie van de Thesaurie, wiens Cel financiële sancties is samengesteld uit vier personen die een persoonlijke toegang hebben tot de gemeenschappelijke gegevensbank. Uit het verslag aan de Koning kan worden opgemaakt dat deze Algemene administratie zich in een positie bevindt om de GGB TF en HP te voeden met relevante informatie. Deze toegang en de gehanteerde veiligheidsmaatregelen dienen evenwel nader te worden geëvalueerd.

Daarnaast houdt de regelgeving rekening met het onafhankelijk statuut van het Openbaar Ministerie, gezien er voor die partnerdiensten geen verplichting (maar wel een mogelijkheid) bestaat om de GGB TF en HP te voeden, ook al heeft

[155] Deze module zou operationeel moeten zijn in de eerste helft van.

ze een rechtstreekse toegang tot de gegevensbank TF. De wetgever heeft geoordeeld dat de gerechtelijke gegevens voornamelijk afkomstig zijn van de politiediensten. In die zin is de verplichting voor de politiediensten om de gemeenschappelijke gegevensbank te voeden voldoende opdat de pertinente gegevens van de gerechtelijke politie worden geregistreerd.[156]

Om zich ervan te vergewissen dat de voeding van de gegegevensbank TF goed wordt uitgevoerd, hebben de gerechtelijke overheden instructies verstuurd. Daarin werd opgenoen dat de parketten de GGB TF en HP niet zullen voeden. Wel voorziet de omzendbrief COL 10/2015 dat de limitatief opgesomde referentiemagistraten terrorisme aan het OCAD, op diens vraag, de informatie met betrekking tot het dossier waarvoor men bevoegd is meedelen wanneer de betrokken persoon het voorwerp uitmaak van een federaal onderzoek door het Federaal Parket. Ook de wijzigingen van deze gerechtelijke maatregelen worden meegedeeld aan het OCAD.

De omzendbrieven werden herzien en geactualiseerd in de schoot van het expertisenetwerk Terrorisme om te komen tot één geïntegreerde en geactualiseerde omzendbrief m.b.t. de gerechtelijke aanpak van *terrorist fighters* en haatpropagandisten. De functie van veiligheidsmagistraat zal daarbij worden opgegeheven en vervangen door een magistraat-veiligheidsofficier. Derhalve zal het Openbaar Ministerie niet meer afhangen van de veiligheidsofficier van de FOD Justitie, maar zal zij beschikken over haar eigen veiligheidsofficieren.

Er wordt beoogd de controle van de loggings van de GGB TF en HP in het takenpakket van de magistraat-veiligheidsofficier op te nemen. Thans zijn de nominatieve lijsten van alle magistraten en medewerkers van het Openbaar Ministerie die toegang hebben tot de gemeenschapplijke gegevensbank TF aangelegd door de veiligheidsmagistraat, maar nadat de verschillende bestaande omzendbrieven zullen opgaan in één nieuwe omzendbrief, zullen deze lijsten ter beschikking zijn bij één van de vijf bevoegde magistraat-veiligheidsofficieren (één per Hof van Beroep). In de praktijk worden de gerechtelijke maatregelen in de GGB TF en HP opgenomen via een lijst die de parketten na een bevraging door het OCAD aan die laatste bezorgen.

In hun toezichtsverslag deden het COC en het Vast Comité I opmerken dat de bevraging door het OCAD aan het Openbaar Ministerie betreffende de gerechtelijke maatregelen niet systematisch gebeurt, waardoor bepaalde informatie in de GGB TF en HP gedateerd of onvolledig kan zijn.

VI.2.3.4. De stand van zaken op het vlak van veiligheidsmachtigingen

Op heden bestaat er geen mechanisme waarbij partnerdiensten de toegang wordt geweigerd tot de GGB TF en HP op basis van het feit dat de gebruiker niet over

[156] Het COC en het Vast Comité I hebben evenwel opgemerkt dat deze redenering niet geldt voor vonnissen en arresten waarvan politiediensten geen kennis hebben.

een veiligheidsmachtiging beschikt.[157] Voor het Openbaar Ministerie bestaat een afzonderlijke regeling. Magistraten bij het Openbaar Ministerie hebben geen veiligheidsmachtinig nodig, enkel de medewerkers van het Openbaar Ministerie dienen over een veiligheidsmachtiging te beschikken. De COL 22/2016 meldt dat zodra de aanvraag daartoe vertrokken is, de medewerkers toegang verkrijgen tot de gemeenschappelijke gegevensbank TF. Het COC en het Vast Comité I waren de mening toegedaan dat het raadzaam is om géén toegang te verlenen tot de gemeenschappelijke gegevensbank TF tot na het verkrijgen van de machtiging; in tussentijd kan de raadpleging van de gegevensbank worden overgelaten aan medewerkers die reeds over een dergelijke machtiging beschikken.

Daarnaast rees de vraag naar de noodzaak om de toegang tot de GGB TF en HP te blijven voorzien voor diensten de de benodigde veiligheidsmachtigingen niet hebben aangevraagd of geen lijst van gebruikers hebben overhandigd aan de Federale Politie. Uit informatie die het COC en het Vast Comité I van de DPO van de GGB TF en HP mochten ontvangen, bleek dat in de praktijk er verschilende partnerdiensten geen gebruik voorzagen en er aan die diensten geen logins zijn verbonden.

Bovendien konden het COC en het Vast Comité I vaststellen dat de waakzaamheid inzake de correcte toepassing van artikel 44/11/3*quater* WPA erg beperkt was. De vraag stelt zich of de toegang tot ongepersonaliseerde mailboxen effectief beperkt is tot de personen met de benodigde veiigheidsmachtiging.

VI.3. DE ADVIESOPDRACHT

VI.3.1. HET VERZOEK OM GEEN VERWERKINGEN UIT TE VOEREN ZONDER DE GEPASTE WETTELIJKE BASIS

Eind maart 2019 werd de voorzitter van het Vast Comité I door de directeur van het OCAD de hoogte gebracht van een schrijven van het OCAD gericht aan de voorzitter van de Gegevensbeschermingsautoriteit (GBA). Met dit schrijven werd de GBA geïnformeerd dat een testperiode zou worden opgetart, waarbij de verwerking van twee nieuwe categorieën, te weten de potentieel gewelddadige extremisten en de terrorisme-veroordeelden, vanaf begin april 2019 zouden worden opgestart in de gegevensbank TF. Nog volgens de directeur van het OCAD beantwoorrdde de opname van deze twee nieuwe categorieën aan belangrijke behoeften op het terrein, met name in detentiecentra, en kwam het tegemoet aan de aanbevelingen van de parlementaire onderzoekscommissie terroristische aanslagen. De directeur van OCAD lichtte toe dat, dankzij de bepaling van duidelijke criteria, de opvolging van entiteiten door de Lokale Task Forces zou worden

[157] De verplichting tot het hebben van een veiligheidsmachtiging vloeit voort uit art. 7 § 2 KB TF en PH.

geünifomiseerd. Verschillende teksten, waaronder het ontwerp van Koninklijk besluit opgesteld op technisch niveau maar nog niet gevalideerd op beleidsniveau, werden als bijlage bij het schrijven gevoegd. De directeur van het OCAD wou dan ook de voorzitter van de GBA '*in volledige democratische transparantie*' op de hoogte brengen en vroeg hem om een voorlopig advies over de ontwerpteksten.

In een brief die midden juni 2019 aan de ministers van Justitie en van Veiligheid en Binnenlandse Zaken werd gestuurd, herinnerden de Vaste Comités I en P en het COC eraan dat de wettelijk vereiste procedure moest worden gevolgd, en dit ongeacht of de verwerking voor een 'testperiode' of op permanente basis werd gepland. Het schrijven legde de nadruk op het gegeven dat persoonsgegevens slechts in een gemeenschappelijke databank kunnen worden verwerkt na de goedkeuring van een in de Ministerraad overlegd Koninklijk besluit (genomen na advies van de toezichthoudende autoriteiten en de Raad van State) en na een voorafgaandelijke aangifte aan het COC en het Vast Comité I. Daarmee traden de Vaste Comité's I en P alsook het COC het standpunt van het College van procureurs-generaal bij. Bijgevolg werd de ministers in hun hoedanigheid van verwerkingsverantwoordelijke verzocht de verwerking van de gegevens met betrekking tot de twee betrokken categorieën te staken. In een brief die midden juli 2019 werd verstuurd, bevestigden de ministers dat zij de Federale Politie hadden opgedragen om het gebruik van de twee nieuwe categorieën technisch onmogelijk te maken.

VI.3.2. ADVIES BETREFFENDE EEN ONTWERP VAN KONINKLIJK BESLUIT TOT INVOEGING VAN DE PGE EN DE TV

Het COC en het Vast Comité I brachten begin 2019 een gezamenlijk advies[158] uit over het ontwerp van Koninklijk besluit tot wijziging van het Koninklijk besluit TF. Zij namen in de eerste plaats kennis van de aanzienlijke uitbreiding van de bestaande TF-databank met de opname van potentieel gewelddadige extremisten. Onder verwijzing naar de risico's, met name in het kader van de doorgifte aan (buitenlandse) instanties, waren de toezichthoudende autoriteiten van mening dat het ontwerp in die zin moest aangepast worden dat personen die gedurende zes maanden in 'vooronderzoek' zijn, alleen gekend mogen zijn bij de basisdiensten die dienen gebruik te maken van hun bestaande wettelijke mogelijkheden om informatie en inlichtingen te bekomen die moeten toelaten de opname in de databank te bevestigen of teniet te doen.

Het COC en het Vast Comité I hebben de verschillende (sub)criteria die de PGE's in het ontwerp van Koninklijk besluit beschrijven, grondig onderzocht.

158 Advies 001/VCI-COC/2019 van 1 augustus 2019 betreffende een ontwerp van Koninklijk besluit tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank *terrorist fighters* (www.comiteri.be).

De toezichthoudende autoriteiten stelden onmiskenbaar begrip te hebben voor de moeilijke opdracht van de politie- inlichtingen- en veiligheidsdiensten inzake de (proactieve) bestrijding van terrorisme en extremisme dat tot terrorisme kan leiden. De oprichting van de gemeenschappelijke gegevensbanken komt in die zin tegemoet aan de aanbevelingen van de parlementaire onderzoekscommissie terroristische aanslagen om informatie efficiënter te laten circuleren door de actoren in de strafrecht- en veiligheidsketen. Maar er wordt door deze onderzoekscommissie geenszins aanbevolen om de doelgroep dermate uit te breiden dat de link met terroristisch geweld verdwijnt. Reden waarom werd gevraagd dat enerzijds hun aanbevelingen in rekening zouden worden genomen en, anderzijds, om de vooropgestelde criteria op een ernstige wijze te hanteren.

Het COC en het Vast Comité I wezen op het risico dat, indien hun aanbevelingen niet worden opgevolgd, de registratiebasis in de GGB verlaagd wordt tot het niveau dat aanknoopt met de verwerkingsvoorwaarden voor de bestuurlijke politie enerzijds en de verwerkingsvoorwaarden voor de inlichtingendiensten anderzijds. Als gevolg daarvan stromen zeer privacygevoelige gegevens in toenemende mate door naar (steeds meer) diensten en instellingen buiten de strafrecht- of veiligheidsketen. Deze (administratieve) diensten hebben echter vaak geen of beperkte ervaring met het beheer van dergelijke gevoelige en soms onzekere gegevens, met mogelijke gevolgen voor het leven van de betrokkenen.

Wat betreft de uitbreiding van de GGB TF door de opname van terrorismeveroordeelden (TV), verzochten het COC en het Vast Comité I de stellers van het ontwerp om vragen in overweging te nemen over personen die in het buitenland werden veroordeeld, over minderjarigen die voor terroristische misdrijven een beschermingsmaatregel kregen opgelegd en over personen die nog niet definitief veroordeeld zijn.

Ten slotte bogen de toezichthoudende autoriteiten zich ook over de nieuwe indirecte toegang voorzien in het ontwerp-KB voor de instelling Brussel – Preventie & Veiligheid (BPV). Het accent kwam in het bijzonder te liggen op het gebrek aan duidelijkheid van de context waarin deze instelling als partnerdienst werd aangeduid en wezen daarbij op 44/11/3*ter*, § 3 WPA. Gezien het ontwerp tal van vragen open liet (over het gebruik en het delen van gegevens door BPV, over de regels inzake bewaring, over voorziene veiligheidsmaatregelen), achtten het COC en het Vast Comité I het niet aanvaardbaar dat een nieuwe instelling aan de reeds bestaande uitgebreide lijst van ontvangers zou worden toegevoegd zonder dat de pertinentie en de maatschappelijke meerwaarde ervan werd aangetoond.

VI.3.3. ADVIES OVER DE 'AANVULLENDE VOORAFGAANDELIJKE AANGIFTEN'

Halfweg juli 2019 hebben de ministers van Justitie en van Veiligheid en Binnenlandse Zaken een vraag tot advies overgemaakt aan het COC en het Vast Comité

aangaande de aanvullende voorafgaandelijke verklaring van de gemeenschappelijke databank TF en HP. Deze (derde) aanvullende voorafgaandelijke verklaring bevatte de praktische regelingen voor de verwerking van gegevens door de Justitiehuizen van de Gemeenschappen en door het Vlaams Agentschap Jongerenwelzijn (VAJ).[159]

In hun gezamenlijk advies van eind november 2019[160] hebben het COC en het Vast Comité I erop gewezen dat het gebrek aan aanwijzing van een DPO inmiddels was opgelost en dat (wijzigingen in) de contactgegevens van DPO's van de (nieuwe) diensten met (nieuwe) toegang moet worden gemeld. Voor het overige brachten zij een gunstig advies uit over deze aanvullende verklaring, onder voorbehoud van de geformuleerde opmerkingen.

159 Het COC en het Vast Comité I konden uit de inhoud van de brief van 24 juli 2019 van de ministers verantwoordelijk voor de verwerking opmaken dat er voor de Nationale Veiligheidsoverheid nog steeds geen toegang werd verleend.

160 www.comiteri.be.

HOOFDSTUK VII
DE OPSPORINGS- EN GERECHTELIJKE ONDERZOEKEN

Naast zijn medewerking aan de toezichtonderzoeken, voert de Dienst Enquêtes I van het Comité ook onderzoeken naar leden van de inlichtingendiensten die verdacht worden van een misdaad of wanbedrijf. Dit doet de enquêtedienst in opdracht van de gerechtelijke overheden. Deze bevoegdheid staat omschreven in artikel 40, derde lid van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse. Met de Wet van 10 juli 2006 betreffende de analyse van de dreiging werd deze bevoegdheid uitgebreid tot misdaden of wanbedrijven gepleegd door de leden van het Coördinatieorgaan voor de dreigingsanalyse (OCAD).[161]

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 heeft vele andere wettelijke opdrachten. Deze opdrachten zouden 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 is voor de uitoefening door het Vast Comité I van zijn opdrachten*' (art. 43, derde lid, W.Toezicht).

Ook in 2019 voerde de Dienst Enquêtes I onderzoeksdaden uit in het kader van zijn gerechtelijke opdracht, meer bepaald in twee opsporingsonderzoeken.

---

161 Wat betreft de leden van de andere 'ondersteunende diensten' van het OCAD geldt deze bepaling alleen ten aanzien van de verplichting om relevante inlichtingen aan het OCAD mee te delen (artt. 6 en 14 W.OCAD).

In 2019 rondde de Dienst Enquêtes I een onderzoek af dat was aangevangen in 2017. Dit onderzoek werd gevoerd op vraag van het Federaal Parket en betrof de mogelijke betrokkenheid van een lid van een inlichtingendienst bij een misdaad of wanbedrijf tegen de inwendige en/of uitwendige veiligheid van de Staat. Samenhangend daarmee werd onderzocht of een ander lid van dezelfde inlichtingendienst ten aanzien van deze persoon zijn beroepsgeheim had geschonden.[162]

Op vraag van een onderzoeksrechter en onder leiding van het Federaal Parket verrichtte de Dienst Enquêtes I ook een aantal onderzoeksdaden in het kader van een onderzoek naar misdrijven die door een criminele bende gepleegd werden en naar de vraag of de inlichtingendiensten eventueel over informatie desbetreffende beschikten.

Verder stelt artikel 50 W.Toezicht dat *'[e]lk lid van een politiedienst dat een misdaad of een wanbedrijf gepleegd door een lid van een inlichtingendienst vaststelt, maakt daarover een informatief verslag op en bezorgt dat binnen de vijftien dagen aan het hoofd van de Dienst Enquêtes I'*. De enquêtedienst ontving in 2019 geen meldingen in die zin.

[162] VAST COMITÉ I, *Activiteitenverslag 2015*, 41 ('II.9. Klacht over het verstrekken van persoonlijke informatie door een inlichtingenagent aan een derde').

HOOFDSTUK VIII
EXPERTISE EN EXTERNE CONTACTEN

VIII.1. EXPERT OP DIVERSE FORA

Leden van het Vast Comité I en van zijn personeel werden in 2019 diverse malen als expert geconsulteerd door binnen- en buitenlandse publieke en private instellingen:

- In maart 2019 nam de voorzitter van het Comité op uitnodiging van de VSSE deel aan de oprichtingsvergadering van het *Intelligence Network Europe* (INE).[163] Het initiatief heeft mee tot ambitie een vormingsplatform op te richten voor de leden van inlichtingendiensten, maar wil ook inzetten op beleidsmakers die in aanraking komen met inlichtingen informeren. Het is intergouvernementeel ingevuld en streeft niet naar het verwerven van een fysieke infrastructuur, maar wil inzetten op verbinding en netwerking.
- De voorzitter en de griffier werden in mei 2019 in Berlijn uitgenodigd om deel te nemen aan een workshop van het *European Intelligence Oversight Network* (EION), met thema's als '*How can oversight bodies better assess and demonstrate the effectiveness of their control instruments*', '*What insights can be distilled from other systems, such as banking supervisory authorities or antitrust compliance programs, to identify innovations for intelligence oversight*?' …
- Op verzoek van de Duitse *Stiftung Neue Verantwortung*, pleegde de griffier in november 2019 een bijdrage ('*A simple yet existential demand: let oversight bodies work together*') voor een nieuw online communicatieplatform (www.aboutintel.eu) dat zich onder meer tot doel stelt te inspireren inzake inlichtingenwerk, technologie en democratie, gespecialiseerde bijdragen over deze items voor een groot publiek toegankelijk te maken en het wederzijds begrip te bevorderen tussen de verschillende actoren uit de inlichtingenwereld.
- De griffier van het Vast Comité I werd uitgenodigd in het kader van het opleidingsonderdeel 'Intelligence' van de Master in de internationale betrekkingen en de diplomatie (Universiteit Antwerpen) om er de werking van het Comité toe te lichten.

