ACTIVITEITENVERSLAG 2018
RAPPORT D'ACTIVITÉS 2018

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.

ACTIVITEITENVERSLAG 2018

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de
inlichtingen- en veiligheidsdiensten

intersentia
Antwerpen – Cambridge

Voorliggend *Activiteitenverslag 2018* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 28 augustus 2019.

(*getekend*)
Serge Lipszyc, voorzitter
Pieter-Alexander De Brock, raadsheer
Laurent Van Doren, raadsheer
Wouter De Ridder, griffier

Activiteitenverslag 2018
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

ISBN 978-94-000-1107-6
D/2019/7849/144
NUR 823

INHOUD

LIJST MET AFKORTINGEN

ADIV	Algemene Dienst Inlichting en Veiligheid
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*
BS	Belgisch Staatsblad
BTA	Bevoegde toezichthoudende autoriteit
CHOD	*Chief of Defence*
CHODOPORDER	Operationeel Order van de Chef Defensie
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
CT	*Counterterrorism*
CTIVD	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten
C-OPS	Operatie Center
DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
DGA/DAO	Directie van de bestuurlijke politie
DG EPI	Directoraat-generaal Penitentiaire Inrichtingen
DGJ/DJO	Directie van de gerechtelijke politie
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
FOD	Federale overheidsdienst

FragO	*Fragmentary Orders*
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 persoonsgegevens (Gegevensbeschermingswet)
GGB	Gemeenschappelijke gegevensbank
HTF	*Homegrown terrorist fighters*
Hand.	Handelingen
HP	Haatpropagandisten
HUMINT	*Human intelligence*
ICP	*Information collection plan*
ICT	Informatie- en communicatietechnologie
IMINT	*Image intelligence*
IPCO	*Investigatory Powers Commissioner's Office*
IR	*Intelligence requirements*
IS	Islamitische Staat
ISTAR	*Intelligence, surveillance, target acquisition and reconnaissance*
JIB	*Joint information box*
K.B.	Koninklijk besluit
KB C&VM	Koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
KB FTF	Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de Wet op het politieambt
KB 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 van10 juli 2006 betreffende de analyse van de dreiging
KPI	*Key performance indicator*
LIVC-R	Lokale Integrale Veiligheidscel inzake radicalisme, extremisme en terrorisme
LTF	*Local task force*
M.B.	Ministerieel besluit
MoU	*Memorandum of Understanding*
NA	*Note aux autorités*
NAVO	Noord-Atlantische Verdragsorganisatie
NBB	Nationale Bank van België
NTF	Nationale Task Force
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OpSec	*Operations Security*
OSINT	*Open sources intelligence*
Parl. St.	Parlementaire Stukken van Kamer en Senaat
PDR	*Plan Directeur du Renseignement* (Inlichtingenstuurplan)
PNR-Wet	Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens
POC	*Point of contact*
RIR	Informatierapport
SIGINT	*Signals intelligence*
SLA	*Service Level Agreements*
SOP	*Standard Operating Procedures*
Sv.	Wetboek van Strafvordering
Sw.	Strafwetboek
TESSOC	*Terrorisme, Espionage, Sabotage, Subversion and Organised Crime*
TF	*Terrorist fighters*
Vast Comité I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten
VN	Verenigde Naties
Vr. en Antw.	Schriftelijke vragen en antwoorden (Kamer of Senaat)
VSSE	Veiligheid van de Staat
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen

W.C&VM	Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen
W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
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

'Un secret a toujours la forme d'une oreille'
Jean Cocteau (Le Rappel à l'ordre)

Van de strijd tegen het terrorisme tot de verdediging van onze strategische belangen inzake telecommunicatie; van Edward Snowden tot de aanwezigheid van spionnen in België; van de erkenning van geloofsgemeenschappen tot de toekenning van veiligheidsmachtigingen … Al deze elementen wijzen op de grote maatschappelijke noodzaak aan performante inlichtingendiensten.

De Staat dient in deze de veiligheid te garanderen, maar tegelijkertijd ook de uitoefening van de fundamentele rechten en de individuele vrijheden te vrijwaren. Deze evenwichtsoefening moet gebeuren via een afgemeten tussenkomst van de inlichtingendiensten, die een van de hoekstenen vormt binnen het veiligheidsarsenaal.

In dit verband bestaat de taak van het Vast Comité I er niet alleen in om zijn eigen opdrachten uit te voeren, maar ook om toe te zien op de gecontroleerde ontwikkeling van de Veiligheid van de Staat, van de Algemene Dienst Inlichting en Veiligheid en – in samenwerking met het Vast Comité P – van het Coördinatieorgaan voor de dreigingsanalyse.

Het Comité wil op diverse gebieden actief zijn. Het moet vooreerst – zoals het de afgelopen 25 jaar heeft gedaan – aanbevelingen formuleren die zowel bestemd zijn voor de verantwoordelijken, voor de bevoegde ministers als voor het Parlement. Deze aanbevelingen zijn gericht op een versterking van de werking van de democratische Staat.

Het Vast Comité I draagt ook bij tot de evolutie van de wetgeving. Omwille van zijn expertise en zijn onafhankelijkheid tegenover de instellingen moet het een bron van reflectie vormen voor de uitdagingen van morgen en voor de toekomstige architectuur van de inlichtingengemeenschap.

Maar het Comité moet ook ten dienste staan van de burger; zowel zij die een klacht indienen omdat zij van oordeel zijn dat de Staat op onwettige wijze informatie over hen heeft ingewonnen of verwerkt, als zij die zich tot het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en –adviezen wenden.

Het Vast Comité I wil in herinnering brengen dat honderden mannen en vrouwen dagelijks bijdragen tot de veiligheid van de Staat en dat de toezichtonderzoeken die in 2018 uitgevoerd werden binnen hun respectieve diensten, getuigen van het engagement en de wil om competent, loyaal en integer te zijn.