[163] Bij aanvang droeg het initiatief de naam Académie européenne de Renseignement (AeR), maar om het netwerk-karakter te onderlijnen, is finaal gekozen voor INE (en het adagium '*Enhancing a common strategic culture*'). Het is de concretisering van een oproep van de Franse president Macron in september 2017 die daarmee wil bouwen aan een Europese inlichtingencultuur.

VIII.2. SAMENWERKINGSPROTOCOL MENSENRECHTENINSTELLINGEN

Met de Wet van 12 mei 2019 werd – na lange jaren aandringen – het 'Mensenrechteninstituut', voluit het Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens, opgericht.[164] De creatie van een nationaal Mensenrechteninstituut, een engagement dat werd aangegaan bij de ondertekening van het Protocol bij het VN-verdrag tegen foltering, liet lang op zich wachten. België werd daarvoor, onder andere door de Verenigde Naties, meermaals op de vingers getikt.

In afwachting van de effectieve oprichting van het instituut, resulteerde de vergaderingen met diverse instellingen met een mandaat op het gebied van mensenrechten[165] in een samenwerkingsprotocol.[166] Daarin kwamen alle deelnemende instanties overeen om praktijken en methoden uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen.

Het nieuw opgerichte instituut ('Federaal Instituut voor de Rechten van de Mens') werd diverse opdrachten toegekend: zo verstrekt het op verzoek of op eigen initiatief adviezen en aanbevelingen betreffende aangelegenheden die verband houden met de bevordering en de bescherming van de fundamentele rechten, volgt het de tenuitvoerlegging op van de internationale verplichtingen die door de Belgische overheden werden aangegaan en stimuleert het de bekrachtiging van nieuwe internationale mensenrechten instrumenten. Een jaar na publicatie van de oprichtingswet werd door de Kamer een raad van bestuur samengesteld door de benoeming van twaalf onafhankelijke personen uit de academische en gerechtelijke wereld, uit het maatschappelijk middenveld en van de sociale partners.

VIII.3. EEN MULTINATIONAAL INITIATIEF INZAKE INTERNATIONALE INFORMATIE-UITWISSELING

De toegenomen internationale gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten brengt een aantal uitdagingen mee voor de nationale toezichtorganen. De toezichtorganen van (oorspronkelijk) vijf Europese landen (België, Denemarken, Nederland, Noorwegen en Zwitserland)[167] werken daarom samen om het hoofd te bieden aan die uitdagingen door werkwijzen te vinden om het

164 Wet van 12 mei 2019 tot oprichting van een Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens, B.S. 21 juni 2019.

165 Zoals het Unia (het voormalige Interfederaal Gelijkekansencentrum), het Federaal Migratiecentrum, het Instituut voor de gelijkheid van vrouwen en mannen, de Gegevensbeschermingsautoriteit, de federale Ombudsman, de Hoge Raad voor Justitie, de Vaste Comités I en P.

166 Samenwerkingsprotocol van 13 januari 2015 tussen de instellingen met een volledig of gedeeltelijk mandaat belast met de eerbiediging van de rechten van de mens.

167 Zie VAST COMITÉ I, *Activiteitenverslag 2015*, 80-81.

risico op een hiaat in het toezicht te verkleinen. Na verloop van tijd werd een nieuwe partner betrokken in dit project, namelijk het *Investigatory Powers Commissioner's Office (IPCO)* uit het Verenigd Koninkrijk. De groep werd herdoopt tot *Intelligence Oversight Working Group* (IOWG) en in 2019 uitgebreid met drie waarnemers, te weten de *Swedisch Foreign Intelligence Inspectorate (Statens inspektion av försvarunderättelse-verksamhet (SIUN))*, de *Swedish Board of Inventions (Statens uppfinnarnämnd, (SUN))* en de Duitse *G10 Commission*.

De partners zijn van oordeel dat het ingestelde toezicht behoefte heeft aan een meer intense samenwerking tussen de nationale toezichthouders. Dit momenteel louter nationaal mandaat en de nationale classificatieregels, vormen uitdagingen voor het toezicht dat bij gegevensuitwisseling vooralsnog maar naar één zijde van het spectrum kan kijken. Ook de toename aan volumes van datatransferts, van multilaterale uitwisseling en van gemeenschappelijke databases vormen voor de toezichthouders een uitdaging, temeer daar de regelgeving hierover eerder summier is en per land verschilt. Tot slot maken technologische evoluties de opdracht van de toezichthouders nog moeilijker.

Afgelopen jaren werden diverse *expert meetings* georganiseerd waarbij methoden, *best practices*, juridische en praktische problemen werden besproken en ervaringen uitgewisseld. Ook werd een 'gemeenschappelijk' toezichtonderzoek gevoerd (cf. I.3). Begin november 2018 werd door de deelnemende toezichtorganen een gemeenschappelijke verklaring en perscommuniqué opgesteld.[168]

In maart 2019 organiseerde het Comité in Brussel een vergadering dewelke kaderde in een nieuw project om met deze instellingen twee onderwerpen gezamenlijk te bestuderen: enerzijds de implicaties van de invoering van het nieuwe PNR-systeem voor de werking van de inlichtingendiensten en het toezicht hierop; anderzijds de innovatie van het toezicht in zonderheid door het gebruiken van een gemeenschappelijke onderzoeksmethodologie en het gebruik hierbij van ICT-middelen.

Halfweg december 2019 werd, op initiatief van de Nederlandse Commissie van toezicht op de inlichtingen- en veiligheidsdiensten, het '*Charter of the Intelligence Oversight Working Group*'[169] ondertekend.

VIII.4. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

Het Vast Comité I onderhield ook in 2019 nauwe contacten met diverse buitenlandse toezichthouders.

168 Zie VAST COMITÉ I, *Activiteitenverslag 2018*, Bijlage D. 'Versterking van het toezicht op de internationale gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten'.

169 Zie bijlage D van dit activiteitenverslag.

Met het oog op het creëren van een normatief kader voor de internationale samenwerking tussen inlichtingendiensten en de toezichthouders, werden de eerste contacten gelegd met diverse BENELUX-instanties. Het thema kon evenwel niet worden geagendeerd op het Benelux Ministerieel Comité.

Tijdens een colloquium dat begin februari 2019 plaatsvond in de Franse *Ecole Militaire* werden de banden aangehaald met de voorzitters van de *Commission nationale de contrôle des techniques de renseignement* (CNCTR) alsook van de *Délégation parlementaire au renseignement* (DPR), dewelke intervenieerden in het kader van het panel '*Le droit du renseignement – un droit exorbitant du droit commun fortement contrôlé*'.

Naar gewoonte vonden er ook bilaterale contacten plaats met de Nederlandse toezichthouder; in Brussel werd in april 2019 tijdens een werkvergadering het Nederlandse '*system based oversight*-concept' toegelicht en werd overlegd over de te volgen strategie aangaande buitenlande samenwerkingsverbanden. In mei 2019 vond een tweedaagse meeting plaats met vertegenwoordigers van de *Commission spéciale chargée d'autoriser les mesures de surveillance et de contrôle des télécommunications ainsi que le repérage des données relatives au trafic* en met de voltallige delegatie van de *Commission de contrôle du Service de renseignement de l'État*'. Ook vond tussen de voorzitters van het Comité en de Franse *Commission nationale de contrôle des techniques de renseignement* (CNCTR) in Parijs in juni 2019 een overleg plaats. Met de nieuwe *Investigatory Powers Commissioner* (UK) werden afspraken gemaakt voor een wederzijdse kennismaking. Naar aanleiding van de inwerkingtreding in juli 2019 van de *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* werd een nieuw Canadees toezichtsorgaan opgericht, met name l'*Office de surveillance des activités en matière de sécurité nationale et de renseignement* (OSSNR) met een ruimer mandaat dan zijn voorganger. Beide voorzitters stemden in met de organisatie van een werkbezoek. Met de Zwitserse *Autorité de surveillance indépendante des activités de renseignement* (AS-Rens) ten slotte werden geprivilegieerde contacten onderhouden met het oog de realisatie van een stage / uitwisselingsproject in de loop van 2020.

In oktober 2019 werd in Londen de derde editie van het *International Intelligence Oversight Forum* over 'Intelligence oversight at a crossroads', georganiseerd door de *Special Rapporteur for Privacy* (SRP) van de Verenigde Naties, Prof. Cannataci. Hieraan namen zowel vertegenwoordigers van toezichthouders, inlichtingendiensten, universiteiten en NGO's deel. Het doel van dit forum bestond erin om in een vertrouwelijke omgeving een beter begrip te krijgen in de uitdagingen waarmee onder meer democratische toezichtorganen worden geconfronteerd.[170]

[170] Met thema's als '*Relationship between overseers and overseen (outreach, transparancy, personnel selction*', '*Oversight across the intelligence cycle*', '*Making oversight affordable and accessible fort he citizen*' ….

VIII.5. MEMORANDUM

In het kielzog van de federale Parlementsverkiezingen van mei 2019 diende het Vast Comité I ten behoeve van de (toenmalige) informateurs een Memorandum in.[171, 172] Het Comité twijfelde niet aan de nodige belangstelling die wordt voorbehouden aan de goede werking van de inlichtingendiensten van het land en aan de noodzaak om democratische en effectieve controle over hen te handhaven. Het Memorandum, dat in deze optiek werd opgesteld, wou de aandacht van de informateurs vestigen op het belang van bepaalde wetgevende initiatieven ter zake. De er in opgenomen voorstellen betroffen onder meer een aanpassing van de Toezichtswet, aandacht voor de versterkte werking van het Comité, de vereisten in het kader van de bescherming van persoonsgegevens (en de installatie van een beveiligd netwerk), de noodzaak tot het opzetten van een interne controle- en auditdienst binnen de inlichtingendiensten en de informatisering en vereenvoudiging van de procedures voor het Beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

171 Ook beide inlichtingendiensten, de ministers van Defensie en Justitie alsook de Voorzitter van de Kamer van Volksvertegenwoordigers waren hiervan bestemmeling.

172 Het Comité nam, op verzoek van de toenmalige informateur van de Koning, al een gelijkaardig initiatief na de federale Parlementsverkiezingen van juni 2007 (VAST COMITÉ I, *Activiteitenverslag 2007*, 52-54).

HOOFDSTUK IX
HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN[173]

IX.1. INLEIDING

Het Beroepsorgaan is het administratief rechtscollege 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, tot slot, de veiligheidsadviezen. Daarnaast kan het Beroepsorgaan ook optreden als 'annulatierechter' tegen beslissingen van publieke of administratieve overheden om in een bepaalde sector, voor een bepaalde plaats of voor een bepaald evenement veiligheidsattesten of -adviezen aan te vragen.[174]

Het Beroepsorgaan is samengesteld uit de voorzitters van het Vast Comité I, het Vast Comité P en de Geschillenkamer van de Gegevensbeschermingsautoriteit. De voorzitter van het Vast Comité I neemt het voorzitterschap van het Beroepsorgaan waar. De griffiefunctie wordt uitgeoefend door de griffier van het Vast Comité I. Het personeel van de griffie is het personeel dat door het Vast Comité I is aangesteld. De activiteiten van het Beroepsorgaan vormen al meer dan twintig jaar een perfect voorbeeld van synergie binnen bepaalde satellietinstellingen van het parlement.

De werking ervan wordt namelijk volledig ondersteund door het Vast Comité I. Het gaat daarbij enerzijds om de terbeschikkingstelling van de voorzitter en zijn plaatsvervangende leden en de griffier, maar ook de juristen en het administratief personeel die de griffie van dit administratief rechtscollege vormen.

Anderzijds neemt het Vast Comité I in zijn begroting ook de kosten van de kantoren op zich als werkingskosten van het Beroepsorgaan.

---

173 Dit hoofdstuk geeft uitvoering aan artikel 13 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, waarin wordt bepaald dat het beroepsorgaan een jaarverslag moet opstellen.

174 Voor meer informatie, zie VAST COMITÉ I, *Activiteitenverslag 2006,* 91-124 en VAST COMITÉ I, *Activiteitenverslag 2018,* 109-122.

De griffier, bijgestaan door juristen en medewerkers van het Vast Comité I, houdt de griffie draaiende, neemt de beroepsdossiers voor de zittingen in ontvangst en bereidt ze voor.

IX.2. EEN BIJ WIJLEN ZWARE EN COMPLEXE PROCEDURE

De toename van het aantal dossiers in 2019 (zie verder) gaat gepaard met een verhoogde werklast. Het administratief beheer van de dossiers, de zittingen en de beslissingen blijft complex. De kwaliteit van het samengestelde dossier is zeker een van de oorzaken, maar ook de steeds frequentere tussenkomst van advocaten heeft een grote impact. Dat brengt immers, en terecht, de verplichting mee voor het Beroepsorgaan om zijn beslissingen te motiveren door te antwoorden op alle argumenten die de advocaten ter verdediging van de belangen van hun cliënt aanvoeren.

Heel wat dossiers voldoen niet aan de vereisten gesteld in de artikelen 2 en 3 van het KB Beroepsorgaan, 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 lege ferenda* moet er beter rekening worden gehouden met de hoedanigheid en zelfs de kwetsbaarheid van tal van verzoekers en worden voorzien in wettelijke bepalingen die geen nietigheid van rechtswege met zich meebrengen.

Maar ook de wijze waarop de verschillende betrokken (veiligheids)overheden instaan voor de administratieve behandeling van deze dossiers brengt soms een extra werklast én een vertraging in de afhandeling van de dossiers met zich mee. Het is evident dat een dergelijke vertraging kan indruisen tegen de belangen van de verzoeker. Om hieraan te verhelpen, stelde het Beroepsorgaan deze overheden regelmatig in kennis van de volgende problemen:

- De wettelijke termijn waarbinnen het administratief dossier aan het Beroepsogaan moet worden overgemaakt, wordt vaak overschreden. Zo wordt het voor het Beroepsorgaan moeilijk om de termijn waarin het een beslissing moet nemen, te respecteren.
- De administratieve dossiers die door de diverse veiligheidsoverheden worden toegezonden, blijken niet steeds volledig, zodat de griffie bijkomende handelingen moet stellen. Soms blijkt het dossier pas te worden samengesteld nadat er beroep is aangetekend.
- De toepassing van artikel 5 § 3 W.Beroepsorgaan is vaak problematisch. Deze bepaling laat het Beroepsorgaan toe op verzoek van een inlichtingen- of politiedienst te beslissen om sommige stukken uit het dossier ter inzage van de eiser of zijn advocaat te halen. Dit is het geval indien de verspreiding ervan een gevaar kan inhouden voor de bescherming van de bronnen, de persoonlijke levenssfeer van derden, de vervulling van de wettelijke opdrachten van de

inlichtingendiensten of het geheim van een lopend opsporings- of gerechtelijk onderzoek. Het verzoek is echter 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. Vaak blijven deze overheden ook verkeerdelijk vasthouden aan de idee dat de verzoeker en diens advocaat geen inzage kunnen krijgen van geclassificeerde gegevens, zonder dat dit een nadere motivering behoeft, en dit ondanks de vaste rechtspraak van het Beroepsorgaan volgens dewelke de W.Beroepsorgaan een *lex specialis* is t.o.v. de Classificatiewet. Tot slot zijn er ook gevallen waarin de voorzitter van het Beroepsorgaan ambtshalve elementen uit het dossier moet verwijderen omdat de betrokken dienst manifest heeft nagelaten zich te beroepen op art. 5 § 3 W.Beroepsorgaan ter bescherming van de persoonlijke levenssfeer van derden.

- De beslissingen van de veiligheidsoverheden zijn onvoldoende gemotiveerd en er wordt – in strijd met de wettelijke vereisten – geen volledig gemotiveerde beslissing opgesteld in de gevallen waarbij artikel 22, vijfde lid W.C&VM toelaat om bepaalde elementen weg te laten in de aan de betrokkene ter kennis gegeven beslissing. Bovendien moet de veiligheidsoverheid in de motivering duidelijk maken welke concrete feiten een tegenindicatie uitmaken, rekening houdend met het reglementair vastgestelde doel van een bepaalde veiligheidsverificatie. Alleen zo kan het Beroepsorgaan nagaan of een beslissing proportioneel is.
- Verder moest worden vastgesteld dat de beslissingen van diverse veiligheidsoverheden niet getuigden van zorgvuldigheid en respect voor de formele beginselen van het administratief recht (beslissingen zonder data en identiteit van de functionaris die de beslissing neemt; betrokkene wordt nooit gehoord; het taalgebruik in bestuurszaken).
- De veiligheidsoverheden volgen de vaste rechtspraak van het Beroepsorgaan niet (bijv. inzake de problematiek van onderzoeken of verificaties naar personen die niet beschikken over de Belgische nationaliteit).

Verder dient te worden vastgesteld dat de zittingen veel meer tijd in beslag namen dan een aantal jaren geleden. Dit heeft verschillende oorzaken. Steeds meer verzoekers laten zich bijstaan door een of twee advocaten. De complexiteit zorgt ervoor dat bepaalde zaken veel tijd vergen. Het Beroepsorgaan moet daardoor meer beslissingen nemen alvorens recht te doen of verdagingen toekennen.

Daardoor neemt ook het aantal zittingen toe. Die zijn immers nodig om de aanvullende informatie te verkrijgen die het rechtscollege nodig heeft om te kunnen beslissen.

Ook het beslissingsproces zelf vergt meer tijd dan een aantal jaren geleden. Hiervoor zijn twee belangrijke redenen aan te halen. Enerzijds is er het grote aantal procedurele kwesties (bijv. ontvankelijkheid, taalgebruik, rechten van verdediging of delegering van de bevoegdheid van de instantie die de beslissing neemt). Anderzijds wordt het Beroepsorgaan vaker geconfronteerd met extreem gevoelige

dossiers. Dergelijke dossiers vereisen uiteraard een uiterst zorgvuldige behandeling en een aangepaste motivatie door het delicate evenwicht tussen de noodzaak voor de rechtsonderhorige om de beslissing te begrijpen en de noodzaak om informatie geheim te houden die de veiligheid van de staat of zijn instellingen in gevaar kan brengen.

Daarenboven moeten soms specifieke veiligheidsmaatregelen worden genomen.

IX.3. EVOLUTIE VAN HET WETGEVEND KADER: TWEE WETSWIJZIGINGEN

In 2018 was het wetgevend kader sterk veranderd, zowel wat betreft de W.C&VM als wat betreft de W.Beroepsorg.

In 2019 heeft de wetgever slechts twee wijzigingen (van relatief belang voor het werk van het Beroepsorgaan) aangebracht. De eerste betrof de definitie van beschermde getuigen zoals bedoeld in artikel 3 van de W.C&VM.[175] Het doel van de tweede wijziging was om geaccrediteerde beroepsjournalisten vrij te stellen van de betaling van de in artikel 22*septies* van de genoemde wet bedoelde retributie.[176]

IX.4. GEDETAILLEERDE CIJFERS

In dit onderdeel worden de aard van de bestreden beslissingen, de hoedanigheid van de bevoegde overheden en 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 vier vorige jaren eveneens opgenomen.

De algemene trend in de cijfers van de afgelopen jaren laat een toename zien van het aantal beroepen dat bij het Beroepsorgaan wordt ingediend. Die stijging speelt zich af rond drie grote assen: ten eerste een verhoging van het aantal beroepen met betrekking tot veiligheidsmachtigingen (van 36 in 2018 naar 51 in 2019). Ten tweede zijn de geschillen over veiligheidsadviezen na een jaar van achteruitgang ook sterk toegenomen (van 92 in 2018 naar 115 in 2019). En ten derde waren er ook meer beroepen met betrekking tot de weigering van veiligheidsattesten voor de nucleaire sector (van 11 in 2018 naar 17 in 2019).

---

175 Wet van 5 mei 2019 houdende diverse bepalingen in strafzaken en inzake erediensten, en tot wijziging van de wet van 28 mei 2002 betreffende de euthanasie en van het Sociaal Strafwetboek (*BS* 24 mei 2019).

176 Wet van 2 mei 2019 houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS* 27 mei 2019).

We melden dat het Beroepsorgaan voor het eerst de kwestie van de toekenning van een veiligheidsattest aan een imam om in Belgische gevangenissen te werken heeft behandeld op basis van wat werd bepaald in het Koninklijk besluit van 17 mei 2019.[177]

Bij het rechtscollege werd ook een zaak aanhangig gemaakt over de kwestie van de toekenning van het veiligheidsadvies voor douanebeambten die een wapen moeten dragen in het kader van de uitoefening van hun functie, in overeenstemming met wat werd bepaald in het koninklijk besluit van 15 december 2013.[178]

Voor zover het Beroepsorgaan weet, is er nog geen gebruikgemaakt van de nieuwe veiligheidsadviesprocedure die in het activiteitenverslag van 2018 werd beschreven. Volgens bepaalde echo's wil men in de toekomst de controles van de integriteit en moraliteit van het personeel van de Europese instellingen en de havens opvoeren. Het is mogelijk dat de nieuwe veiligheidsadviesprocedure daarvoor wordt toegepast.

Tot slot vonden er 21 zittingen van het Beroepsorgaan plaats in 2019.

Tabel 1. Betrokken veiligheidsoverheid

	2015	2016	2017	2018	2019
Nationale Veiligheidsoverheid	68	92	129	113	114
Veiligheid van de Staat	1	0	0	0	0
Algemene Dienst Inlichting en Veiligheid	47	68	53	32	61
Federaal Agentschap voor Nucleaire Controle	10	8	7	10	17
Federale politie	3	1	3	3	3
Lokale politie	1	0	0	0	1
TOTAAL	**130**	**169**	**192**	**158**	**196**

Tabel 2. Aard van de bestreden beslissing

	2015	2016	2017	2018	2019
Veiligheidsmachtigingen (Art. 12 e.v. W.C&VM)					
Vertrouwelijk	9	5	1	2	5
Geheim	35	38	33	31	39
Zeer geheim	4	7	6	3	7

177 Koninklijk besluit van 17 mei 2019 betreffende de aalmoezeniers, de consulenten van de erediensten en de moreel consulenten bij de gevangenissen (artikel 3§ 3,1°).

178 Koninklijk besluit van 15 december 2013 tot vaststelling van de diensten bij de Algemene Administratie van de Douane en Accijnzen waar de uitoefening van een functie afhankelijk wordt gesteld van een veiligheidsverificatie.

	2015	2016	2017	2018	2019
Weigering	36	28	30	26	39
Intrekking	7	9	7	4	16
Weigering en intrekking	0	0	0	0	0
Machtiging voor beperkte duur	3	4	1	1	3
Machtiging voor een lager niveau	0	1	0	0	0
Geen beslissing binnen de termijn	2	7	2	5	0
Geen beslissing binnen de verlengde termijn	0	1	0	0	0
SUBTOTAAL VEILIGHEIDSMACHTIGINGEN	48	50	40	36	51
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)					
Weigering	6	1	3	3	1
Intrekking	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	0	0	0
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)					
Weigering	12	9	20	15	12
Intrekking	1	0	0	0	0
Geen beslissing binnen de termijn	0	0	0	0	0
Veiligheidsattesten voor nucleaire sector (art. 8*bis* W.C&VM)					
Weigering	–	7	7	11	17
Intrekking	–	1	0	0	0
Geen beslissing binnen de termijn	–	0	0	1	0
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)					
Negatief advies	63	101	122	92	115
Geen advies	0	0	0	0	0
Herroeping van positief advies	0	0	0	0	0
Normatieve rechtshandelingen van een administratieve overheid (Art. 12 W.Beroepsorgaan)					
Beslissing van een publieke overheid om veiligheidsattesten te eisen	0	0	0	0	0
Weigering van de NVO om verificaties voor veiligheidsattesten te verrichten	0	0	0	0	0
Beslissing van een administratieve overheid om veiligheidsadviezen te eisen	0	0	0	0	0
Weigering van de NVO om verificaties voor veiligheidsadviezen te verrichten	0	0	0	0	0
SUBTOTAAL ATTESTEN EN ADVIEZEN	82	119	152	122	145
TOTAAL BESTREDEN BESLISSINGEN	130	169	192	158	196

Tabel 3. Hoedanigheid van de verzoeker

	2015	2016	2017	2018	2019
Ambtenaar	4	2	4	5	4
Militair	29	23	20	8	27
Particulier	93	139	164	140	163
Rechtspersoon	4	5	4	5	2

Tabel 4. Taal van de verzoeker

	2015	2016	2017	2018	2019
Franstalig	75	99	115	83	101
Nederlandstalig	54	70	77	75	95
Duitstalig	0	0	0	0	0
Anderstalig	1	0	0	0	0

Tabel 5. Handelingen van de griffie

	2015	2016	2017	2018	2019
Volledig dossier opvragen (1)	130	167	191	154	191
Aanvullende informatie opvragen (2)	7	23	36	12	18
Herinneringen versturen naar veiligheidsoverheden (3)	/	/	/	/	21[179]

(1) Het Beroepsorgaan beschikt over de mogelijkheid om het gehele dossier op te vragen bij de veiligheidsoverheden. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan door de griffie.

(2) Het Beroepsorgaan beschikt over de mogelijkheid om tijdens de procedure aanvullende informatie die het nuttig acht, op te vragen. In de praktijk neemt de griffie de taak op zich om de overheden te vragen de dossiers te vervolledigen.

(3) Art. 6 van het KB Beroepsorgaan voorziet de termijnen voor de aanlevering van de dossiers door de veiligheidsoverheden. Die termijnen vangen aan wanneer de griffier een kopie van het beroep naar de betrokken veiligheidsoverheid stuurt. Ze variëren naargelang de aard van de betwiste handeling. Zo moet de veiligheidsoverheid haar dossier aanleveren binnen de 15 dagen

[179] Het gaat om herinneringen die de griffie per brief naar de veiligheidsoverheden stuurt (11 herinneringen hadden betrekking op onderzoeksdossiers, 2 hadden betrekking op veiligheidsverificatiedossiers voor veiligheidsattesten en 8 hadden betrekking op veiligheidsverificatiedossiers voor veiligheidsadviezen). Er waren ook tal van telefonische herinneringen, maar die kunnen om praktische redenen niet in aanmerking worden genomen of in deze statistieken worden opgenomen.

voor veiligheidsmachtigingen, binnen de vijf dagen voor veiligheidsattesten en binnen de tien dagen als het beroep betrekking heeft op een veiligheidsadvies. Wanneer die termijnen niet worden nageleefd, legt de griffie de nodige contacten. Deze gegevens worden geregistreerd vanaf 2019.

Tabel 6. Voorbereidende gerechtelijke handelingen van het Beroepsorgaan[180]

	2015	2016	2017	2018	2019
Horen van een lid van een overheidsinstantie (1)	7	10	0	1	6
Beslissing van de voorzitter (2)	0	0	0	0	0
Verwijderen van informatie uit het dossier door het Beroepsorgaan (3)	50	54	80	72	77
Beslissingen alvorens recht te doen (4)	/	/	/	/	9[181]

(1) Het Beroepsorgaan kan beslissen om de leden van de inlichtingen- en politiediensten of van de veiligheidsoverheden die aan het veiligheidsonderzoek of de veiligheidsverificatie hebben meegewerkt, te horen.
(2) De voorzitter van het Beroepsorgaan kan beslissen dat het lid van de inlichtingendienst bepaalde gegevens geheim houdt tijdens zijn verhoor.
(3) Indien de betrokken inlichtingen- of politiedienst hierom verzoekt, kan de voorzitter van het Beroepsorgaan beslissen dat bepaalde informatie wordt verwijderd uit het dossier dat ter inzage aan de verzoeker zal worden voorgelegd.
(4) Het kan bijvoorbeeld gaan om een beslissing om twee dossiers samen te voegen of om nadere informatie te vragen over de context van een gerechtelijk dossier. Deze gegevens worden geregistreerd vanaf 2019.

Tabel 7. Wijze waarop de verzoeker zijn rechten van verdediging uitoefent

	2015	2016	2017	2018	2019
Inzage van het dossier door de verzoeker en/of zijn advocaat	84	87	105	69	96
Horen van de verzoeker (al dan niet bijgestaan door zijn advocaat)[182]	107	127	158	111	143

180 De cijfers voor 'voorbereidende gerechtelijke handelingen' (tabel 6), 'wijze waarop de verzoeker zijn rechten van verdediging uitoefent' (tabel 7) of 'aard van de beslissingen van het Beroepsorgaan' (tabel 8) komen niet noodzakelijkerwijs overeen met het aantal ingediende verzoeken (zie tabellen 1 tot 4). Sommige dossiers werden bijvoorbeeld al opgestart in 2019, terwijl de beslissing pas viel in 2020.

181 Van die interlocutoire beslissingen werden er 5 genomen met betrekking tot veiligheidsmachtigingen, 1 met betrekking tot een veiligheidsattest en 3 met betrekking tot veiligheidsadviezen.

182 De W.Beroepsorg. regelt de bijstand door een advocaat tijdens de zitting, maar niet de vertegenwoordiging door die laatste. In bepaalde dossiers wordt de verzoeker (al dan niet bijgestaan door zijn advocaat) meermaals gehoord.

Tabel 8. Aard van de beslissingen van het Beroepsorgaan

	2015	2016	2017	2018	2019
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)					
Beroep onontvankelijk	4	0	3	0	1
Beroep zonder voorwerp	3	7	0	4	3
Beroep ongegrond	19	18	13	12	12
Beroep gegrond (volledige of gedeeltelijke toekenning)	24	24	24	12	25
Bijkomende onderzoeksdaden door de overheid	0	2	0	1	1
Bijkomende termijn voor de overheid	1	2	1	1	0
Verleent akte van afstand van beroep	1	0	0	3	2
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)					
Beroep onontvankelijk	0	0	1	0	0
Beroep zonder voorwerp	0	0	1	0	0
Beroep ongegrond	4	1	0	1	1
Beroep gegrond (toekenning)	2	1	1	0	3
Verleent akte van afstand van beroep	–	–	–	-	1
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)					
Beroep onontvankelijk	0	0	1	2	4
Beroep zonder voorwerp	0	0	1	0	0
Beroep ongegrond	8	2	12	2	4
Beroep gegrond (toekenning)	10	4	7	3	4
Verleent akte van afstand van beroep	2	0	1	2	0
Veiligheidsattesten voor nucleaire sector (art. 8*bis*, § 2 W.C&VM)					
Beroep onontvankelijk	–	1	1	0	1
Beroep zonder voorwerp	–	1	0	1	0
Beroep ongegrond	–	0	1	1	5
Beroep gegrond (toekenning)	–	7	5	6	7
Verleent akte van afstand van beroep	–	–	–	2	0
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)					
Beroepsorgaan onbevoegd	0	0	20[183]	12	0

[183] Het betreft *in casu* de beroepen ingediend tegen (negatieve) veiligheidsadviezen van de Nationale Veiligheidsoverheid met betrekking tot personeel van onderaannemers actief bij Europese instellingen. Het Beroepsorgaan had beslist dat er geen wettelijke basis was voor de adviezen van de Nationale Veiligheidsoverheid. Bijgevolg verklaarde het Beroepsorgaan zich onbevoegd om te oordelen over de al dan niet gegrondheid van de veiligheidsadviezen van de Nationale Veiligheidsoverheid.

	2015	2016	2017	2018	2019
Beroep onontvankelijk	6	15	10	3	7
Beroep zonder voorwerp	0	0	1	3	1
Bevestiging van negatief advies	28	42	49	46	40
Omzetting in positief advies	23	46	41	27	43
Verleent akte van afstand van beroep	0	0	1	0	1
Beroep tegen normatieve rechtshandelingen van een administratieve overheid (art. 12 W.Beroepsorgaan)	0	0	0	0	0
TOTAAL	135[184]	173	195	144	166

IX.5. VOORUITZICHTEN

Op aansturen van de voorzitter zijn er uitgebreide reflecties en stappen ondernomen om de werking van het Beroepsorgaan te moderniseren. Er zijn enkele belangrijke doelstellingen bepaald: de vereenvoudiging en standaardisering van de procedure, de verbetering van de toegang tot het rechtscollege voor burgers en de gedigitaliseerde verwerking van dossiers door de griffie.

Net als andere rechtscolleges heeft het Beroepsorgaan zich geëngageerd om zijn juridisch taalgebruik te vereenvoudigen.

Om het Beroepsorgaan te transformeren tot een toegankelijker, efficiënter en moderner rechtscollege moeten de organieke wet en het KB tot regeling van de rechtspleging voor het Beroepsorgaan gewijzigd worden. Om de basisteksten te herzien heeft het een beroep gedaan op een externe deskundige. Het gaat om Ivan Verougstraete, voormalig voorzitter van het Hof van Cassatie. Er vonden verschillende vergaderingen plaats met hem.

Er moet een eenvoudigere procedure met uniforme termijnen voor beroepen worden ontwikkeld. Die procedure moet de rechtsonderhorige ook in staat stellen zijn verzoek langs elektronische weg in te dienen en van de griffie langs dezelfde weg brieven en andere kennisgevingen van beslissingen te verkrijgen.

Ten slotte is het de bedoeling om met dit project de voorwaarden te creëren voor het raadplegen van dossiers op afstand, rekening houdend met de eventuele classificatie van bepaalde documenten waaruit het dossier bestaat.

Ad futurum zal beveiligde elektronische communicatie van zowel het dossier en de documenten ervan als van de beslissingen de norm moeten worden met de verschillende veiligheidsoverheden.

De wens om te vereenvoudigen gaat hand in hand met de ontwikkeling van een IT-platform om de griffie in staat te stellen een beroep volledig digitaal te verwerken.

---

184 Er waren nog twee specifieke beslissingen van verlenen van akte van afstand van beroep, waardoor het totaal in 2015 op 137 kwam.

Daarnaast wordt er ook een specifieke website voor het rechtscollege ontwikkeld. De rechtsonderhorigen, de balies en de administratieve overheden zullen er alle nodige informatie kunnen vinden. De website zal zo worden ontworpen dat, met het oog op de ontwikkeling van de wetgeving, beroepsprocedures langs elektronische weg kunnen worden ingesteld. Bovendien zullen de partijen via dit platform met de griffie in contact kunnen staan over hun dossier.

We merken ook nog op dat er wordt overwogen om de beslissingen te publiceren op die website. Het is belangrijk dat de rechtspraak van het Beroepsorgaan voor iedereen toegankelijk is. Dat is een garantie voor de transparantie van een instelling voor de burger. Die publicatie zal gebeuren in geanonimiseerde vorm, in aanmerking genomen dat de informatie niet van die aard mag zijn dat ze gevaren inhoudt voor een fundamenteel staatsbelang, de geheimhouding van informatie of van een lopend strafonderzoek, de bescherming van de bronnen of de bescherming van de persoonlijke levenssfeer van derden.