Het Comité is als toezichthouder samen met zijn homologen actief zowel op nationaal als op internationaal vlak, en dit om beter de realiteit en de uitdagingen te vatten met betrekking tot het respect voor persoonsgegevens. In die context moet vastgesteld worden dat zowel publieke als private organisaties inlichtingen inwinnen en onderworpen zijn aan dwingende bepalingen inzake de beveiliging van informatie. Vandaar dat het Comité zich de vraag stelt of zijn rol niet moet geherdefinieerd worden.

Precies een jaar legde ik de eed af in de handen van de Voorzitter van de Kamer van Volksvertegenwoordigers in aanwezigheid van mijn voorganger Guy Rapaille. Het Comité wil het belang van het werk van zijn erevoorzitter onderlijnen; het vormt de basis waarop wij vandaag kunnen verder werken.

Samen met de Raadsheren van het Comité, de Griffier en alle medewerkers wens ik op mijn beurt de weg te openen en de lijnen uit te zetten voor het Belgische toezichtorgaan op de inlichtingendiensten. Met deze ploeg wens ik vandaag op continue basis te werken aan de omschrijving van nieuwe doelstellingen, aan de realisatie van onze opdrachten en aan het toezicht op het respect voor onze democratische waarden.

Serge Lipszyc,
Voorzitter van het Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

28 augustus 2019

HOOFDSTUK I
DE TOEZICHTONDERZOEKEN

In 2018 finaliseerde het Vast Comité I vijf toezichtonderzoeken (I.1 tot I.5). Verder opende het Comité in dat jaar drie nieuwe onderzoeken. Twee van de afgesloten onderzoeken werden ambtshalve opgestart, in één onderzoek werd het Vast Comité I gevat door de minister van Defensie (art. 32 W.Toezicht)[1] en twee onderzoeken – waarvan één samen met het Vast Comité P – werden uitgevoerd op verzoek van de parlementaire Begeleidingscommissie. Een korte omschrijving van de in 2018 nog lopende en/of opgestarte onderzoeken, volgt in I.6. De naar aanleiding van de toezichtonderzoeken geformuleerde aanbevelingen werden gebundeld in Hoofdstuk XII.

In totaal ontving het Comité in 2018 72 klachten of aangiften. Sinds 2016 werd een aanvang genomen met een versoepeling, deformalisering en standaardisering van het werkproces 'klachten en aangiften'.[2] Desgevallend na een kort vooronderzoek en de verificatie van een aantal objectieve gegevens, wees het Comité 68 klachten of aangiften af omdat ze kennelijk niet gegrond waren (art. 34 W.Toezicht) of omdat het Comité onbevoegd was om de opgeworpen vraag te behandelen. In die laatste gevallen werden de klagers zo mogelijk doorverwezen naar de bevoegde instanties (Vast Comité P, Federale Politie, procureur des Konings of andere instanties). Eén klacht leidde tot de opening van een toezichtonderzoek (I.5), twee klachten werden toegevoegd aan een bestaand lopend onderzoek (I.1) en de klacht die betrekking had op de werking van het OCAD werd omwille van de gemeenschappelijke bevoegdheid eind 2018 aangemeld aan het Vast Comité P voor een gezamenlijke behandeling.

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.[3] Indien

---

1 Het feit dat het Comité gevat wordt door een lid van de uitvoerende macht, is eerder uitzonderlijk. Hierover: VAN LAETHEM, W. en VANDERBORGHT, J., 'Torture numbers, and they'll confess to anything. Een analyse van twintig jaar toezichtonderzoeken, studies en adviezen' in VAN LAETHEM, W. en VANDERBORGHT, J. (eds.), *Inzicht in toezicht*, Antwerpen, Intersentia, 2013, 266.

2 In eerste instantie wordt de ontvankelijkheid bestudeerd en vervolgens 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 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

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 2017 werd onder meer een informatiedossier geopend over de ontplooiing van een inlichtingencapaciteit van ADIV in een conflictzone, wat leidde tot de opstart van een toezichtonderzoek in 2018 (I.3).

Ten slotte worden ook zeer regelmatig briefings georganiseerd waarbij leden van de inlichtingendiensten het Comité voorlichten over actuele en belangrijke thema's binnen de *intelligence community* (bijv. over de *Belgian Passenger Information Unit* (BELPIU), de inzet van bijzondere inlichtingenmethoden …). Deze briefings moeten een geïnformeerde discussie over de werking, de bevoegdheden en de controle op de inlichtingen- en veiligheidsdiensten en het OCAD alsook op het inlichtingenwerk bevorderen. Zij kunnen ook aanleiding geven tot het openen van een onderzoek.

I.1. DE WERKING VAN DE DIRECTIE COUNTERINTELLIGENCE (CI) VAN DE ADIV

I.1.1. 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 half december 2016 van het 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[4]; het werd afgerond in februari 2018. 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.

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 ….

4 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').

I.1.2. DE (WETTELIJKE) OPDRACHT VAN DE DIRECTIE CI

I.1.2.1. Ambities, missie en visie m.b.t. 'counterintelligence'

In een intern document uit 2012 werd de ambitie van wat toen nog de 'Divisie' CI heette, als volgt omschreven: '*Teneinde elke bedreiging te voorkomen moet de Div CI instaan voor de identificatie, de preventie en neutralisatie van al de activiteiten die kunnen ontplooid worden door buitenlandse inlichtingendiensten, door andere organisaties of door individuele personen in het kader van terrorisme, spionage, sabotage of subversie (TESS) en die de belangen van Defensie in de ruimste zin van het woord, hetzij haar personeel, haar infrastructuur, haar plannen en operaties worldwide; of deze van haar militaire partners in België zou kunnen bedreigen*'.

In hetzelfde document werd ook de visie weergegeven*: 'Be able to prevent all threats to all Defence related matters'. 'De Divisie CI moet in staat zijn elke realistische bedreiging waaraan de vitale belangen van Defensie kan aan blootgesteld worden, te voorkomen. De werking van de Div CI moet in alle DISCRETIE kunnen gebeuren. Dit betreft de kennis van de structuur, de modus operandi, het personeel en de middelen. Het uitvoeren van de operaties en van de opdrachten moet AFGESCHERMD gebeuren*'.

Deze ambitie en visie werden in het 'Veiligheidsinlichtingen Stuur- en Veiligheid Actieplan 2015-2018'[5] in strategische doelstellingen vertaald: '*Le Dept CI doit être en mesure de prévenir de manière réaliste chaque menace pouvant exposer des intérêts vitaux de la Défense, et ce, dans le cadre des missions et des moyens prévus par les textes légaux. En outre, le Dept CI doit être en mesure de pouvoir honorer les engagements et les accords en vigueur conclus avec des services homologues, et plus particulièrement dans le cadre d'une coopération avec les services de renseignement, avec les services de police et avec la Justice. Le Dept CI doit également être en mesure de porter assistance à ses partenaires militaires étrangers localisés sur le territoire belge dans le domaine de la contre-ingérence*'.[6] In datzelfde Stuur- en Veiligheid Actieplan 2015-2018 werden daarenboven vijf prioriteiten gedefinieerd.

Deze ambitie, missie en visie vloeien voort uit de NAVO-reglementering en zijn geënt op de Belgische wetgeving.

---

5 SGRS, Plan Directeur du renseignement de Sécurité et d'Actions Sécuritaires 2015-2018. Révision 2016 – Veiligheidsinlichtingen Stuur- en Veiligheid Actieplan 2015-2018. Herziening 2016, SECRET (Loi 11 décembre 1998), March 1, 2016, 11. Het betreft een 'herziening' van een eerder in 2016 opgesteld plan. Deze passage werd door de dienst gedeclassificeerd.

6 *'De CI-afdeling moet in staat zijn om in het kader van de opdrachten en middelen voorzien in wetsteksten, elke dreiging waaraan de vitale belangen van de Defensie kunnen worden blootgesteld, op een realistische wijze te voorkomen. Bovendien moet de CI-afdeling in staat zijn de bestaande verbintenissen en overeenkomsten met homologe diensten na te komen, met name in het kader van de samenwerking met de inlichtingendiensten, de politiediensten en de rechterlijke macht. De CI-afdeling moet ook in staat zijn om zijn buitenlandse militaire partners op Belgisch grondgebied bij te staan op het gebied van de contraspionage'*. (vrije vertaling).

I.1.2.2. De NAVO-reglementering

In 2014 definieerde de NAVO in een *standardization agreement* (STANAG) op eenduidige wijze de binnen het kader van haar werking gehanteerde begrippen.[7] Onder *counterintelligence* werd voortaan het volgende begrepen:

- *'Counter Intelligence (CI organizations, military or civilian, of the member nations including Law Enforcement Organizations) of the Alliance are responsbile for counteracting the threat to security posed by hostile intelligence services and subversive, criminal or terrorist groups or individuals'.*
- *Counter-intelligence includes those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organisations or by individuals engaged in espionage, sabotage, subversion or terrorism. […] (2) The main thrust of the CI effort is to protect personnel, information, plans and resources, both at home and when deployed. It aims to provide knowledge and understanding of the prevailing situation to keep privileged information secret, equipment secure and personnel safe. CI should be proactive and preventative in its approach. (3) CI is an intelligence function that provides commanders at all levels with a detailed understanding of threats, vulnerabilities and risks to enable them to make well-educated decisions on security measures. In reality, there are likely to be compromises between what is needed and what is feasible.*[8]

In datzelfde NAVO-document wordt teruggekomen op de specifieke rol van counterintelligence: '*to ensure succesful military operations the commandor should deny the adversary the opportunity to conduct terrorism, espionage, subversion, sabotage, organized crime or computer network attacks against friendly force. To achieve this requires identification of friendly force's vulnerability to an adversary's*

---

7 NATO Standardization Office (NSO), STANAG 2190. Allied Joint Doctrine for intelligence, counter-intelligence and security, Edition 2, September 2014 (NSO(JOINT)1165(2014) JINT/2190, 7-2.

8 *Counterintelligence (militaire of civiele CI-afdelingen van de lidstaten met inbegrip van rechthandhavingsorganisaties) van de Alliantie zijn verantwoordelijk voor het tegengaan van de bedreiging van de veiligheid die uitgaat van vijandige inlichtingendiensten en subversieve, criminele of terroristische groepen of individuen'.*
Onder contraspionage vallen activiteiten die betrekking hebben op het identificeren en bestrijden van de veiligheidsdreiging van vijandige inlichtingendiensten of -organisaties of van personen die betrokken zijn bij spionage, sabotage, subversie of terrorisme. […] (2) De belangrijkste doelstelling van de CI-inspanning is de bescherming van personeel, informatie, plannen en middelen, zowel in eigen land als wanneer elders ontplooid. Het doel ervan is kennis en begrip te verschaffen van de heersende situatie om bevoorrechte informatie geheim te houden, de uitrusting te beveiligen en het personeel veilig te houden. CI moet proactief en preventief zijn in zijn aanpak. (3) CI is een inlichtingenfunctie die bevelhebbers op alle niveaus een gedetailleerd inzicht verschaft in dreigingen, kwetsbaarheden en risico's om hen in staat te stellen goed onderbouwde beslissingen over veiligheidsmaatregelen te nemen. In werkelijkheid bestaat de kans dat er compromissen dienen te worden gesloten tussen wat nodig en wat haalbaar is'. (vrije vertaling).

intelligence gathering operations. This information is used to inform OPSEC, counter surveillance and deception planning including Protective Security Policy'.[9]

In nog twee andere documenten, respectievelijk uit 2001 en 2016[10], werd een omschrijving gegeven van de missie van CI-divisies in de schoot van de nationale, militaire inlichtingendiensten. Hun opdracht bestaat erin spionage, sabotage en de dreigingen van terrorisme en subversie tegen de NAVO en de coalitiepartners, te detecteren en te counteren. Voor sommige naties komt erbovenop nog de bescherming tegen dreigingen uitgaande van georganiseerde criminaliteit, fundamentalisme, extremisme en inlichtingenoperaties (van vreemde landen).