HOOFDSTUK X
DE INTERNE WERKING VAN HET VAST COMITÉ I

X.1. SAMENSTELLING VAN HET VAST COMITÉ I

In 2019 wijzigde de samenstelling van het Comité niet: Serge Lipszyc, eerste substituut arbeidsauditeur bij het arbeidsauditoraat van Luik (F), die in al september 2018 de eed aflegde[185], vervulde zijn opdracht als voorzitter. Raadsheren Laurent Van Doren (F), voormalig hoofdcommissaris van politie[186] en Pieter-Alexander De Brock (N), bleven in functie. Hoewel het mandaat van deze laatste verliep in mei 2019, vond zijn herbenoeming pas halfweg januari 2020 plaats.[187]

Bij de Dienst Enquêtes I werd wel een wijziging opgetekend door de aanwerving van een bijkomende commissaris-auditor, gespecialiseerd in ICT. Na enkele maanden tewerkstelling verliet deze de dienst; in september 2019 werd in een vervanging voorzien. De enquêtedienst bestaat daarmee uit zes commissaris-auditoren, waaronder de directeur Frank Franceus (N).

De administratieve staf van het Vast Comité I, onder leiding van griffier Wouter De Ridder (N), bleef in 2019 met 18 administratieve personeelsleden ongewijzigd. Wel verschenen vacatures voor de aanwerving van een Franstalige en een Nederlandstalige statutaire jurist(e) en een Franstalige statutaire secretaris/secretaresse.[188] Het Comité kon blijven beroep doen op de *Data Protection Officer* (DPO) aangesteld voor alle gegevensverwerkingen die buiten de 'nationale veiligheid' vallen (bijvoorbeeld verwerkingen in het kader van het personeelsbeheer en logistiek).

---

185 Op 28 februari 2019 werden respectievelijk Vanessa Samain en Didier Maréchal aangeduid als eerste en tweede plaatsvervangend voorzitter.

186 Er dienden in 2018 meerdere oproepen te worden gelanceerd voor de mandaten van eerste en tweede opvolger van Franstalig lid van het Comité. Op 22 november 2018 werden Thibaut Vandamme en Michel Croquet aangeduid als respectievelijk eerste en tweede plaatsvervanger.

187 *Hand.* Kamer 2019-20 CRIV55PLEN020, 52.

188 *B.S.* 13 juni 2019 en *B.S.* 22 oktober 2019.

X.2. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE

De Kamer van Volksvertegenwoordigers paste tijdens haar plenaire zitting van 17 oktober 2019 het Kamerreglement aan. Hierdoor werd de samenstelling van 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 gewijzigd. Voortaan worden zoveel leden als nodig is benoemd opdat elke in de vaste commissie vertegenwoordigde politieke fractie in de commissie vertegenwoordigd zou zijn door ten minste één lid. Elke politieke fractie die niet vertegenwoordigd is in de commissie wijst onder haar leden een lid aan dat zal deelnemen aan de werkzaamheden van de commissie, zonder evenwel stemgerechtigd te zijn.[189] Maken als stemgerechtigde leden deel uit van de commissie[190]: Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen), Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Marco Van Hees (PVDA-PTB), Egbert Lachaert (Open Vld) en Meryame Kitir (sp.a). De Commissie vergaderde vanaf juni 2019 onder het voorzitterschap van Kamervoorzitter Patrick Dewael (Open Vld). Georges Dallemagne (cdH) neemt deel als niet-stemgerechtigd lid.

In de loop van 2019 vonden slechts twee vergaderingen plaats. Tijdens deze commissievergaderingen werden – achter gesloten deuren – diverse door het Vast Comité I afgesloten toezichtonderzoeken besproken. Ook 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) alsook het verslag opgesteld in het kader van zijn controlebevoegdheid – samen met het Controleorgaan op de politionele informatie (COC) – aangaande de gemeenschappelijke gegevensbanken (art. 44/6 WPA). Tijdens haar vergadering van 17 december 2019 werd het algemeen *Activiteitenverslag 2018* besproken.[191] Het Comité werd bedankt voor '*zijn nauwkeurig verslag, dat voor de commissie een heel nuttig instrument vormt*'. Een aantal thema's weerhielden de bijzondere aandacht van de Kamerleden, zoals de werking van de ADIV, het toezicht op de opvolging van politieke mandatarissen, of nog, de *follow-up* van de aanbevelingen. De Commissie nam als eindconclusie '*akte van het activiteitenverslag 2018 van het Comité I'.* In tegenstelling tot vorige jaar-

189 *B.S.* 25 oktober 2019. '*De reglementswijziging zorgt in de huidige samenstelling van het Parlement voor een kleinere samenstelling van de begeleidingscommissie, wat hopelijk de efficiëntie ten goede zal komen*', in *Hand.* Kamer 2019-20, 17 oktober 2019, CRIV55PLEN009, 33.

190 *Hand.* Kamer 2019-20, 24 oktober 2019, CRIV55PLEN010, 2.

191 De Commissie verwijst daartoe naar artikel 66*bis*, § 2, W.Toezicht, zoals gewijzigd bij de wet van 6 januari 2014 tot wijziging van diverse wetten tot hervorming der instellingen (*BS* 31 januari 2014).

gangen werd '*de goedkeuring aan de aanbevelingen van het Comité*' niet geëxpliciteerd.[192]

In de loop van december 2019 werd de Kamervoorzitter het 'Charter of the Intelligence Oversight Working Group' – ondertekend in het kader van de ontwikkeling van de internationale betrekking van zes controleorganen[193] alsook het 'Beheersplan 2019-2022 van het Vast Comité I' bezorgd.[194] Dat plan bevat enerzijds een '*mission statement*' bedoeld om de institutionele rol van het Comité, de finaliteit van de opdrachten en de waarden die het wenst te bevorderen, vast te leggen. Anderzijds bevat het een opsomming van de strategische en operationele doelstellingen.

X.3. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITÉ P

In 2019 vonden, naast informele contacten op de werkvloer, vijf gemeenschappelijke vergaderingen plaats. 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 tweeerlei: enerzijds het uitwisselen van informatie en anderzijds het opstarten en bespreken van lopende gemeenschappelijke toezichtonderzoeken.

In 2019 was één gemeenschappelijk toezichtonderzoek aan de orde: het reeds eerder opgestarte onderzoek naar de ondersteunende diensten van het OCAD (cf. I.7.1). Er werd beslist geen bijkomende gemeenschappelijke onderzoeken (bijv. naar rechts-extremisme) op te starten.

Verder werden uiteenlopende punten geagendeerd: het gemeenschappelijk statuut van het administratief personeel, de redactie van een deontologisch charter en de aanpassing van het huishoudelijk reglement, de tegensprekelijkheid in het kader van toezichtonderzoeken of nog, de zoektocht naar mogelijke synergiën tussen beide instellingen. Wat dat laatste betreft, werd onder meer een protocol afgesloten inzake het gebruik van de verhoorzaal 'audio en video', werd de (gezamenlijke) schietopleiding van de commissaris-auditoren bestudeerd en werd een opleiding georganiseerd in het kader van de gerechtelijke plaatsopneming.

---

192 *Parl. St.* Kamer 2019-20, nr. 55K0888/001, 20 januari 2020 (Activiteitenverslag 2018 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).

193 Zie bijlage D van dit activiteitenverslag.

194 Het plan werd op 18 oktober 2019 goedgekeurd en per 9 december 2019 bezorgd aan de Kamervoorzitter.

X.4. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Het 'budget 2019' van het Vast Comité I werd vastgelegd op 4,211 miljoen euro, wat een vermeerdering inhield van 12,02% ten aanzien van het budget 2018.[195] Deze belangrijke verhoging werd ingegeven door de betrokkenheid van het Comité in de uitvoering van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (*BS* 5 september 2018) dewelke rechtstreeks voortvloeit uit de Verordering (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016. Titel III van deze wet wijst immers het Vast Comité I aan als 'gegevensbeschermingsautoriteit belast met de controle van de verwerking van persoonsgegevens door de inlichtingen – en veiligheidsdiensten en hun verwerkers'. Deze nieuwe opdracht vereiste een personeelsversterking door de toevoeging van twee juristen en een commissaris-auditor.

De financieringsbronnen van het budget werden door de Kamer van Volksvertegenwoordigers[196] als volgt toegewezen: 89,76% dotatiebudget en 10,24% boni van 2017.

Omwille van het ontslag van de Regering op 21 december 2018 kon het wetsontwerp houdende de algemene uitgavenbegroting voor het begrotingsjaar 2019 niet worden gestemd. Niettemin liet de chronologie van de parlementaire werkzaamheden toe om het budget 2019 formeel goed te keuren en de bepalingen van artikel 2 van de Wet van 25 december 2016[197] uit te voeren, waarmee de toepassing van de bepalingen aangaande de voorlopige twaalfden werd vermeden.

De uitvoering van het budget 2019 leverde een budgettaire bonus op van 475.019 euro, te weten het vastgestelde verschil tussen de inkomsten en de samengestelde uitgaven.

Het budget is traditiegetrouw gebaseerd op verschillende financieringsbronnen en de enige nieuwe bijdrage in termen van eigen beheer, staat ingeschreven in de dotatie van de algemene uitgavenbegroting van de Staat. Tot 2017 was deze dotatie onvoldoende om de reële uitgaven van het Comité te dekken, wat een structureel verlies als gevolg met zich meebracht. De tendens om zoveel mogelijk artikel 57, lid 1, W.Toezicht toe te passen hetwelke vermeldt dat de kredieten die noodzakelijk zijn voor de werking dienen te worden uitgetrokken op de begroting van de dotaties, laat heden ten dage het Comité toe zijn activiteiten te financieren.

Het aanzienlijk boekhoudkundig overschot is vooral te wijten aan het tijdsverloop tussen de goedkeuring van de begroting en met name de daadwerkelijke

---

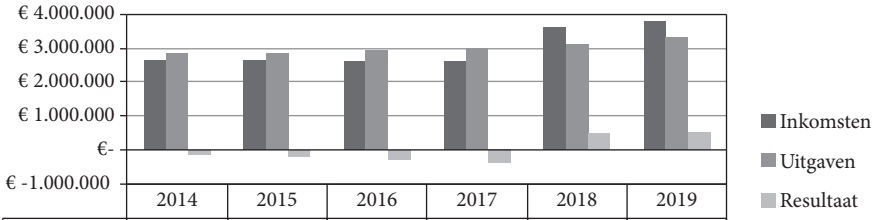
195 *Hand.* Kamer 2019-20 CRIV55PLEN020, 52.

196 *Parl. St.* 2017-2018 Kamer, 54K3418/001, 57-58 en *Hand.* Kamer 2019-20, 20 december 2018, CRIV54PLEN264.

197 Wet van 25 december 2016 tot wijziging van de wet van 22 mei 2003 houdende organisatie van de begroting en van de comptabiliteit van de federale Staat, *B.S.* 29 december 2019, 3° ed.

indiensttreding van het personeel als gevolg van de langdurige aanwervingsprocedures en het verkrijgen van de vereiste veiligheidsmachtigingen. Het valt echter te verwachten dat, van zodra deze nieuwe personeelsleden zijn aangeworven, er een natuurlijk *ceteris paribus* evenwicht zal zijn tussen de inkomsten en uitgaven.

Vast Comité I : Evolutie van de balans



	2014	2015	2016	2017	2018	2019
Inkomsten	€ 2.626.	€ 2.597.	€ 2.570.	€ 2.565.	€ 3.582.3	€ 3.780.9
Uitgaven	€ 2.799.	€ 2.792.	€ 2.889.	€ 2.937.	€ 3.106.8	€ 3.284.9
Resultaat	€ -173.6	€ -194.9	€ -318.8	€ -372.5	€ 475.494	€ 496.019

Parallel met de verwerving van de nieuwe taken die werden toegewezen, waakte het Vast Comité I erover dat het synergiën blijft zoeken en uitvoeren tussen de verschillende dotatiegerechtigde instellingen.

X.5. IMPLEMENTATIE VAN DE AANBEVELINGEN VAN DE AUDIT VAN HET REKENHOF

Op verzoek van de Commissie van de Comptabiliteit van de Kamer van Volksvertegenwoordigers startte het Rekenhof al in december 2017 samen met Ernst and Young een onderzoek naar de dotatiegerechtigde instellingen, waaronder het Vast Comité I. Het Rekenhof richtte zich vooral op de budgettaire aspecten (een analyse van de inkomsten en uitgaven) en op de afbakening van de taken van de diverse instellingen. Ernst and Young op zijn beurt analyseerde de processen, de systemen en de organisatie die in elk van deze instellingen aanwezig zijn. Het auditverslag[198] werd eind maart 2018 opgeleverd. Het formuleerde aanbevelingen voor de 'opdrachten' van de negen bij de audit betrokken dotatiegerechtigde instellingen. Het gemeenschappelijk kenmerk in de opdrachten van deze instellingen *'ligt in het doel om tot een betere rechtsbescherming voor burgers te komen door het uitoefenen van verschillende vormen van toezicht in specifieke beleidsdomeinen'*.

198 *Dotatiegerechtigde instellingen. Opdrachten – Ontvangsten – Uitgaven.* Audit op vraag van de Commissie voor de Comptabiliteit van de Kamer van Volksvertegenwoordigers, Verslag goedgekeurd op 28 maart 2018 door de algemene vergadering van het Rekenhof.

2019 stond in het teken van de implementatie van de talrijke aanbevelingen van de audit. Dit bracht heel wat werk mee voor het Vast Comité I en dit bovenop de toegenomen werklast (*supra*).[199]

X.6. VORMING

Omwille van het belang voor de organisatie, moedigt het Vast Comité I zijn leden en medewerkers aan tot het volgen van algemene (informatica, management …) of sectoreigen opleidingen en conferenties.[200] In dat kader werd in april 2019 een samenwerkingsprotocol afgesloten tussen het Comité en het Instituut voor Gerechtelijke Opleiding.[201] Onderstaande studiedagen werden door een of meerdere (personeels)leden van het Vast Comité I bijgewoond:

DATE	TITRE	ORGANISATION	LIEU
2019-2020	Hogere studies Veiligheid en Defensie	Koninklijk Hoger Instituut voor Defensie	Brussel
24-25 januari 2019	Oversight	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD)	Den Haag
31 januari 2019	Radicalisering, burgerschapszin en onderwijs'	Belgian Intelligence Studies Centre (BISC)	Willebroek
8 februari 2019	Le droit du renseignement	Académie du renseignement	Parijs
5 maart 2019	Oprichtingsvergadering Intelligence Network Europe (INE)	Franse regering	Parijs
7-8 maart 2019	Oversight on intelligence services		Brussel
29-30 maart 2019	Bonne gouvernance dans le domaine de la sécurité	Democratic Centre for Armed Forces (DCAF) / MinInt Tunesië	Tunis
2 april 2019	22ste congres openbare sector 'de digitale ambtenaar'	4Instance	Brussel
25 april 2019	European Defence – the capability issue	Koninklijk Hoger Instituut voor Defensie	Brussel
14 juni 2019	Datarevolutie en terrorismestudies in België – gedachtewisseling tussen praktijk en onderzoek	Egmont Instituut en Coördinatieorgaan voor de dreigingsanalyse (OCAD)	Brussel

199 Het resulteerde in 2020 in een 'opvolgrapport': COUR DES COMPTES, *Institutions à dotation. Suivi des recommandations formulées en 2018*, 57 p.

200 Er vonden ook interne opleidingen plaats, waaronder een aantal (door de medewerkers verplicht bij te wonen) veiligheidsbriefings alsook inlichtingengerelateerde opleidingen.

201 Samenwerkingsprotocol tussen het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten en het Instituut voor Gerechtelijke Opleiding, 4 april 2019.

DATE	TITRE	ORGANISATION	LIEU
31 juli 2019	Werkbezoek	Coordination nationale du renseignement et de la lutte contre le terrorisme, Unité de coordination de la lutte anti-terroriste, Service national du renseignement pénitentiaire	Parijs
13 september 2019	De politionele omgang met geesteszieken en suïcidalen	Vast Comité P	Brussel
8-9 oktober 2019	International Intelligence Oversight Forum (IIOF 2019)	UN-High Commissioner for Human Rights	Londen
2-3 december 2019	Werkbezoek MI5		Londen
12-13 december 2019	European Intelligence Oversight Conference 2019	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD)	Den Haag

Ook worden zeer regelmatig briefings georganiseerd waarbij diverse experten het Comité voorlichten over actuele en belangrijke thema's binnen de *intelligence community* (bijv. over de relatie tussen de inlichtingendiensten en de Algemene directie van de gerechtelijke politie (Directeur-generaal Eric Snoeck), over de strategische visie voor de Belgische Defensie (CHOD Marc Compernol), over de oprichting van de *Joint Intelligence Centers* en *Joint Decision Centers*[202] (Procureur-generaal Johan Delmulle) … Deze briefings moeten een geïnformeerde discussie over de werking, de bevoegdheden en de controle op de inlichtingen- en veiligheidsdiensten en het OCAD alsook op het inlichtingenwerk bevorderen.

[202] Een *Joint Intelligence Centre* (JIC) moet toelaten dat de betrokken diensten (beide inlichtingendiensten, het OCAD en de Federale Gerechtelijke Politie) wekelijks overleg plegen over nieuwe operationele informatie, prioriteiten en taakverdeling. Het *Joint Decision Center* (samengesteld uit voorgaande diensten aangevuld met het Federaal Parket) beslist, op basis van gemeenschappelijke beeldvorming van het JIC, welke dienst met verder onderzoek wordt belast. De (strikte) scheiding tussen politie, inlichtingendiensten en justitie wordt daarmee verlaten en vervangen door een circulaire en collegiale benadering. Zie *Parl. St.* Kamer, 2017-18, nr. 54K1752/008, p. 58.

HOOFDSTUK XI
AANBEVELINGEN

Op basis van de in 2019 afgesloten toezichtonderzoeken, controles en inspecties formuleert het Vast Comité I – soms met het Controleorgaan voor politionele informatie – onderstaande aanbevelingen. Zij hebben zowel betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen, op de coördinatie en de efficiëntie van de inlichtingendiensten, het OCAD en de ondersteunende diensten als op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I.