I.1.2.3. De Belgische wetgeving

In de Wet van 30 november 1998 wordt counterintelligence niet expliciet vermeld. Wel kunnen een aantal van de opdrachten uit artikel 11 W.I&V begrepen worden als opdrachten van counterintelligence-aard. Ook in het KB van 21 december 2001[11] dat de algemene structuur van het Ministerie van Defensie bepaalde en de bevoegdheden van bepaalde autoriteiten vastlegde, werd het begrip counterintelligence niet gedefinieerd en werd ook geen gewag gemaakt van een Directie Counterintelligence. Hetzelfde geldt voor het KB van 4 juli 2014 dat het statuut bepaalt van een deel van het burgerpersoneel van de ADIV.[12]

I.1.3. DE OPDRACHTEN VAN CI IN DE PRAKTIJK

I.1.3.1. CI in binnen- en buitenland

Oorspronkelijk concentreerde de Directie CI zich op het opsporen van activiteiten van militaire spionage – zowel door leden van het Belgisch leger zelf als door

---

9 '*Om een succesvolle militaire operatie te garanderen moet de bevelhebber de tegenpartij de mogelijkheid ontzeggen om terrorisme, spionage, subversie, sabotage, georganiseerde misdaad of computernetwerk aanvallen tegen bevriende strijdkrachten uit te voeren. Om dit te bereiken is het nodig de kwetsbaarheden van de bevriende strijdkrachten voor de inlichtingenvergaring van een tegenstander in kaart te brengen. Deze informatie wordt gebruikt om OPSEC, counter surveillance en planning van de misleiding, inclusief Protective security Policy, te informeren.* (vrije vertaling).

10 Het betreft de 'Allied Joint doctrine for Intelligence, Counterintelligence and Security (AJP 2(A) (februari 2016)' en de 'AJP 2.2 '(Restricted) Counter-intelligence and Security Procedures' (november 2001) van de NAVO.

11 KB 21 december 2001 tot bepaling van de algemene structuur van het ministerie van Landsverdediging en tot vastlegging van de bevoegdheden van bepaalde autoriteiten, *BS* 12 januari 2002. Dit KB werd vervangen bij KB van 2 december 2018. Ook in dit KB wordt het begrip counterintelligence niet gedefinieerd en is er geen sprake van een Directie Counterintelligence.

12 KB van 4 juli 2014 tot vaststelling van het statuut van bepaalde burgerlijke ambtenaren van het stafdepartement inlichting en veiligheid van de Krijgsmacht, *BS* 18 juli 2014.

buitenlandse diensten – en het tegengaan van subversie (ondermijning) in het binnenland. De invulling van het begrip counterintelligence werd door de jaren heen ruimer opgevat en omvat nu het zgn. 'TESSOC': 'Terrorisme, Espionage, Sabotage, Subversion, Organised Crime'. De Directie CI rekent het daarbij ook tot zijn taak om de TESSOC-fenomenen binnen de eigen dienst (ADIV) op te sporen. Dit is niet onlogisch aangezien een nationale militaire inlichtingendienst een belangrijke target kan zijn (voor infiltratie) van andere, buitenlandse inlichtingendiensten.

Door de toenemende inzet van Belgische troepen in het buitenland en in het kader van de NAVO-samenwerking kreeg de Directie vanaf 2012 ook een zogenaamde 'CI in OpsZone'-opdracht: het zenden van CI-personeel naar het buitenland in steun van de aldaar ontplooide Belgische troepen ten einde op te treden tegen de lokale, militaire spionage of tegen vormen van georganiseerde criminaliteit (prostitutie, drugs …) die tot infiltratie of subversie van individuele militairen kunnen leiden. Ook deze opdracht, die doorgaans aangeduid wordt met de term *force protection*, heeft een wettelijke basis in artikel 11 W.I&V.

I.1.3.2. Counterterrorisme en de bevoegdheid van de ADIV

Het Vast Comité I stelde reeds eerder dat de opgang van het (islamistisch) terrorisme de werking van de Belgische inlichtingendiensten, en *in casu* de ADIV en de Directie CI, sterk beïnvloedde. De veranderde kenmerken van het terrorisme (meer grensoverschrijdende *filières* en activiteiten …) hadden een vermenging van taken en verantwoordelijkheden tot gevolg, en dit zowel wat betreft de territorialiteit (binnenland *versus* buitenland) als de aspecten die moesten worden opgevolgd (burgerlijk *versus* militair). Het Vast Comité I pleitte in dat kader voor een grondige evaluatie van de manier waarop de militaire inlichtingendienst in het algemeen en de Directie CI in het bijzonder in een bepaalde richting werd gedirigeerd.[13]

Het feit dat terroristen met zware, militaire middelen gingen optreden[14], vanuit een militaire logica werden aangestuurd (cellen in Europa die door de militaire leiding van IS vanuit Syrië/Irak werden geleid) én vooral de aanslagen van maart 2016 in Brussel en Zaventem, versterkte deze evolutie (de vermenging van de taken) nog meer. Deze periode vormde voor de ADIV (en de Directie CI) een sleutelmoment. De eigen bevoegdheid, die tot dan toe 'militair' was, werd door de dienst gaandeweg breder – lees: 'civiel' – geïnterpreteerd.

In een periode waarin van elke dienst een maximale medewerking nodig was, werd door de leiding echter niet duidelijk onderzocht of de ADIV – en in het bij-

---

13 De ADIV dient zijn eigenheid ('militaire focus') te behouden. Hierover: VAST COMITÉ I, *Activiteitenverslag 2016*, 4 e.v. ('II.1. De problematiek van de *foreign terrorist fighters*').

14 Het feit dat de terroristen die zich in Europa bevonden, over 'militaire' wapens beschikten, vormde een extra aanknopingspunt voor de bevoegdheid van ADIV. Immers, art. 11 § 2, 1° W.I&V beperkt de bevoegdheid van de ADIV tot activiteiten die het nationaal grondgebied of de bevolking bedreigen en uitgevoerd zijn '*met middelen van militaire aard*'.

zonder de Directie CI – zich hiertoe daadwerkelijk geroepen voelde en, in voorkomend geval, ook een duidelijke meerwaarde kon bieden gegeven de middelen die ter beschikking stonden.

Deze situatie zorgde afgelopen jaren derhalve voor heel wat problemen: opslorping van middelen, versnippering van bevoegdheden binnen de dienst of het niet-opnemen van bepaalde taken of bevoegdheden, technische bijstand in gerechtelijke dossiers met een beperkte meerwaarde …

Bovendien hield de Directie CI zich bij zijn rolbeschrijving vast aan de NAVO-regels waarin de strijd tegen terrorisme zich focust op terrorisme tegen militaire doelen en dit in hoofdzaak in een internationale context (bijv. in buitenlandse operatiegebieden). Het terrorisme dat zich richt tegen voornamelijk burgerlijke doelen en dat historisch vooral binnenlands was (bijv. CCC en RAF), behoorde in die visie in principe niet tot de *scope* van de militaire instanties, maar wel tot deze van de burgerlijke inlichtingendienst (VSSE).

Het Comité was dan ook van oordeel dat de missie inzake contraterrorisme duidelijk moest worden uitgeklaard en dat de ADIV, en in het bijzonder de Directie CI, binnen de bestaande politieke beleidslijnen, expliciet diende vast te leggen 'hoe ver het militaire reikt', waar het louter 'civiele' begint en hoe beiden met elkaar in relatie staan.

Het Comité beveelde aan dat zowel intern (binnen de ADIV, binnen de Directie CI en ook ten overstaan van de Directie I(ntelligence) als extern (in relatie tot de VSSE, het Parket, het OCAD …) de ADIV en de Directie CI een ondubbelzinnig gedragen standpunt zouden uitwerken omtrent wat van de dienst kan en mag worden verwacht en dit rekening houdende met de beschikbare middelen. Eens visie, ambitie en strategie is uitgewerkt, moet daaraan daadwerkelijk de hand worden gehouden zodat de dienst zich als een waardevolle partner in het Belgische antiterrorisme-beleid kan manifesteren.

I.1.4. DE DIRECTIE COUNTERINTELLIGENCE BINNEN DE ADIV

De leiding van de ADIV wordt uitgeoefend door het Commando (ADIV/C), dat kan beschikken over een staf en een secretariaat. De ADIV – waar zowel burgers als militairen tewerkgesteld zijn – was voor 2013 ingedeeld in vier divisies: A(ppui), C(ounter)I(ntelligence), S(ecurity) en I(ntelligence). In 2013 werden CI en S samengevoegd. Wat later werd de Divisie A opgeheven. In 2017 werd een nieuwe reorganisatie doorgevoerd. 'Divisies' werden 'Directies' en de op het binnenland gerichte Directie S(ecurity) en de Directie C(ounter)I(ntelligence) werden opnieuw uit elkaar gehaald. Naast de eerder op het buitenland gerichte Directie Intelligence werd ook een nieuwe Directie Cyber opgericht.

Het Comité stelde echter vast dat er geen eenvormig/uniek uitgetekend organigram van de Directie CI voorhanden was; er circuleerden verschillende versies

waarin geen eenduidige terminologie werd gehanteerd (directies, bureaus, afdelingen, pijlers …). Het personeel van CI kon dus onmogelijk een duidelijk zicht krijgen op de eigen organisatie en wie precies welke verantwoordelijkheid droeg.

I.1.5. DE VASTSTELLINGEN VAN HET ONDERZOEK

I.1.5.1. De (veronderstelde) tegenstelling tussen 'ADIV' en 'ACOS IS'

Het Comité diende – opnieuw – vast te stellen dat er grote onduidelijkheid heerste over de inhoud en het gebruik van de benamingen 'ADIV' en 'ACOS-IS'.[15] Een groot deel van het personeel – waaronder leidinggevenden – van de Directie CI was van mening dat hun directie eigenlijk 'dé ADIV' vormt, terwijl de overige directies (vooral de Directie I) 'ACOS-IS' vormen. Ze waren bovendien van mening dat de Directie CI onafhankelijk dient te zijn van de militaire structuur van Defensie. Hiervoor was geen enkele legale of reglementaire basis.

Veel onduidelijkheid en discussie over de opdracht van de Directie CI bleek net het gevolg van het feit dat de regelgeving zowel spreekt over de Algemene Dienst Inlichting en Veiligheid (ADIV) als van het Stafdepartement Inlichting en Veiligheid (ACOS-IS). De opdrachten van de ADIV worden gedefinieerd in de W.I&V (met name art. 10) en de dienst valt direct onder het gezag van de minister van Defensie (art. 2 W.I&V). ACOS-IS werd vermeld in het KB van 21 december 2001 tot bepaling van de algemene structuur van het Ministerie van Landsverdediging en tot vastlegging van de bevoegdheden van bepaalde autoriteiten.[16] Deze dienst moet blijkens dit besluit inlichtingensteun leveren aan de operaties van Defensie (artt. 22-24 KB) en staat onder leiding van de Onderstafchef inlichtingen en veiligheid, die op zijn beurt aan de CHOD (Chief of Defense) verantwoording aflegt. Nog blijkens het besluit zijn de Onderstafchef en het hoofd van de ADIV één en dezelfde persoon. Wel ressorteert deze laatste rechtstreeks onder de minister van Defensie en heeft de ADIV ruimere opdrachten die in de W.I&V werden bepaald. Het Comité verwachtte dat de leiding van de ADIV en van de Directie CI deze hardnekkige begripsverwarring definitief zou uitklaren.