XI.1. AANBEVELING IN VERBAND MET DE BESCHERMING VAN DE RECHTEN DIE DE GRONDWET EN DE WET AAN PERSONEN WAARBORGEN

XI.1.1. DE AFKONDIGING VAN EEN INTERCEPTIE-KB

Artikel 44/4 W.I&V bepaalt dat het Comité, '*[o]ngeacht de andere bevoegdheden aan dit Comité toegekend op basis van de wet van 18 juli 1991, het recht [heeft] de aan de gang zijnde intercepties, intrusies of beeldopnames te doen stopzetten wanneer blijkt dat ze de wettelijke bepalingen of de [ministeriële] toelating niet respecteren. Het beveelt dat de gegevens die onwettig werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd, volgens de door de Koning te bepalen nadere regels*.' Ook artikel 44/5 W.I&V (verplichte medewerking van een operator) behoeft een uitvoeringsbesluit. Er werden evenwel nog geen dergelijk Koninklijk besluiten getroffen. Het Vast Comité I dringt er (opnieuw) op aan om dit zo spoedig mogelijk te doen.

XI.2. AANBEVELINGEN IN VERBAND MET DE COÖRDINATIE EN DE EFFICIËNTIE VAN DE INLICHTINGENDIENSTEN, HET OCAD EN DE ONDERSTEUNENDE DIENSTEN

XI.2.1. DIVERSE AANBEVELINGEN NAAR AANLEIDING VAN HET TOEZICHTONDERZOEK NAAR VEILIGHEIDSSCREENINGS[203]

XI.2.1.1. Coherente en vereenvoudigde wetgeving inzake screenings

De wetgeving op het vlak van screenings is complex en divers. Het Vast Comité I beveelt aan dat de wetgever deze coherenter en eenvoudiger maakt. Tevens dient voor elke screening duidelijk de inhoud en de finaliteit ervan te worden weergegeven. Ook dient de wetgever te bepalen in welke gevallen een bijkomend inlichtingenonderzoek toegelaten moet zijn. Het is ook aangewezen dat wordt verduidelijkt onder welke omstandigheden de inlichtingendiensten bijkomende informatie mogen inwinnen aangaande de persoon die het voorwerp is van een verificatie. Dit kan nodig zijn om bijvoorbeeld voorhanden zijnde gegevens te actualiseren of te contextualiseren.

XI.2.1.2. Afspraken met overheidsdiensten die bestemmeling zijn van beslissingen van beroepsinstanties

Het Vast Comité I beveelt aan dat beide inlichtingendiensten de nodige afspraken maken met de overheidsdiensten die bestemmeling zijn van de beslissingen van de beroepsinstantie inzake veiligheidsscreenings, ten einde kennis te kunnen nemen van deze beslissingen. Op deze wijze kunnen beide diensten de rechtspraak analyseren, en hiermee rekening houden bij de uitvoering van toekomstige screenings.

XI.2.1.3. Overleg over de finaliteit van de screening

Het Vast Comité I beveelt aan dat de VSSE en de ADIV regelmatig overleg plegen met de verschillende overheden/cliënten die bestemmeling zijn van hun veiligheidsadviezen of inlichtingen. Dit teneinde zich ervan te verzekeren dat de meegedeelde inlichtingen tegemoetkomen aan de finaliteit van de gevraagde screening.[204]

---

203 Zie Hoofdstuk I.1. ('De uitvoering van veiligheidscreenings door de inlichtingendiensten').

204 Welke informatie is nuttig en dient te worden meegedeeld aan de aanvragende overheid in het kader van welk type van verificatie of screening (bijv. de invulling van het begrip '*beletsel wegens gewichtige feiten, eigen aan de persoon*' in het kader van een naturalisatieprocedure).

XI.2.1.4. Systematische bevraging van buitenlandse partnerdiensten

Het Comité beveelt aan dat de nodige (personele) middelen en procedures worden voorzien, in het bijzonder om een systematische bevraging van de buitenlandse partnerdiensten mogelijk te maken, indien de veiligheidsscreening een persoon betreft die voor langere tijd in het buitenland heeft verbleven.[205]

XI.2.1.5. Het opzetten van een registratie- en raadplegingssysteem

Het Vast Comité I beveelt aan dat de VSSE en de ADIV een registratie- en raadplegingssysteem opzetten van de dossiers. Het betreft een *consultation list* waarin wordt vermeld welke dossiers bij de diensten werden onderzocht. Dit moet toelaten om een systematische, centrale registratie van alle interne bewegingen in een dossier te verwezenlijken. Met name is het ook van belang dat er een gecentraliseerd beheer komt van alle antwoorden die door de dienst (bijv. ook door de analysediensten) aan de betrokken overheid/cliënt worden overgemaakt. Dit is noodzakelijk om ervoor te zorgen dat eventuele antwoordtermijnen worden gerespecteerd en dat er coherentie wordt verzekerd in de manier waarop met de partners wordt gecommuniceerd. Het is ook aangewezen om alle stukken van een oorspronkelijk dossier in het kader van een screening, te bewaren en te klasseren. Dit is nuttig voor de uitvoering van een (kwaliteits)controle.

XI.2.1.6. Streven naar een uniforme samenstelling van de dossiers

De manier waarop de VSSE en de ADIV de dossiers in het kader van screenings behandelen, is tevens afhankelijk van externe factoren. Eén van deze factoren is de manier waarop te behandelen dossiers door de overheden/cliënten aan de diensten worden meegedeeld. De diverse (digitale) samenstelling van deze dossiers en eventuele onnauwkeurigheden, kunnen de behandeling ervan beïnvloeden/bemoeilijken. Het Comité beveelt aan om te streven naar een uniforme samenstelling van dossiers, en zelfs voor de aanvraag en behandeling van screenings een integratie van ICT-systemen door te voeren bij de diverse actoren. Ook wordt de creatie van een gemeenschappelijk platform aanbevolen, en dit naar analogie met voor aanvragen van veiligheidsmachtigingen.

XI.2.1.7. Het opzetten van een systeem van interne controle

Het Vast Comité I beveelt aan dat de VSSE en de ADIV een systeem van interne controle opzetten, met inbegrip van de bepaling van prestatie- en beheersindica-

[205] Het alternatief is dat de VSSE en ADIV hieromtrent duidelijke afspraken maken met de NVO om de bevraging van buitenlandse diensten aan deze laatste over te laten.

toren en met uitvoering van een voldoende grote en systematische steekproef om de kwaliteit van de verificaties te controleren en op peil te houden.

XI.2.1.8. Doorgedreven automatisering van de aanvragen

Een doorgedreven automatisering van de aanvragen voor verificaties wordt eveneens aanbevolen. Ideaal zou zijn om een IT-tool te ontwikkelen die toelaat om de controle van namen in een gegevensbank automatisch uit te voeren.

XI.2.1.9. De realisatie van een vademecum

Het Vast Comité I beveelt aan dat zowel de VSSE als de ADIV een vademecum ontwikkelen waarin de interne procedure – met inbegrip van de informatiedoorstroming – en methodologie voor veiligheidsverificaties en screenings wordt beschreven.

XI.2.1.10. Een betere integratie van de Dienst Veiligheidverificaties in het informatiebeheersysteem van de VSSE

Het Vast Comité I beveelt een betere integratie van de Dienst Veiligheidsverificaties in het informatiebeheersysteem van de VSSE aan. De door deze dienst opgestelde documenten dienen consulteerbaar te zijn voor andere departementen. Er dient ook een mechanisme te worden opgezet waarbij door de Dienst VVS opgemerkte onjuistheden in de databank van de VSSE, gemeld en gecorrigeerd worden. Van cruciaal belang is de ontwikkeling van een *'flagging'* systeem in de databank, waarbij alle personen die in deze databank bekend zijn en die het voorwerp uitmaken of hebben uitgemaakt van een veiligheidsverificatie, als dusdanig staan aangeduid. Op deze manier kan dit worden vastgesteld door alle departementen, en kan nieuwe, relevante informatie met betrekking tot de persoon onder de aandacht worden gebracht, waarna indien nodig een nieuw veiligheidsadvies kan worden meegedeeld aan de betrokken overheid.

XI.2.1.11. Omkadering van de opdracht inzake veiligheidsscreenings bij de ADIV

Het Vast Comité I is van mening dat de opdracht inzake veiligheidsverificaties en screenings door de ADIV stiefmoederlijk wordt behandeld, en niet behoorlijk wordt omkaderd door de hiërarchie. Hiertoe moet een duidelijke hiërarchische lijn, inclusief een duidelijk bepaalde eindverantwoordelijke, worden bepaald.[206]

[206] De oplossing die door de ADIV hieromtrent werd vooropgesteld is de integratie van de Cel Screenings binnen het coördinatieorgaan DISCC. De vraag is of dit een afdoende oplossing biedt voor de bestaande dubbelzinnigheid met betrekking tot de hiërarchische verantwoordelijkheid. Naar de mening van het Comité, is het problematisch dat de Cel Screenings onafhankelijk van de Directie S opereert.

XI.2.1.12. Verificaties in alle databanken van de ADIV

Het Comité beveelt aan dat bij de ADIV de Cel Screenings in de mogelijkheid moet zijn om verificaties te doen in alle databanken van de ADIV. Daarenboven dient de ADIV de nodige maatregelen te nemen om zich ervan te verzekeren dat alle databanken die binnen de dienst in gebruik zijn, in voldoende mate worden 'gevoed' met de relevante informatie, en dat dit ook tijdig gebeurt.

XI.2.1.13. Bijhouden van cijfergegevens over de verrichte veiligheidsscreenings

Het Comité beveelt aan dat er bij de ADIV op korte termijn werk wordt gemaakt van het bijhouden van cijfergegevens met betrekking tot het aantal te verrichten en uitgevoerde veiligheidsverificaties. Dit met als doel om een regelmatige evaluatie te kunnen maken van de werklast en de haalbaarheid van antwoordtermijnen in te kunnen schatten. Op deze manier kunnen ook trends worden herkend, kan eventueel worden geanticipeerd op een stijging van het aantal bevragingen, en kunnen desgevallend extra (personele) middelen worden ingezet. Deze cijfergegevens worden best gegroepeerd volgens type van verificatie (wettelijke basis).

XI.2.2. AANBEVELINGEN NAAR AANLEIDING VAN HET TOEZICHTONDERZOEK NAAR CARLES PUIGDEMONT[207]

XI.2.2.1. Een aanpassing van de richtlijn inzake internationale samenwerking

Wat betreft de samenwerking met buitenlandse inlichtingendiensten beveelt het Vast Comité I aan om de richtlijn van de Nationale Veiligheidsraad aan te passen en te actualiseren. Deze richtlijn zou de inhoud moeten specificeren van de inlichtingen die worden uitgewisseld met buitenlandse diensten en zou moeten rekening houden met titel 3 van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, dewelke voorziet in specifieke bepalingen met het oog op het verwerken van persoonsgegevens door inlichtingen- en veiligheidsdiensten, en meer in het bijzonder in specifieke modaliteiten al naargelang de betrokken dienst een Europees dienst is of niet.

XI.2.2.2. Het afsluiten van een samenwerkingsakkoord tussen de ADIV en de VSSE

Wat betreft de verdeling van de taken tot het inwinnen, analyseren en verwerken van inlichtingen met betrekking tot activiteiten van buitenlandse inlichtingen-

[207] Zie Hoofdstuk I.5. ('Puigdemont en de mogelijke activiteiten van buitenlandse inlichtingendiensten in België').

diensten op Belgisch grondgebied, beveelt het Vast Comité I aan dat de Nationale Veiligheidsraad richtlijnen zou aannemen, en dat er een samenwerkingsakkoord zou worden afgesloten tussen de VSSE en de ADIV in uitvoering van artikel 20, § 4, W.I&V.

XI.2.2.3. Opmaak van een lijst van buitenlandse inlichtingen- en veiligheidsdiensten

Wat betreft de aard van de buitenlandse diensten, beveelt het Vast Comité I aan dat de VSSE en de ADIV een lijst zouden opmaken van buitenlandse diensten die zouden kunnen worden gekwalificeerd als zijnde 'een inlichtingen-en veiligheidsdienst' en dit naar analogie met zijn aanbeveling in het kader van het onderzoek naar de internationale contacten van het OCAD.[208]

XI.2.2.4. De ontwikkeling van een gemeenschappelijke methodologie inzake de dreigingsanalyse

Wat betreft de dreigingsevaluatie beveelt het Vast Comité I aan dat de VSSE en de ADIV een gemeenschappelijke methodologie zouden aannemen, geïnspireerd op de methodologie van de VSSE die toelaat om, na een risicoanalyse, maatregelen te nemen qua geloofwaardigheid, qua mogelijke acties en qua proportionaliteit. Dergelijke methodologie moet tevens toelaten om onder meer:
- de traceerbaarheid van documenten en van beslissingen te garanderen met de bedoeling om *a posteriori* een controle mogelijk te maken door het Vast Comité I;
- zich ervan te vergewissen dat de inlichtingendienst zijn beslissingen en genomen maatregelen meedeelt aan de bevoegde minister.

XI.2.3. AANBEVELINGEN NAAR AANLEIDING VAN HET TOEZICHTONDERZOEK NAAR DE WERKING VAN DE AFDELING HUMINT VAN DE ADIV[209]

XI.2.3.1. Aanbevelingen voor het beheer en de planning van de inlichtingenactiviteiten

Het Vast Comité I beveelt aan:
- dat de ADIV in de verschillende plannen aanduidt waarom de landen of thema's een bepaald prioriteitsniveau worden toegewezen, door expliciet te verwijzen naar nationale of internationale belangen;

---

208 VAST COMITÉ I, *Activiteitenverslag 2015*, 106-108.

209 Zie Hoofdstuk I.2. ('De werking van de Afdeling HUMINT bij de militaire inlichtingendienst doorgelicht').

- om het gebruik van de verschillende beheersdocumenten, het Inlichtingenstuurplan, *IntelFocus* en de *Intelligence Collection Plans* te uniformiseren. Waar nodig moeten eventuele verschillen in die beheersdocumenten expliciet worden gemotiveerd (bijv. de reden waarom landen die in één plan als prioritair worden beschouwd dat in een ander plan niet zijn);
- dat de *Intelligence Collection Plans* binnen de Directie Intelligence van de ADIV een vaste en eenvormige structuur krijgen voor alle collectediensten (inclusief I/H) en continu worden bijgewerkt;
- om een inventaris op te stellen van de inzet van de middelen van zijn verschillende collectediensten om eventuele hiaten op te sporen en te bepalen welke dreigingen of prioriteiten aandacht en middelen in beslag nemen. Dat overzicht zou het mogelijk maken om *in fine* de collectediensten te optimaliseren en complementair te maken;
- dat de ADIV een evaluatie van de bronnen uitvoert (al naargelang de situatie een specifieke, permanente of periodieke), om na te gaan of hun inzet strookt met de prioriteiten;
- om te zorgen dat de menselijke bronnen van zijn verschillende collecte-organen, waaronder I/H, gezamenlijk worden gecoördineerd en beheerd. Wat dat betreft, raadt het Vast Comité I ook aan om de bestaande bronnen te zuiveren om capaciteiten vrij te maken en om nieuwe bronnen te rekruteren, en om zo een zekere evolutie/vernieuwing te verzekeren;
- om te zorgen voor de opvolging, evaluatie en bijwerking van de verschillende beheersdocumenten, het Inlichtingenstuurplan, *IntelFocus* en de *Intelligence Collection Plans*.

XI.2.3.2. Aanbevelingen voor de middelen van de Afdeling I/H

Eens het beheer en de planning van de inlichtingenactiviteiten van Afdeling I/H gedefinieerd zijn (in aanvulling op andere collecteverzamelingsdiensten van de ADIV), moeten er middelen worden toegewezen. Wat betreft het organigram en de toewijzing van personeel heeft het Vast Comité I meerdere problemen vastgesteld waarvan de ADIV de minister van Landsverdediging op de hoogte moet brengen, opdat er investeringen zouden worden gedaan. Het Comité beveelt dan ook aan:

- om een analyse van de personeelsbehoeften uit te voeren[210], een toekomstgerichte organieke tabel op te stellen en het personeelsbestand van de dienst op peil te brengen op basis van de behoeften van een dienst die menselijke bronnen beheert in het kader van opdrachten zoals die van de ADIV;

[210] Onder meer rekening houdend met het aantal bronnen dat een Case Officer kan beheren en de steun die hij nodig heeft. Dat vereist een samenwerking met de 'Personeel en Organisatie'-specialisten van Landsverdediging en een benchmarking bij andere diensten die dezelfde opdrachten krijgen toegewezen.

– om het verloop van het personeel binnen de Afdeling I/H te beperken;
– herhaalt ook dat de ontwikkeling van een nieuwe 'inlichtingen'-tak binnen Landsverdediging of de uitwerking van alternatieve oplossingen kan bijdragen tot het aantrekken van personeel dat gespecialiseerd is in inlichtingen en tot het ontwikkelen van hun carrière. Het Comité verwijst naar zijn eerdere aanbevelingen.[211]

XI.2.3.3. Aanbevelingen voor het beheer van de bronnen en voor de procedures

Eens het beheer en de planning van de inlichtingenactiviteiten zijn opgesteld en de middelen zijn vrijgemaakt om ze in de praktijk te brengen, moeten er processen en werkprocedures worden uitgewerkt. Het Vast Comité I benadrukte dat het gebruik van menselijke bronnen voor het verzamelen van gegevens (zie artikel 18 W.I&V) richtlijnen van de Nationale Veiligheidsraad vereist.

Het Vast Comité I stelde vast dat ondanks het op dat moment ontbreken van een dergelijke richtlijn van de Nationale Veiligheidsraad de meerderheid van de interne richtlijnen (SOP) van de Afdeling I/H-dienst werd bijgewerkt in 2018. Niettemin beveelt het Comité aan:
– dat de Afdeling I/H zijn inspanningen voor de evaluatie van bronnen en de inlichtingenbulletins die ze aanleveren, voortzet. Wat betreft die laatste moeten I/H en de analysediensten een gemeenschappelijke planning vastleggen om samen de doelstelling te bereiken[212];
– een proces voor interne controle te implementeren, met name om steeds te blijven letten op de naleving van de procedures, vooral binnen I/H geïmplementeerde procedures[213];
– dat de verschillende richtlijnen (SOP) opgenomen worden in een geclassificeerd *vademecum* voor het personeel.

---

211 Zie VAST COMITÉ I, *Activiteitenverslag 2011*, p. 12 en 106, *Activiteitenverslag 2018*, p. 135, Aanbevelingen met betrekking tot het personeelsbeheer en de carrières, opleiding en training.

212 De verantwoordelijkheid voor de evaluatie van de bron ligt bij I/H zelf, wetende dat die dienst zelf afhankelijk is van de evaluatie van de inlichtingenbulletins en de feedback van de analysediensten voor wie de informatie *in fine* bestemd is. De reorganisatie van de ADIV begin 2020 zou tot gevolg hebben dat alle collectediensten van de ADIV worden samengebracht in één pijler en alle analysediensten in een andere pijler, terwijl die diensten in de huidige situatie gemengd zijn. Die reorganisatie zou kunnen worden benut om de eerder vermelde doelstelling te bereiken. Maar de aanpak moet realistisch zijn in de zin dat hij rekening moet houden met de beschikbare middelen.

213 Het Vast Comité I erkent dat deze aanbeveling bij gebrek aan meetbaarheid onrealistisch kan lijken.

XI.2.4. AANBEVELINGEN MET BETREKKING TOT DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN

XI.2.4.1. Evaluatie van belangenconflicten en de tijdsbesteding van de functionaris van de gegevensbescherming

Gelet op de veelheid aan functies die de functionaris van de gegevensbescherming bij de GGB TF en HP combineert, is het van belang dat, met het oog op een eerstvolgende controle van het COC en het Vast Comité I, een heldere evaluatie wordt gemaakt van eventuele belangenconflicten, alsook van de tijdsbesteding aan de taken die de functionaris van de gegevensbescherming van de gemeenschappelijke gegevensbank hoort te vervullen.

XI.2.4.2. Waken over het need to know-principe

Gelet op de nakende uitbreiding van het aantal partnerdiensten dat rechtstreeks toegang zal hebben tot de GGB TF en HP, is het van belang dat de DPO van de GGB TF en HP nauwlettend in de gaten houdt in hoeverre de voeding van de gegevensbank door de verschillende partnerdiensten kan overlappen, en in welke mate dergelijke overlapping in strijd is met het '*need to know*'-principe. Diensten die rechtstreekse of onrechtstreekse toegang hebben tot de GGB TF en HP moeten hiertoe een 'noodzaak' hebben bij het nemen van beslissingen die kaderen binnen hun bevoegdheden. In dat kader dient erop gewezen te worden dat een partnerdienst (met uitzondering van het Openbaar Ministerie) de nodige inspanning dient te leveren om de gegevensbank te voeden, en kan het geenszins de bedoeling zijn dat een rechtstreekse toegang met schrijfrecht wordt verstrekt om in de praktijk zich ervan te verzekeren dat één van de diensten met schrijfrecht de relevante informatie zou opnemen in de GGB TF en HP.

XI.2.4.3. Ondernemen van actie bij veiligheidsincidenten

De standaardprocedure inzake veiligheidsincidenten dient voldoende te worden bekendgemaakt bij de betrokken diensten opdat zij niet enkel met het bestaan ervan maar ook met de werking ervan vertrouwd zouden zijn. Daarnaast dienen het COC en het Vast Comité I (sneller) ingelicht en (nauwer) betrokken te worden bij dergelijke incidenten. Zowel 'kleine' als 'grote loggingcontroles' dienen systematischer te worden uitgevoerd door alle betrokken diensten. De operationeel beheerder bekleedt hierbij een sleutelpositie.

XI.2.4.4. Protocollen inzake de doorgifte van mailinglijsten

De operationeel verantwoordelijke van de gemeenschappelijke gegevensbank, alsook de functionaris van de gegevensbescherming dienen erop toe te zien dat

voor de mailinglijsten aan derde instanties op grond van artikel 44/11/3*quater* WPA protocollen voorhanden zijn waarin de voorwaarden zijn geregeld voor dergelijke doorgiften. Daarin dient de nodige aandacht te worden besteed aan het verbod om deze gegevens verder te verspreiden. Het opstellen van dergelijke protocollen zal in een volgend rapport verder worden opgevolgd.

XI.2.4.5. Evaluatie van de rechtstreekse toegang voor partnerdiensten

Met betrekking tot de partnerdiensten die voor meerdere jaren géén gebruiker en géén loggings hebben aangeduid voor de GGB TF en HP, wijzen het COC en het Vast Comité I op een mogelijk gebrek aan de 'behoefte om te kennen' en dient er in de toekomst te worden geëvalueerd in welke mate nog aan de voorwaarden van artikel 44/11/3*ter* § 2 WPA is voldaan. Mogelijks dient na voormelde evaluatie de al dan niet rechtstreekse toegang van bepaalde partnerdiensten te worden herzien.

XI.3. AANBEVELING IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

XI.3.1. ACCURATE INFORMATIE OVER DE WERKING VAN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN

Het COC en het Vast Comité I dienen nauwer op de hoogte gesteld te worden van beleidsbeslissingen, overlegmomenten tussen de betrokken diensten, (jaar)rapporten en vergaderingsverslagen betreffende (de werking van) de GGB TF en HP.

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 2019 TOT 31 DECEMBER 2019)

Wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, *BS* 3 mei 2019

Wet van 2 mei 2019 tot wijziging van diverse bepalingen betreffende de verwerking van passagiersgegevens, *BS* 24 mei 2019

Wet van 9 mei 2019 tot wijziging van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid voor wat betreft de verwerking van gegevens, *BS* 5 juni 2019

Wet van 3 juli 2019 tot wijziging van de wet van 21 december 2013 houdende het Consulair Wetboek en van de wet van 10 februari 2015 met betrekking tot geautomatiseerde verwerkingen van persoonsgegevens die noodzakelijk zijn voor de Belgische paspoorten en reisdocumenten, *BS* 22 augustus 2019

K.B. 17 augustus 2018 tot uitvoering van artikel 2, eerste lid, 2°, g) van de wet van 10 juli 2006 betreffende de analyse van de dreiging – addendum, *BS* 10 januari 2019

K.B. 2 december 2018 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten, *BS* 18 januari 2019

K.B. 31 januari 2019.tot wijziging van het koninklijk besluit van 2 juni 2015 tot oprichting van het Strategisch Comité en Coördinatiecomité voor inlichting en veiligheid, *BS* 11 februari 2019

K.B. 3 februari 2019 ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, houdende de verplichtingen opgelegd aan de HST-vervoerders en de HST-ticketverdelers, *BS* 12 februari 2019

K.B. 3 februari 2019 ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, houdende de verplichtingen opgelegd aan de busvervoerders, *BS* 12 februari 2019

K.B. 26 april 2019 houdende gedeeltelijke verdeling, betreffende de strijd tegen het terrorisme en het radicalisme van het provisioneel krediet ingeschreven in het programma 06-90-1 van de wet van 27 maart 2019 tot opening van voorlopige kredieten voor de maanden april, mei, juni en juli 2019 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* 6 mei 2019

K.B. 12 juli 2019 tot uitvoering van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, en van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren, *BS* 18 juli 2019

K.B. 16 juli 2019 tot wijziging van het koninklijk besluit van 26 juni 2002 betreffende het voorhanden hebben en het dragen van wapens door de diensten van het openbaar gezag of van de openbare macht, *BS* 2 augustus 2019

K.B. 1 oktober 2019 tot wijziging van diverse koninklijke besluiten ter uitvoering van de wapenwet, *BS* 9 oktober 2019

K.B. 2 oktober 2019 tot wijziging van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, *BS* 4 november 2019

Vergelijkende Nederlandstalige selectie voor bevordering naar niveau A (reeks 3) voor de Veiligheid van de Staat: Attachés analisten (m/v/x) – selectienummer: BNG19004, *BS* 25 februari 2019

Vergelijkende Nederlandstalige selectie voor bevordering naar niveau C (specifiek gedeelte) voor de Veiligheid van de Staat: Veiligheidsassistenten (m/v/x) – selectienummer: BNG19005, *BS* 25 februari 2019

Resultaat van de voorafgaande proef in de vergelijkende selectie van Nederlandstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B), voor de Veiligheid van de Staat – selectienummer: ANG18253, *BS* 5 maart 2019

Resultaat van de vergelijkende selectie van Franstalige deskundigen rekrutering en selectie (m/v/x) (niveau B), voor de Veiligheid van de Staat – selectienummer: AFG18285, *BS* 5 maart 2019

Resultaat van de voorafgaande proef in de vergelijkende selectie van Franstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B) voor de Veiligheid van de Staat – selectienummer: AFG18249, *BS* 6 maart 2019

Bericht voorgeschreven bij artikel 74 van de bijzondere wet van 6 januari 1989, bij verzoekschrift dat aan het Hof is toegezonden bij op 13 maart 2019 ter post aangetekende brief en ter griffie is ingekomen op 14 maart 2019, is beroep tot vernietiging ingesteld van artikel 5 van de wet van 30 juli 2018 tot oprichting van lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme (bekendgemaakt in het Belgisch Staatsblad van 14 september 2018) door de vzw "TCC-Accueil, ASBL", de vzw "AtMOsphères", de vzw "Bureau d'Accueil et de Défense des Jeunes", de vzw "Coordination des Organisations non gouvernementales pour les droits de l'enfant", de vzw "Dynamo international", de vzw "Dynamo", de vzw "Fédération Laïque de l'Aide à la Jeunesse", de vzw "Kinderrechtencoalitie Vlaanderen", de vzw "Ligue des droits humains", de vzw "Samarcande" en de vzw "Uit de marge/CMGJ". Die zaak is ingeschreven onder nummer 7141 van de rol van het Hof, *BS* 19 april 2019

Resultaat van de vergelijkende selectie van Nederlandstalige Jurist Algemene Dienst Inlichtingen en Veiligheid (ADIV) (m/v/x), (niveau A1), voor het Ministere van Defensie – selectienummer: ANG18305, *BS* 7 mei 2019

Uittreksel uit arrest nr. 41/2019 van 14 maart 2019, rolnummer 6758, in zake: het beroep tot vernietiging van de artikelen 4, 4°, en 5, litterae e), f) en g), tweede streepje, 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" (nieuw artikel 2, § 3, artikel 3, 12°, artikel 3, 12°/1, en artikel 3, 14°, litterae a) en b), van de voormelde wet van 30 november 1998), ingesteld door de vzw "Liga voor Mensenrechten", *BS* 8 mei 2019

Personeel – aanstelling van een titularisvan een managementfunctie, *BS* 21 mei 2019

Huishoudelijk reglement van 24 april 2019 van het directiecomité van de Veiligheid van de Staat, *BS* 31 mei 2019

Resultaat van de vergelijkende Nederlandstalige selectie voor bevordering naar niveau C (specifiek gedeelte) voor de Veiligheid van de Staat: Veiligheidsassistenten (m/v/x) – selectienummer: BNG19005, *BS* 11 juni 2019

Resultaat van de vergelijkende Franstalige selectie voor bevordering naar niveau C (specifiek gedeelte) voor de Veiligheid van de Staat: Veiligheidsassistenten (m/v/x) – selectienummer: BFG19006, *BS* 11 juni 2019

Vast Comité van Toezicht op de Inlichtingen- en veiligheidsdiensten, aanwerving voor indiensttreding en samenstelling van een wervingsreserve van een Nederlandstalige statutaire jurist(e), (niv. A), *BS* 13 juni 2019

Vast Comité van Toezicht op de Inlichtingen- en veiligheidsdiensten – aanwerving voor indiensttreding en samenstelling van een wervingsreserve van een Franstalige statutaire jurist(e), (niv. A), *BS* 13 juni 2019

Resultaat van de vergelijkende Nederlandstalige selectie voor bevordering naar niveau A (reeks 3) voor de Veiligheid van de Staat Attachés analisten (m/v/x) – selectienummer: BNG19004, *BS* 19 juli 2019

Resultaat van de vergelijkende Franstalige selectie voor bevordering naar niveau A (reeks 3) voor de Veiligheid van de Staat: Attachés analisten (m/v/x) – selectienummer: BFG19005, *BS* 19 juli 2019

Vergelijkende selectie van Nederlandstalige Ingenieurs Inlichting en Veiligheid (m/v/x) (niveau A1) voor het Ministerie van Defensie – selectienummer: ANG18292, *BS* 2 augustus 2019

Uittreksel uit arrest nr. 112/2019 van 18 juli 2019, rolnummers 6749 en 6755, in zake: de beroepen tot gehele of gedeeltelijke vernietiging van de wet van 24 februari 2017 tot wijziging van dewet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering vanvreemdelingen, met het doel de bescherming van de openbare orde en de nationale veiligheid te versterken, ingesteld-door de "Ordre des barreaux francophones et germanophone" en door de vzw "Association pour le droit des Étrangers" en anderen, *BS* 26 augustus 2019

Vergelijkende selectie van Nederlandstalige Cyber Security Expert (A2) (m/v/x) (niveau A2) voor het Ministerie van Defensie – selectienummer: AFG19115, *BS* 2 september 2019

Vergelijkende selectie van Franstalige Cyber Security Expert (A2) (m/v/x) (niveau A2) voor het Ministerie van Defensie – selectienummer: AFG19115, *BS* 2 september 2019

Vergelijkende selectie van Franstalige operationele netwerkspecialisten (m/v/x) (niveau B) voor het ministerie van Defensie – selectienummer: AFG19118, *BS* 9 september 2019

Vergelijkende selectie van Franstalige Senior system engineer (m/v/x) (niveau A2) voor het Ministerie van Defensie – selectienummer: AFG19119, *BS* 9 september 2019

Vergelijkende selectie van Nederlandstalige Psychologen (m/v/x) (niveau A1) voor de Veiligheid van de Staat – selectienummer: ANG19287, *BS* 19 september 2019

Resultaat van de vergelijkende selectie van Nederlandstalige Ingenieurs Inlichting en Veiligheid (m/v/x), (niveau A1), voor het Ministerie van Defensie – selectienummer: ANG18292, *BS* 21 oktober 2019

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, samenstelling van een wervingsreserve van een Franstalige statutaire secretaris/secretaresse, (niv. B), *BS* 22 oktober 2019

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, aanwerving voor indiensttreding en samenstelling van een wervingsreserve van een Franstalige statutaire jurist(e), (niv. A), *BS* 22 oktober 2019

Reglement van de Kamer van volksvertegenwoordigers, wijzigingen, *BS* 25 oktober 2019

Uittreksel uit arrest nr. 111/2019 van 18 juli 2019 Rolnummers 6733, 6750 en 6753, in zake: de beroepen tot gehele of gedeeltelijke vernietiging van de wet van 15 maart 2017 tot wijziging van artikel 39/79 van de wet van 15 december 1980 betreffende de toegang tot het grondgebied, het verblijf, de vestigingen de verwijdering van vreemdelingen, ingesteld door de vzw "Liga voor Mensenrechten" en de vzw "Ligue desDroits de l'Homme", door de "Ordre des barreaux francophones et germanophone" en door de vzw "Association pour le droit des Étrangers" en anderen, *BS* 8 november 2019

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 2019 TOT 31 DECEMBER 2019)

Senaat

Interparlementaire Conferentie over het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB) en het Gemeenschappelijk Veiligheids- en Defensiebeleid (GVDB) Helsinki, 4-6 september 2019, *Parl. St.* Senaat 2019, nr. 7-10/1

Kamer van Volksvertegenwoordigers

De problematiek van de uitreiking van de humanitaire visa – hoorzitting met: F. Roosemont, directeur-generaal van de Dienst Vreemdelingenzaken; D. Van den Bulck, commissaris-generaal voor de Vluchtelingen en de Staatlozen; F. De Smet, directeur, en A. Declercq en I. Vandenberghe, beleidsmedewerkers van Myria, *Hand.* Kamer 2018-19, 29 januari 2019, CRIV54COM1021, 1

De problematiek van de uitreiking van de humanitaire visa – hoorzitting met: J. De Volder en P. Wieërs, vertegenwoordigers van Sant'Egidio; M. Geleyn, oud-directeur-generaal van de FOD Buitenlandse Zaken; J.-F. Parmentier, Belgische consul in Beiroet, *Hand.* Kamer 2018-19, 5 februari 2019, CRIV54COM1027, 1

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – benoeming van de voorzitter en van de eerste en tweede plaatsvervangende voorzitter – ingediende kandidaturen, *Hand.* Kamer 2018-19, 7 februari 2019, CRIV54PLEN269, 56

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – benoeming van de eerste en van de tweede plaatsvervangende voorzitter, *Hand.* Kamer 2018-19, 28 februari 2019, CRIV54PLEN273, 29

Voorstel van resolutie over de evolutie en de modernisering van het reservekader van de Krijgsmacht, *Parl. St.* Kamer 2018-19, nrs. 54K2683/006 en 54K2683/009 tot 54K2683/011

Wetsontwerp tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, *Parl. St.* Kamer 2018-19, nrs. 54K3340/003 en 54K3340/004

Activiteitenverslag 2017 van het Vast Comité van Toezicht op de inlichtingen- en de veiligheidsdiensten, *Parl. St.* Kamer 2018-19, nr. 54K3375/001

Het verslag van de onderzoekscommissie van de assemblée nationale van de Franse Republiek betreffende "de veiligheid en de beveiliging van de nucleaire installaties" en de Belgische kerncentrales: analyse van het FANC, *Parl. St.* Kamer 2018-19, nr. 54K3479/001

Wetsvoorstel houdende diverse bepalingen in strafzaken en inzake erediensten, *Parl. St.* Kamer 2018-19, nrs. 54K3515/001 tot 54K3515/003, 54K3515/005 tot 54K3515/011 en 54K3515/014

Wetsvoorstel houdende diverse bepalingen inzake informatisering van Justitie en modernisering van het statuut van rechters in ondernemingszaken, *Parl. St.* Kamer 2018-19, nr. 54K3549/001