I.1.5.2. Polarisatie tussen burgers en militairen

Het Vast Comité I kon vaststellen dat de CI-medewerkers de mening waren toegedaan dat de Directie CI een 'bijzondere plaats' inneemt binnen de ADIV (*infra*) en een eigen 'cultuur' heeft. Door de aard van zijn opdrachten, dient CI immers

15 ACOS-IS is het acroniem van 'Assistant Chief of Staff Intelligence and Security'.

16 Dit KB werd vervangen bij het KB van 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. Wat voorliggend onderzoek betreft, veranderde dit besluit niets aan de situatie.

onderzoeken te voeren waarin ook medewerkers van Defensie (in hoofdzaak militairen) betrokken zijn; zij zien deze directie als een controleorgaan. Hierdoor ontstond binnen CI het gevoel dat zij door de andere directies van de ADIV, alsook door andere componenten van Defensie, worden gewantrouwd en dat andere entiteiten de taak en rol van CI niet begrepen.

Dat wantrouwen, het gebrek aan wederzijds begrip alsook de gebrekkige informatiedoorstroming tussen de Directies CI en I leidde onder meer tot conflicten en ondermijnde de mogelijkheden tot samenwerking.[17] Bovendien leefde de indruk dat de sterke korpsgeest onder militairen er vaak toe leidde dat CI-onderzoeken in een vroeg stadium dreigden te worden 'verbrand'. Het Vast Comité I meende dat dit risico niet irreëel was. Het baseerde zich hiervoor op een aantal incidenten in zeer delicate dossiers waarbij bepaalde gegevens of gedragingen van leden van de ADIV onterecht niet aan de Directie CI waren gemeld. Het omgekeerde was echter ook waar: de Directie CI hield bepaalde informatie buiten de militaire keten in die zin dat soms zelfs de chef van de ADIV niet in kennis werd gesteld.

Het Comité was van oordeel dat CI zich te veel afsloot van de rest van de ADIV. Er ontstond een overdreven neiging om bepaalde informatie – noodzakelijk voor een goede werking van de ADIV – niet te delen. Significant in deze is dat een deel van het personeel van CI zijn Directie bij voorkeur zou zien functioneren buiten de ADIV. Het Comité was van oordeel dat dit standpunt ertoe kon leiden dat hierdoor het risico zou kunnen ontstaan dat binnen deze directie normen en regels worden gehanteerd die verschillen van deze bij andere onderdelen van de ADIV. De coördinatie van de onderscheiden inlichtingenactiviteiten zou hierdoor gehypothekeerd worden.

I.1.5.3. (Aan)sturing en planning

Net zoals in 2013[18] stelde het Comité vast dat de medewerkers van CI niet steeds kennis hadden van de precieze inlichtingendoelen waarop ze zich moesten richten. Een aantal essentiële sturingsdocumenten was niet voorhanden. Het gevolg was dat er binnen de Directie CI en op de werkvloer onduidelijkheid heerste over de eigen taakstelling. De relatie tussen CI en andere directies was daardoor eerder problematisch; er heerste een gebrek aan eensgezindheid over de juiste taakstelling.

I.1.5.4. Organisatie en structuur

De Directie CI beschikte niet over een officieel erkend en eenvormig/uniek organogram, de organieke tabel kwam niet overeen met de reële bezetting en verschil-

17 Het Vast Comité I kaartte dit al veel langer aan, zie VAST COMITÉ I, *Activiteitenverslag 2010*, 41 ('II.10. Informatiehuishouding bij de militaire inlichtingendienst').

18 VAST COMITÉ I, *Activiteitenverslag 2013*, 20 ('II.1.3.3.5. Onduidelijkheid over de aard van in te winnen inlichtingen'). Het Comité I beveelde aan dat de '*ADIV verbanden definieert die tussen operationele, tactische en strategische inlichtingen en de wettelijke opdrachten beschreven in de W.I&V, moeten gelegd worden*' (*Ibid*., 113).

lende personeelsleden vervulden taken die niet overeenstemden met hun functie. Bepaalde functies bleken zelfs niet ingevuld en er was een gebrek aan logistieke ondersteuning.

I.1.5.5. De aard van de producten

De werking van de verschillende afdelingen en bureaus van CI was afgestemd op operationeel inlichtingenwerk.[19] Er werd vooral reactief en *ad hoc* gewerkt rond concrete dossiers, er werden weinig of geen inlichtingenproducten op strategisch niveau aangeleverd. Een herdefiniëring van de verhouding tussen de collecte en de analyse (eventueel gepaard met een herstructurering binnen de Directie CI en/of ruimer) drong zich volgens het Comité op.

I.1.5.6. De provinciale detachementen

De provinciale detachementen – de lokale antennes van de Directie CI – zijn verantwoordelijk voor de collecte van informatie (onder meer via HUMINT), voor de vertegenwoordiging van de ADIV op lokaal niveau alsook voor het onderhouden van relaties met lokale autoriteiten en instellingen en de lokale eenheden van Defensie. Het Vast Comité I noteerde een gebrekkige communicatie en *feedback* vanwege de diensten op het hoofdkwartier, problemen met de rechtstreekse toegang tot de databank van CI, een ondermaatse personeelsbezetting, een gebrek aan ondersteuning … Ook was het onduidelijk wat de verhouding en wisselwerking (coördinatie en taakverdeling) was tussen de provinciale detachementen en het nationale detachement; beiden functioneerden immers los van elkaar. Ten slotte ontbrak het ook aan overleg tussen de provinciale detachementen onderling.

I.1.5.7. CI in Ops-zone

Een bijzonder onderdeel van de Directie CI vormt de sectie CI in Ops-zone.[20] Aanvankelijk zette de ADIV gemengde equipes in bij de steun aan operaties: personeel van de Divisie I. werkte samen met personeel van de Divisie CI. Omwille van personeelstekort, kon de Directie CI dit niet langer waarmaken. De sectie I/Ops nam de taak volledig op zich en coverde de aspecten van '*force protection*' in steun van de ontplooide troepen. In 2012/2013 uitte de Directie CI opnieuw de

19 Operationele analyse leidt tot inlichtingen die gebruiksklaar zijn, die m.a.w. onmiddellijk toepasbaar zijn in concrete dossiers. Operationele inlichtingen zijn doorgaans ook bestemd voor intern gebruik en hebben een tactische waarde. Zij leveren een bijdrage aan de realisatie van doelstellingen op korte termijn.

20 De NATO ontwikkelde richtlijnen inzake de ontplooiing van nationale inlichtingencellen (BENIC). Deze richtlijnen schrijven voor dat voornoemde cellen, indien mogelijk, nationale CI-elementen dienen te integreren.

wens om personeel in operatiezones te kunnen inzetten. Deze personeelsleden werden niet geïntegreerd in de structuur I/Ops in zone opdat ze niet zouden worden geassimileerd met dat detachement. Echter, het kader van de Directie CI liet toen niet toe om op permanente wijze personeel voor deze bijzondere opdracht in te zetten. Na verloop van tijd konden twee officieren worden vrijgemaakt om deze cel permanent te bemannen.

Het Comité stelde vast dat de tweeledige structuur in operaties een bron van spanningen vormde.

I.1.5.8. Processen en methoden: SOP's, werklastmeting, KPI's en interne feedback

Het Comité moest vaststellen dat de *Standing Operating Procedures* (SOP's)[21] die van toepassing waren op CI, geen coherent geheel vormden en niet geactualiseerd bleken; ze hielden geen rekening met de gewijzigde structuur van CI noch met de gewijzigde wettelijke opdrachten. CI weet dit aan personeelsgebrek.

Het Vast Comité I stelde tevens vast dat de werklast binnen de Directie CI nergens werd gemeten, geanalyseerd, beheerd noch geëvalueerd. De werklast was ook niet objectiveerbaar, wat te wijten was aan een gebrek aan prioriteitsbepaling, aan duidelijke objectieven, aan structuur binnen de Directie CI, aan functiebeschrijvingen, aan (kennis van) procedures, beheersindicatoren en aan een *benchmark* als referentiepunt (graadmeter). Het Comité stelde op dat vlak de gebrekkige investering vanwege zowel het ADIV-commando als de CI-directie vast.

Ook werden geen gestandaardiseerde *key performance indicatoren* (KPI's)[22] ontwikkeld in de schoot van CI. Wel werden analysecriteria bepaald. Het betrof *quasi* uitsluitend kwalitatieve en geen kwantitatieve criteria.

Verder kon het Comité vaststellen dat er zich problemen voordeden op vlak van het beheer van interne communicatie.

I.1.5.9. Processen en methoden: het beheersen van de tradecraft

Inlichtingenwerk vereist het beheersen van de *tradecraft*.[23] Dit begrip omvat 'de methoden, technieken, technologieën, procedures en basisprincipes opgesteld en

---

21 Een '*standing (standard) operating procedure* (SOP)' is '*a set of instructions covering those features of operations which lend themselves to a definite or standardized procedure without the loss of effectiveness. The procedure is applicable unless ordered otherwise*' (NATO Glossary Terms and Definitions, AAP-6(V)).

22 Een performantie-indicator is een efficiëntie- of resultaatsindicator (effectiviteit) die een meetinstrument vormt voor beslissingsondersteuning. Een KPI richt zich op een vooruitgangsproces. Deze kan collectief of persoonsgebonden zijn en is noodzakelijkerwijs afgestemd op de gekozen strategie. Ze worden gehanteerd bij de voorstelling van beheersboordtabellen.

23 Deze regels zijn zelden formeel vastgelegd maar wel heel belangrijk om het vertrouwen tussen inlichtingendiensten die met elkaar samenwerken in stand te houden.

gebruikt door de inlichtingendiensten teneinde hun opdrachten en operaties tot een goed einde te kunnen brengen'.[24]

Het Comité kreeg kennis van voorbeelden die duidden op een gebrek aan kennisuitwisseling, aan inzicht en aan gemeenschappelijke tenuitvoerlegging van de *tradecraft*. Daarbij werd vastgesteld dat er een spanningsveld bestond tussen de manier waarop vanuit CI naar de *tradecraft* wordt gekeken en de wijze waarop die bijvoorbeeld in het kader van counterterrorisme (CT) wordt benaderd: de cultuur van *need-to-know* botste met deze van *need-to-share*.

I.1.5.10. Personeelsbeheer

Verschillende statuten en een daling van het aantal effectieven

Meer dan de helft van het CI-personeel zijn burgers die in vier verschillende groepen onder te verdelen zijn: de vastbenoemde 'Commissarissen en Inspecteurs' die een bijzondere loopbaan hebben die afwijkt van het gewone Rijkspersoneel (statuut KB van 4 juli 2014[25]), de vastbenoemde 'Commissarissen-analisten', eveneens met een bijzondere loopbaan (eveneens KB van 4 juli 2014), het vast benoemde Rijkspersoneel van het statuut Camu (KB van 2 oktober 1937) en de contractuele personeelsleden (Arbeidsovereenkomstenwet 1978). De loopbaan van de personeelsleden die onder het statuut van 4 juli 2014 vallen, is nauw verbonden met de ADIV: zij kunnen slechts in deze dienst worden ingezet, terwijl het Rijkspersoneel van het statuut Camu en de contractuelen, in principe ook in andere onderdelen van Defensie kunnen tewerkgesteld worden.