Wetsvoorstel tot wijziging van de wet van 21 december 2013 houdende het Consulair Wetboek en van de wet van 10 februari 2015 met betrekking tot geautomatiseerde verwerkingen van persoonsgegevens die noodzakelijk zijn voor de Belgische paspoorten en reisdocumenten (3574/1-3), *Parl. St.* Kamer 2018-19, nr. 54K3574/001 en *Hand.* Kamer 2018-19, 28 maart 2019, CRIV54PLEN278, 4

Wetsvoorstel houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *Parl. St.* Kamer 2018-19, nrs. 54K3575/001 tot 54K3575/006 en *Hand.* Kamer 2018-19, 21 februari 2019, CRIV54PLEN271, 91

De problematiek van de uitreiking van humanitaire visa – gedachtewisseling met de minister van Sociale Zaken en Volksgezondheid, en van Asiel en Migratie over de resultaten van het administratief onderzoek, *Hand.* Kamer 2018-19, 13 maart 2019, CRIV54COM1056, 1

Wetsontwerp tot wijziging van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid voor wat betreft de verwerking van persoonsgegevens, *Parl. St.* Kamer 2018-19, nrs. 54K3639/001, 54K3639/002, 54K3639/005 tot 54K3639/007

Voorstel van resolutie over de bevordering van de investeringen van Defensie in dual use-innovaties voor burgerlijk en militair gebruik, en over de verrekening van die investeringen in de NAVO-doelstelling om 2% van het bbp aan Defensie te besteden, *Parl. St.* Kamer 2018-19, nrs. 54K3641/001

Wetsontwerp tot wijziging van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, *Parl. St.* Kamer 2018-19, nrs. 54K3652/001, 54K3652/003 en 54K3652/004

Voorstel tot herziening van het Reglement van de Kamer van volksvertegenwoordigers, teneinde de opvolging van de aanbevelingen van het Comité P en het Comité I te verbeteren, *Parl. St.* Kamer 2018-19, nr. 54K3654/001

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, alsook tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van het Vast Comité I en van het Vast Comité P, *Parl. St.* Kamer 2018-19, nr. 54K3658/001

Wetsvoorstel tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft, *Parl. St.* Kamer 2018-19, nrs. 54K3697/001, 54K3697/003, 54K3697/004 en van 54K3697/006 tot 54K3697/008

De mogelijke uitbreiding van de camerawet, *Parl. St.* Kamer 2018-19, nr. 54K3727/001

Voorstel van resolutie over de oprichting van een federaal inlichtingenagentschap, *Parl. St.* Kamer 2019-20, nr. 55K0287/001

Voorstel van resolutie tot het invoeren van een mechanisme voor de screening van buitenlandse investeringen in ondernemingen die actief zijn in strategische sectoren, *Parl. St.* Kamer 2019-20, nr. 55K0422/001

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – benoeming van het Nederlandstalig lid en van het eerste en het tweede Nederlandstalig plaatsvervangend lid – Ingediende kandidaturen, *Hand.* Kamer 2019-20, 26 september 2019, CRIV55PLEN006, 43

Voorstel tot wijziging van artikel 149 van het Reglement van de Kamer van volksvertegenwoordigers betreffende de samenstelling van de commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I, *Parl. St.* Kamer 2019-20, nrs. 55K0520/001 tot 55K0520/003

De veiligheidssituatie van de gevangeniskampen in Noord-Syrië en het lot van de Belgische Foreign Terrorist Fighters, gelet op de Turkse invasie – hoorzitting met luitenant-generaal Cl. Van de Voorde, hoofd van de Algemene Dienst Inlichting en Veiligheid (ADIV); – de heer P. Van Tigchelt, directeur van het Coördinatieorgaan voor de Analyse van de Dreiging (OCAD); – de heer F. Van Leeuw, federaal procureur, *Hand.* Kamer 2019-20, 16 oktober 2019, CRIV55COM032, 1

Reglement van de Kamer, *Hand.* Kamer 2019-20, 17 oktober 2019, CRIV55PLEN009, 52

Samenstelling commissie begeleiding Vast Comité P + I, *Hand.* Kamer 2019-20, 24 oktober 2019, CRIV55PLEN010, 3

Voorstel van resolutie over het HR-beleid bij Defensie, *Parl. St.* Kamer 2019-20, nr. 55K0567/006

Voorstel van resolutie over de betreffende het terughalen van kinderen van Syriëstrijders, *Parl. St.* Kamer 2019-20, nr. 55K0674/001

Opvolging van de aanbevelingen van de parlementaire onderzoekscommissie "Terroristische aanslagen". Gedachtewisseling met de minister van Veiligheid en Binnenlandse Zaken, belast met Buitenlandse Handel, *Hand.* Kamer 2019-20, 5 november 2019, CRIV55COM044, 1

Opvolging van de aanbevelingen van de parlementaire onderzoekscommissie "Terroristische aanslagen" – Antwoorden van de vice-eersteminister en minister van Justitie, belast met de Regie der Gebouwen, en minister van Europese Zaken, en van de minis-

ter van Veiligheid en Binnenlandse Zaken, belast met Buitenlandse Handel, *Hand.* Kamer 2019-20, 10 december 2019, CRIV55COM069, 1

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, Gegevensbeschermingsautoriteit, Benoemingscommissies voor het notariaat, BIM-Commissie, Controleorgaan op de politionele informatie, Federale Deontologische Commissie, Centrale Toezichtsraad voor het Gevangeniswezen – Rekeningen van het begrotingsjaar 2018 – Begrotingsaanpassingen van het begrotingsjaar 2019 – Begrotingsvoorstellen voor het begrotingsjaar 2020 (867/1-3), *Hand.* Kamer 2019-20, 19 december 2019, CRIV55PLEN018, 94

Voorstel tot herziening van het Reglement van de Kamer van volksvertegenwoordigers, teneinde de opvolging van de aanbevelingen van het Comité P en het Comité I te verbeteren, *Parl. St.* Kamer 2019-20, nr. 55K0868/001

Benoeming van het Nederlandstalig effectief lid en van het eerste en het tweede Nederlandstalig plaatsvervangend lid van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, *Parl. St.* Kamer 2019-20, nr. 55K0878/001

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 2019 TOT 31 DECEMBER 2019)

Senaat

Schriftelijke vraag van L. Bajart aan de minister van Financiën over de religieuze liefdadigheidsorganisaties – scherpere controle door de belastingdiensten – Nederland – cijfers' (Senaat 2018-19, 11 januari 2019, Vr. nr. 6-2114)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Ondersteuningsnetwerk van veroordeelde terroristen – oproepen tot het bevrijden van gedetineerden – handhaving – Veiligheid van de Staat' (Senaat 2018-19, 11 januari 2019, Vr. nr. 6- 2118)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Veroordeelde terroristen – communicatie via smartphones – aanwezigheid gsm's in gevangenissen – Veiligheid van de Staat' (Senaat 2018-19, 11 januari 2019, Vr. nr. 6- 2119)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Ondersteuningsnetwerk van veroordeelde terroristen – mogelijke rol als incubator voor terroristen – bezoekrecht in gevangenissen – Veiligheid van de Staat' (Senaat 2018-19, 14 januari 2019, Vr. nr. 6- 2124)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Kinderen van Belgische Syriëstrijders – indoctrinatie door ISIS – trauma's – risico's voor onze samenleving' (Senaat 2018-19, 14 januari 2019, Vr. nr. 6- 2130)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'minderjarige jihadisten – kindsoldaten – risico's voor onze samenleving – bevestigde gedetecteerde aanwezigheid tussen asielzoekers in ons land' (Senaat 2018-19, 14 januari 2019, Vr. nr. 6- 2138)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Religieuze liefdadigheidsorganisaties – giften vanwege Golfstaten – Nederland – cijfers' (Senaat 2018-19, 14 januari 2019, Vr. nr. 6- 2140)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Veiligheid van de Staat (VSSE) – buitenlandse partnerdiensten – vraag tot telefoonidentificatie – responstijd – terrorisme' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2174)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Algemene Dienst Inlichting en Veiligheid (ADIV) – Operation Vigilant Guardian – aanslag in Parijs – twee rapporten over de aanwezigheid van mededader op Zaventem – doorstroming van de informatie tussen de diensten' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2176)

Schriftelijke vraag van L. Bajart aan de minister van Buitenlandse Zaken over de 'Algemene Dienst Inlichting en Veiligheid (ADIV) – Operation Vigilant Guardian – aanslag in Parijs – twee rapporten over de aanwezigheid van mededader op Zaventem – doorstroming van de informatie tussen de diensten' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2177)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Algemene Dienst Inlichting en Veiligheid (ADIV) – force protection – Operation Vigilant Guardian (OVG) – doorgeven en ontvangen van informatie' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2178)

Schriftelijke vraag van L. Bajart aan de minister van Buitenlandse Zaken over de 'Algemene Dienst Inlichting en Veiligheid (ADIV) – force protection – Operation Vigilant Guardian (OVG) – doorgeven en ontvangen van informatie' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2179)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Algemene Dienst Inlichting en Veiligheid (ADIV) – aanwezigheid van de heer Abaaoud in de Brusselse regio in 2015 – doorstroming van de informatie tussen de diensten' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2180)

Schriftelijke vraag van L. Bajart aan de minister van Buitenlandse Zaken over de 'Algemene Dienst Inlichting en Veiligheid (ADIV) – aanwezigheid van de heer Abaaoud in de Brusselse regio in 2015 – doorstroming van de informatie tussen de diensten' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2181)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'Algemene Dienst Inlichting en Veiligheid (ADIV) – Operation Vigilant Guardian – verdachte die veiligheidsdispositief Zaventem filmt in november 2015 – melding – doorstroming van de informatie tussen de diensten' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2182)

Schriftelijke vraag van L. Bajart aan de minister van Buitenlandse Zaken over de 'Algemene Dienst Inlichting en Veiligheid (ADIV) – Operation Vigilant Guardian – verdachte die veiligheidsdispositief Zaventem filmt in november 2015 – melding – doorstroming van de informatie tussen de diensten' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2183)

Schriftelijke vraag van L. Bajart aan de minister van Buitenlandse Zaken over de 'wetenschappelijk en economisch potentieel (WEP) – bescherming – relaties tussen de Veiligheid van de Staat, deonderzoekscentra en de privésector' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2184)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'jihadistische vrouwen – risico's voor onze samenleving – terugkeer naar ons land' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2185)

Schriftelijke vraag van L. Bajart aan de minister van Buitenlandse Zaken over de 'Veiligheid van de Staat (VSSE) – Algemene Dienst Inlichting en Veiligheid (ADIV) – Social Media Intelligence (SOCMINT) – personeelsleden – aanwerving – personeel met (Arabische) talenkennis en kennis van allochtone milieus' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6- 2189)

Schriftelijke vraag van L. Bajart aan de minister van Justitie over de 'salafisten – geweldsdreiging – Nederland – salafisering van noodlijdende moskeeën – antidemocratische activiteiten – propaganda – financiële ondersteuning door buitenlandselanden – aanpak in België' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6-2222)

Schriftelijke vraag van L. Bajart aan de minister van Binnenlandse Zaken over de 'dreigingsniveau – verandering van het dreigingsbeeld van het terrorisme – jihadistische beweging – verspreiding van de jihadistische boodschap – wraak narratief – maatregelen' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6-2223)

Schriftelijke vraag van L. Bajart aan de minister van Justitie over de 'dreigingsniveau – verandering van het dreigingsbeeld van het terrorisme – jihadistische beweging – verspreiding van de jihadistische boodschap – wraaknarratief – maatregelen' (Senaat 2018-19, 15 januari 2019, Vr. nr. 6-2224)

Schriftelijke vraag van P. Van Rompuy aan de minister van Binnenlandse Zaken over de 'uitgeweken en teruggekeerde Syriëstrijders – onderzoeken – bevolkingsregister – schrapping' (Senaat 2018-19, 24 januari 2019, Vr. nr. 6-2272)

Schriftelijke vraag van G. D'haeseleer aan de minister van Binnenlandse Zaken over de 'veiligheidsdiensten – zelfmoorden – aantal' (Senaat 2018-19, 29 januari 2019, Vr. nr. 6-2314)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over de 'radicalisering – strijd – moskeeën – erkenning – ondersteuning procedure – vereenvoudiging – maatregelen – samenwerking tussen de federale overheid en de gemeenschappen en gewesten' (Senaat 2019-20, 19 september 2019, Vr. nr. 7-51)

Schriftelijke vraag van C. Van Cauter aan de minister van Binnenlandse Zaken over de 'extreemrechts en extreemlinks – geweldsdreiging – toename – indicatoren – aantal daden van geweld – handhaving – deradicalisering' (Senaat 2019-20, 19 september 2019, Vr. nr. 7-64)

Schriftelijke vraag van W.-F. Schiltz aan de minister van Telecommunicatie over de 'fake news – deepfake – politieke beïnvloeding – Veiligheid van de Staat – social media' (Senaat 2019-20, 14 oktober 2019, Vr. nr. 7-83)

Schriftelijke vraag van R. Daems aan de minister van Binnenlandse Zaken over de 'inlichtingendiensten – gevolgen van de Brexit – veiligheid terrorisme – Europees aanhoudingsmandaat' (Senaat 2019-20, 14 oktober 2019, Vr. nr. 7-91)

Schriftelijke vraag van G. D'haeseleer aan de minister van Binnenlandse Zaken over de 'islamitische Staat (IS) – IS-strijders – repatriëring van kinderen – opvolging' (Senaat 2019-20, 15 oktober 2019, Vr. nr. 7-99)

Schriftelijke vraag van G. Van Goidsenhoven aan de minister van Binnenlandse Zaken over de 'lokale integrale veiligheidscel (LIVC R) – oprichting – evolutie activiteiten – opdrachten – werking' (Senaat 2019-20, 25 november 2019, Vr. nr. 7-160)

Schriftelijke vraag van P. Van Rompuy aan de minister van Telecommunicatie over de 'toekomstig 5G-netwerk – uitrol – cyberveiligheid – potentiële bedreiging van Huawei' (Senaat 2019-20, 17 december 2019, Vr. nr. 7-246)

Kamer van Volksvertegenwoordigers

Samengevoegde vragen van A. Carcaci en F. Dewinter aan de minister van Binnenlandse Zaken over 'de antisemitische uitlatingen van de voorzitter van de Ligue des imams de Belgique' (*Hand.* Kamer 2018-19, 10 januari 2019, CRIV54PLEN265, 43, Vr. nrs. 3326 en 3328)

Vraag van B. Lutgen aan de minister van Binnenlandse Zaken over de 'detachering van het federale politiepersoneel naar de lokale politie' (*Vr. en Ant.* Kamer 2018-19, 4 februari 2019, QRVA 179, 38, Vr. nr. 3385)

Vraag van P. Buysrogge aan de minister van Binnenlandse Zaken over 'de investeringen in de infrastructuur van de VSSE' (*Vr. en Ant.* Kamer 2018-19, 4 februari 2019, QRVA 179, 55, Vr. nr. 3796)

Vraag van S. Van Hecke aan de minister van Justitie over 'de uitspraken van minister Schauvliege over de Staatsveiligheid' (*Hand.* Kamer 2018-19, 6 februari 2019, CRIV54COM1028, 4, Vr. nr. 28659)

Samengevoegde vragen van S. Van Hecke en G. Dallemagne aan de minister van Justitie over 'de uitspraken van minister Schauvliege over de Staatsveiligheid' (*Hand.* Kamer 2018-19, 6 februari 2019, CRIV54COM1028, 6, Vr. nrs. 28526 tot 28529 en 28658)

Vraag van K. Metsu aan de minister van Justitie over 'de Syriëstrijders' (*Hand.* Kamer 2018-19, 20 februari 2019, CRIV54COM1042, 1, Vr. nr. 28862)

Samengevoegde vragen en actualiteitsdebat van R. Hedebouw, M. Van Hees, V. Waterschoot, W. De Vriendt, S. Smeyers, M. De Coninck, G. Dallemagne en J. Fernandez aan de eerste minister over 'de problematiek van de uitreiking van humanitaire visa' (*Hand.* Kamer 2018-19, 20 februari 2019, CRIV54COM1043, 12, Vr. nrs. 28366 tot 28369, 28394, 28466, 28572, 28851, 28858 en 28864)

Vraag van S. Smeyers aan de minister van Sociale Zaken over 'de nakende verplichte vrijlating van een geradicaliseerde Marokkaanse onderdaan' (Hand. Kamer 2018-19, 20 februari 2019, CRIV54COM1043, 51, Vr. nr. 28522)

Samengevoegde vragen van F. Dewinter, Ph. Pivin, H. Vuye, C. Van Cauter, H. Bonte en N. Ben Hamou aan de eerste minister over 'de mogelijke terugkeer van Belgische IS-strijders' (*Hand.* Kamer 2018-19, 21 februari 2019, CRIV54PLEN271, 3, Vr. nrs. 3437 tot 344)

Vraag van V. Waterschoot aan de minister van Justitie over 'het VN-onderzoek naar de dood van Dag Hammarskjöld en de archieven van de Veiligheid van de Staat' (*Hand.* Kamer 2018-19, 27 februari 2019, CRIV54COM1046, 12, Vr. nr. 28909)

Vraag van R. Deseyn aan de minister van Financiën over 'de douane in het kader van de Brexit' (*Vr. en Ant.* Kamer 2018-19, 28 februari 2019, QRVA 181, 76, Vr. nr. 2508)

Vraag van C. Cassart-Mailleux aan de minister van Buitenlandse Zaken over de 'ontploffing van een F-16 in Florennes' (*Vr. en Ant.* Kamer 2018-19, 28 februari 2019, QRVA 181, 105, Vr. nr. 1656)

Vraag van J.-J. Flahaux aan de minister van Binnenlandse Zaken over de 'aantal door de politie afgevuurde schoten' (*Vr. en Ant.* Kamer 2018-19, 28 februari 2019, QRVA 181, 152, Vr. nr. 3810)

Samengevoegde vragen van B. Pas, K. Metsu en J.-J. Flahaux aan de eerste minister over 'de beveiliging van Brussels Airport' (*Hand.* Kamer 2018-19, 28 februari 2019, CRIV54PLEN272, 34, Vr. nrs. 3474 tot 3476)

Samengevoegde vragen van W. De Vriendt en P. Buysrogge aan de minister van Buitenlandse Zaken over 'de malaise bij de militaire inlichtingendienst' (*Hand.* Kamer 2018-19, 13 maart 2019, CRIV54COM1053, 4, Vr. nrs. 28883 en 29085)

Vraag van A. Top aan de minister van Buitenlandse Zaken over 'de werking van de ADIV' (*Hand.* Kamer 2018-19, 13 maart 2019, CRIV54COM1053, 20, Vr. nr. 29078)

Vraag van K. Degroote aan de minister van Justitie over 'de werking van de Spaanse inlichtingendiensten op ons grondgebied' (*Hand.* Kamer 2018-19, 13 maart 2019, CRIV54COM1055, 11, Vr. nr. 29083)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'databank inzake terrorisme en extremisme' (*Vr. en Ant.* Kamer 2018-19, 13 maart 2019, QRVA 182, 224, Vr. nr. 3792)

Samengevoegde vragen van J. Fernandez Fernandez en M. De Coninck aan de minister van Sociale Zaken over 'de humanitaire visa' (*Hand.* Kamer 2018-19, 20 maart 2019, CRIV54COM1062, 33, Vr. nrs. 29124 en 29145)

Vraag van J. Fernandez Fernandez aan de minister van Buitenlandse Zaken over de 'situatie van het ISTAR-bataljon' (*Vr. en Ant.* Kamer 2018-19, 21 maart 2019, QRVA 183, 160, Vr. nr. 1623)

Vraag van G. Dallemagne aan de minister van Justitie over de 'maatregelen voor de surveillance van de heer Jean-Louis Denis' (*Vr. en Ant.* Kamer 2018-19, 21 maart 2019, QRVA 183, 248, Vr. nr. 2977)

Vraag van K. Degroote aan de minister van Justitie over de 'gebruik van schietstanden door criminelen volgens de Federale Wapendienst van de FOD Justitie' (*Vr. en Ant.* Kamer 2018-19, 21 maart 2019, QRVA 183, 252, Vr. nr. 3012)

Vraag van C. Van Cauter aan de minister van Justitie over 'het monitoren en analyseren van extremistische boodschappen op digitale platformen' (*Vr. en Ant.* Kamer 2018-19, 21 maart 2019, QRVA 183, 260, Vr. nr. 3066)

Vraag van S. Van Hecke aan de minister van Mobiliteit over de 'luchthavenbeveiliging verder in handen van de private luchthavenuitbater' (*Vr. en Ant.* Kamer 2018-19, 21 maart 2019, QRVA 183, 337, Vr. nr. 3546)

Samengevoegde vragen van A. Laaouej en H. Bonte aan de minister van Binnenlandse Zaken over 'het dreigingsniveau na de aanslag in Nieuw-Zeeland' (*Hand.* Kamer 2018-19, 21 mars 2019, CRIV54PLEN276, 21, Vr. nrs. 3506 en 3507)

Samengevoegde vragen van S. Van Hecke, S. Becq en V. Van Peel aan de minister van Justitie over 'het seksueel misbruik bij de getuigen van Jehova' (*Hand.* Kamer 2018-19, 28 mars 2019, CRIV54PLEN277, 33, Vr. nrs. 3530 tot 3532)

Vraag van H. Bonte aan de minister van Justitie over 'het lot van de IS-kinderen in Syrië' (*Hand.* Kamer 2018-19, 28 mars 2019, CRIV54PLEN277, 42, Vr. nr. 3534)

Vraag van S. Schlitz aan de minister van Binnenlandse Zaken over de 'veiligheid van het in Tihange opgeslagen kernafval' (*Vr. en Ant.* Kamer 2018-19, 4 april 2019, QRVA 184, 327, Vr. nr. 3904)

Vraag van S. Van Hecke aan de minister van Financiën over de 'isopropanol-case Belgische douane (' (*Vr. en Ant.* Kamer 2018-19, 4 april 2019, QRVA 184, 199, Vr. nr. 2556)

Vraag van G. Calomne aan de minister van Justitie over de 'personen zonder verblijfplaats in België – verwerking van de aanvragen voor het dragen van een vuurwapen' (*Vr. en Ant.* Kamer 2018-19, 4 april 2019, QRVA 184, 337, Vr. nr. 2142)

Vraag van K. Jadin aan de minister van Justitie over 'In België in beslag genomen wapens' (*Vr. en Ant.* Kamer 2018-19, 4 april 2019, QRVA 184, 343, Vr. nr. 2517)

Vraag van F. Dewinter aan de minister van Justitie over 'de financiering van moskeeën en islamitische organisaties vanuit het buitenland' (*Vr. en Ant.* Kamer 2018-19, 4 april 2019, QRVA 184, 356, Vr. nr. 2909)

Vraag van B. Pas aan de minister van Justitie over de 'databank inzake terrorisme en extremisme' (*Vr. en Ant.* Kamer 2018-19, 4 april 2019, QRVA 184, 368, Vr. nr. 3009)

Vraag van E. Kir aan de minister van Binnenlandse Zaken over de 'aanslag in Nieuw-Zeeland – haatberichten op internet' (*Vr. en Ant.* Kamer 2018-19, 15 mei 2019, QRVA 186, 236, Vr. nr. 3951)

Vraag van B. Pas aan de minister van Justitie over de 'erkenning moskeeën' (*Vr. en Ant.* Kamer 2018-19, 22 mei 2019, QRVA 187, 127, Vr. nr. 2992)

Vraag van P. Buysrogge aan de minister van Justitie over 'de investeringen in de infrastructuur van de VSSE' (*Vr. en Ant.* Kamer 2018-19, 22 mei 2019, QRVA 187, 131, Vr. nr. 3044)

Vraag van K. Ravyts aan de minister van Buitenlandse Zaken over 'Dag Hammarskjöld – Belgische inbreng in VN-onderzoek' (*Vr. en Ant.* Kamer 2019-20, 9 september 2019, QRVA 001, 36, Vr. nr. 2)

Vraag van S. Rohonyi aan de VEM Justitie over 'de evaluatie van de bijzondere deradicaliseringsafdelingen (Deradex) in de gevangenissen' (*Hand.* Kamer 2019-20,
18 september 2019, CRIV55COM12, 3, Vr. nr. 174)

Samengevoegde vragen van J. Crombez, K. Bury, K. Van Vaerenbergh en N. Boukili aan de VEM Justitie over 'de organisatie van het proces over de aanslagen in Brussel' (*Hand.* Kamer 2019-20, 18 september 2019, CRIV55COM12, 29, Vr. nrs. 410, 433, 438 en 496)

Vraag van S. Van Hecke aan de VEM Justitie over 'de intrekking van de erkenning van de moskee Al Ihsaan in Leuven' (*Hand.* Kamer 2019-20, 18 september 2019, CRIV55COM12, 41, Vr. nrs. 480)

Vraag van N. Boukili aan de VEM Justitie over 'de timing van de seponering van een klacht tegen een minister' (*Hand.* Kamer 2019-20, 2 oktober 2019, CRIV55COM20, 4, Vr. nr. 700)

Vraag van T. Francken aan de minister van Buitenlandse Zaken over 'het omgekeerde interview' (*Vr. en Ant.* Kamer 2019-20, 2 oktober 2019, QRVA 003, 48, Vr. nr. 32)

Vraag van F. Demon aan de minister van Buitenlandse Zaken over de 'controles op private bewakingsfirma's in luchthavens' (*Vr. en Ant.* Kamer 2019-20, 2 oktober 2019, QRVA 003, 63, Vr. nr. 20)

Vraag van D. Senesael aan de minister van Binnenlandse Zaken over 'de aan extreemrechts toegeschreven misdaden en misdrijven' (*Hand.* Kamer 2019-20, 9 oktober 2019, CRIV55COM24, 24, Vr. nr. 323)

Vraag van G. Colebunders aan de minister van Binnenlandse Zaken over 'het etnisch profileren bij de politie' (*Hand.* Kamer 2019-20, 9 oktober 2019, CRIV55COM24, 50, Vr. nr. 844)

Samengevoegde vragen van C. Thibaut en S. Cogolati aan de minister van Binnenlandse Zaken over 'de ambassade van Rwanda en de veiligheid op het Belgische grondgebied' (*Vr. en Ant.* Kamer 2019-20, 16 oktober 2019, CRIV55COM34, 3, Vr. nrs. 746, 774 en 775)

Vraag van K. Jadin aan de minister van Justitie over de 'wetgevende instrumenten ter bestrijding van spionage' (*Vr. en Ant.* Kamer 2019-20, 25 oktober 2019, QRVA 004, 41, Vr. nr. 10)

Vraag van G. Dallemagne aan de minister van de Binnenlandse Zaken over de 'Bloedbad in het gebouw van de politieprefectuur van Parijs' (*Vr. en Ant.* Kamer 2019-20, 25 oktober 2019, QRVA 004, 179, Vr. nr. 200)

Samengevoegde vragen van T. Francken en K. Verduyckt aan de minister van Buitenlandse Zaken over 'de bewaking van het kamp van Al-Hawl' (*Hand.* Kamer 2019-20, 6 november 2019, CRIV55COM46, 24, Vr. nrs. 381 tot 383 en 1365)

Samengevoegde vragen van E. Samyn, W. De Vriendt, Y. Kherbache, K. Jadin, Ch. Lacroix, G. Dallemagne, N. Boukili, J. Soors en P. De Roover aan de minister van Buitenlandse Zaken over de 'nieuwe ontwikkelingen i.v.m. IS-strijders na de Europese Raad BUZA van 14/10/19' (*Hand.* Kamer 2019-20, 12 november 2019, CRIV55COM49, 3, Vr. nrs. 933, 973, 976, 1048, 1129, 1148, 1370, 1470,1490, 1501 en 1527)

Vraag van K. Bury aan de minister van Justitie over de 'activiteiten extremistische moslim-vzw' (*Vr. en Ant.* Kamer 2019-20, 12 november 2019, QRVA 005, 47, Vr. nr. 45)

Vraag van J. Soors aan de minister van Justitie over de 'screening geloofsgemeenschappen door Vlaanderen' (*Vr. en Ant.* Kamer 2019-20, 12 november 2019, QRVA 005, 67, Vr. nr. 99)

Vraag van M. Dillen aan de minister van Justitie over de 'samenwerking tussen openbaar ministerie en fiscale overheden' (*Vr. en Ant.* Kamer 2019-20, 12 november 2019, QRVA 005, 86, Vr. nr. 81)

Vraag van W. Vermeersch aan de minister van Binnenlandse Zaken over de 'West-Vlaamse politiereis naar China' (*Vr. en Ant.* Kamer 2019-20, 12 november 2019, QRVA 005, 156, Vr. nr. 249)

Vraag van L. Dierick aan de minister van Telecommunicatie over de 'Veiligheid 5G' (*Vr. en Ant.* Kamer 2019-20, 12 november 2019, QRVA 005, 249, Vr. nr. 29)

Vraag van Ph. Goffin aan de minister van Justitie over de 'beul van Raqqa' (*Vr. en Ant.* Kamer 2019-20, 29 november 2019, QRVA 006, 73, Vr. nr. 43)

Vraag van K. Bury aan de minister van Justitie over de 'radicaalislamitische imams, moskeeën en verenigingen' (*Vr. en Ant.* Kamer 2019-20, 29 november 2019, QRVA 006, 86, Vr. nr. 77)

Vraag van Ch. Lacroix aan de minister van Buitenlandse Zaken over de 'hybride dreigingen' (*Vr. en Ant.* Kamer 2019-20, 29 november 2019, QRVA 006, 143, Vr. nr. 88)

Vraag van S. Cogolati aan de minister van Buitenlandse Zaken over de 'Chinese inlichtingendiensten in België' (*Hand.* Kamer 2019-20, 4 december 2019, CRIV55COM64, 7, Vr. nr. 1441)

Samengevoegde vragen van W. De Vriendt en S. Cogolati aan de VEM Justitie over 'samenwerking tussen de Belgische en de Rwandese inlichtingendiensten' (*Hand.* Kamer 2019-20, 4 december 2019, CRIV55COM64, 35, Vr. nrs. 1762 en 1868)

Vraag van J. Soors aan de minister van Binnenlandse Zaken over de 'rechts-extremistische organisaties en geweld in België' (*Hand.* Kamer 2019-20, 4 december 2019, CRIV-55COM65, 49, Vr. nr. 1795)

Samengevoegde vragen van C. Thibaut en J. Arens aan de Minister van Binnenlandse Zaken) over 'de indrukwekkende politiemacht die werd ingezet voor een betoging in Aarlen' (*Hand.* Kamer 2019-20, 4 december 2019, CRIV55COM65, 56, Vr. nrs. 1878 en 1937)

Vraag van de Ph. Pivin aan de VEM Justitie over 'de uitbreiding van de databank met informatie over de Foreign Terrorist Fighters' (*Hand.* Kamer 2019-20, 12 december 2019 CRIV55PLEN017, 28, Vr. nr. 286)

Vraag van S. Creyelman aan de minister van Buitenlandse Zaken over de 'cyberveiligheid' (*Vr. en Ant*. Kamer 2019-20, 17 december 2019, QRVA 007, 240, Vr. nr. 132)

Samengevoegde vragen van K. Verduyckt, H. Bayet en Ch. Lacroix aan de minister van Buitenlandse Zaken over 'de reorganisatie binnen de ADIV' (*Hand.* Kamer 2019-20, 18 december 2019, CRIV55COM78, 17, Vr. nrs. 1295, 1399 en 1323)

Vraag van de K. Aouasti aan Minister van Werk over 'de discriminatie bij de aanwervingen op Brussels Airport' (*Hand.* Kamer 2019-20, 19 december 2019, CRIV55PLEN018, 11, Vr. nr. 317)

BIJLAGE D.
CHARTER OF THE INTELLIGENCE OVERSIGHT WORKING GROUP

1. **Members of the European Intelligence Oversight Group**
   This Charter establishes the Intelligence Oversight Working Group, an informal cooperation between the following oversight bodies:
   - Belgian Standing Intelligence Agencies Review Committee,
     Comité permanent de contrôle des services de renseignement et de sécurité /Vast Comité van Toezichtop de inlichtingen- en veiligheidsdiensten (Belgium);
   - Danish Intelligence Oversight Board,
     Tilsynet med Efterretningstjenesterne (Denmark);
   - Review Committee on the Intelligence and Security Services,
     Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (The Netherlands);
   - EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee, *EOS-utvalget* (Norway);
   - Independent Oversight Authority for Intelligence Activities (OA-IA),
     Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND (Switzerland);
   - Investigatory Powers Commissioner's Office, (United Kingdom).

2. Purposes of the Intelligence Oversight Working Group

The Intelligence Oversight Working Group aims to:

- strengthen cooperation between the participating oversight bodies;
- increase transparency between oversight bodies within the limits and according to the standards set by national legislators, in order to support effective oversight of international cooperation between intelligence and security services;
- exchange knowledge, experiences and best practices of oversight;
- provide a platform for developing new and/or more effective oversight methods;
- maintain contact, share information and provide each other with mutual assistance as appropriate, in accordance with the boundaries set by national laws and regulations.

3. Meetings

a) Chair meetings

The Intelligence Oversight Working Group shall annually hold at least one meeting between the chairs of the oversight bodies, or a member of the oversight body representing the chair. In principle, each chair will be supported by their head of secretariat and/or another senior staff member.

b) Staff meetings

The intelligence Oversight Working Group shall regularly, when appropriate, hold staff meetings. The staff meetings are aimed at practically substantiating the purposes referred to in Section 2 of this Charter and carrying out the cooperation projects referred to in Section 4 of this Charter.

c) Preparation of meetings

Chair meetings shall be prepared by the oversight body hosting the meeting in cooperation with the informal secretariat referred to in Section 5 of this Charter. Staff meetings shall be prepared by the oversight body hosting the meeting. All Members voluntarily contribute to hosting meetings on a rotation basis.

4. Cooperation projects

The Intelligence Oversight Working Group may decide to enter into cooperation projects. Cooperation projects relate to a specific interest of the Group. The decision to enter into a cooperation project will be taken during a Chair meeting on the basis of a project proposal. Project proposals are prepared at staff level and shall include at a minimum:

- the intended goals for the project;
- the proposed methods to reach those goals;
- the timeframe in which the project is to be carried out.

5. Informal secretariat

The informal secretariat will be responsible for:

- reporting conclusions of the chair meetings;
- reporting conclusions of the staff meetings in cooperation with the oversight body that organised the respective meeting;
- monitoring progress on the cooperation projects;
- communication with regard to outside interest in the Group. The secretariat will rotate every two years.

6. **Information exchange**
   The participating oversight bodies commit to facilitating information sharing within the Group to further the purposes referred to in Section 2 of this Charter, where appropriate and in accordance with the boundaries set by national laws and regulations. The nature and extent of information sharing within the Group may also be defined by or dependent upon bilateral and/or multilateral agreements between the intelligence and security services overseen by the participating oversight bodies.

7. **Membership**
   Extending membership of the Intelligence Oversight Working Group to other European oversight bodies on their request, shall take place on the basis of a decision by consensus taken during a Chair meeting.

8. **Status, Implementation and Amendment of the Charter**
   This Charter reflects the intent of the participating oversight bodies within the Intelligence Oversight Working Group. Each participating oversight body commits to implementing this Charter. Amendment of this Charter shall take place on the basis of a decision by consensus taken during a Chair meeting. This Charter is not legally binding.

Signed in The Hague on 12 December 2019,

Mr. Serge Lipszyc, Chair of the Belgian Standing Intelligence Agencies Review Committee

Mr. Michael Kistrup, Chair of the Danish Intelligence Oversight Board

Mr. Nico van Eijk, Chair of the Dutch Review Committee on the Intelligence and Security Services

Mr. Svein Grønnern, Chair of the EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee

Mr. Thomas Fritschi, Director of the Swiss Independent Oversight Authority for Intelligence Activities

Sir Brian Leveson, Investigatory Powers Commissioner, United Kingdom