De Directie CI beschikt over minder personeel dan in de jaren '80 en dat terwijl andere diensten zoals de VSSE, de politie en het OCAD, ondertussen versterkt zijn.[26] Zelfs met de voorziene rekruteringsgolf (*infra*) zou de dienst slechts op de oorspronkelijke getalsterkte komen. Dit leidde tot desillusie en ontmoediging. Het leidinggevend personeel van CI meende dan ook dat de continuïteit van de dienst in het gedrang kon komen. Het Commando erkende deze problemen en

---

24 Zo is er bijvoorbeeld de *need-to-know*, de regel van de derde dienst, de naleving van de classificatie, van toezicht en countertoezicht, van legendes (*cover story*), van operationele veiligheid, het beheer en de bescherming van menselijke bronnen, de BIM's, het gebruik van cryptografie …. *Tradecraft* heeft eveneens te maken met het aanvaarden van een aantal principes/concepten zoals bijv. de inlichtingencyclus. Wel moet er over gewaakt worden dat deze 'vaknormen' in overeenstemming blijven met de reglementaire normen, en dat deze *tradecraft* voldoende duidelijk wordt gedocumenteerd en waar nodig gedifferentieerd.

25 KB van 4 juli 2014 tot vaststelling van het statuut van bepaalde burgerlijke ambtenaren van het stafdepartement inlichtingen en veiligheid van de Krijgsmacht, *BS* 18 juli 2014. Het gelijknamige KB van 7 juli 2003 werd opgegeven.

26 In het strategisch plan van de minister van Defensie van 29 juni 2016 werd bepaald dat het personeelsbestand van de ADIV in zijn geheel tegen 2030 met ongeveer een derde zou groeien. De ADIV sprak zijn twijfels uit over de haalbaarheid van deze doelstelling, gelet op het feit dat de afbouw van de personeelsaantallen in Defensie (25.000 eenheden in 2020) veel sneller gebeurt dan verwacht.

wees er op dat dit te wijten was aan de tussen 1988 en 2009 geldende wervingsstop in het federaal openbaar ambt.

Met betrekking tot de diverse aspecten van de personeelsproblematiek, is de militaire inlichtingendienst – net zoals alle andere entiteiten van Defensie – afhankelijk van het DG Human Resources en zijn de mogelijkheden voor de ADIV zelf zeer beperkt.

Het opnemen van functies en taken van burgers door militairen: een probleem?

Waar de Directie CI oorspronkelijk grotendeels uit burgers was samengesteld, is dit al lang niet meer het geval. Historisch had het creëren van een burger-component binnen de militaire inlichtingendienst tot doel ten aanzien van mogelijke bedreigingen binnen dat militaire apparaat zelf (vooral spionage, maar ook subversie of extremisme) een beroep te kunnen doen op een van het militaire apparaat onafhankelijk burgerlijk korps. Bij het burgerpersoneel leeft de idee dat enkel burgers de noodzakelijke onafhankelijkheid ten opzichte van de militaire hiërarchie kunnen waarborgen. Het Comité deelde die mening niet; onafhankelijkheid heeft niet noodzakelijkerwijze te maken met het statuut (burgers of militairen), maar wel met de ingesteldheid van de personen, de structuren en procedures. Mede door de invoering van de wervingsstop sinds 1988 bleken gaandeweg meer militairen ingeschakeld te worden binnen de Directie CI. Wettelijk is hiertegen niets in te brengen. Deze 'mix' werd door velen binnen CI als een meerwaarde gezien.

Weliswaar verloopt het inzetten van militair personeel niet zonder problemen: reeds tijdens de Audit 2011 stelde het Comité vast dat de snelle rotatie bij militairen belangrijke uitdagingen stelde op het vlak van hun onthaal, opleiding en kennisbeheer. Er zijn echter ook voordelen (overdracht *best practices,* instroom van nieuwe ideeën …). Het Comité besefte wel dat de inschakeling van militairen in een CI-opdracht niet voor de hand ligt.

Een andere belangrijke kwestie was deze van de erkenning en waardering van het burgerpersoneel. Veel burgers voelden zich ondergewaardeerd. Tijdens de Audit 2011 bleek reeds dat van alle personeelscategorieën dit het meest uitgesproken was bij de commissarissen (niveau A van CI). In die audit stelde het Comité dat het daarom beter was om '*niet te denken in termen van 'personeelsgroepen' (militairen en burgers, contractuelen en statutairen, niveau X en niveau Y …, maar in termen van 'functies'*.[27] Aangezien dit geen positief effect ressorteerde, moeten er naar het oordeel van het Comité meer verregaande structurele maatregelen worden genomen. De denkpiste van een volledige herstructurering van de ADIV mag daarbij niet uitgesloten worden, zonder daarbij de eigenheid van de diverse opdrachten uit het oog te verliezen.

27 VAST COMITÉ I, *Activiteitenverslag 2011*, 11.

De problematiek van het contractueel personeel

De Directie CI telt een beperkt aantal contractuele analisten die reeds zeer lang in dienst zijn. Hun loopbaanmogelijkheden en verloning zijn het minst aantrekkelijk. Het Commando erkende de problematiek en gaf aan dat er in 2016 en 2017 inspanningen waren geleverd om tot een verbetering van hun statuut te komen. Het Commando verwees ook naar de initiatieven van de minister van Ambtenarenzaken ter zake.

Functiebeschrijving en jobinhoud

De door het Comité vastgestelde problemen hebben veelal te maken met een gebrek aan procedures, onduidelijkheid over wie wat doet en wie welke verantwoordelijkheid draagt. Ondanks de aanbevelingen van het Vast Comité I in de Audit 2011, diende te worden vastgesteld dat nog steeds vele functieomschrijvingen ontbraken of weinig transparant waren.

Anderzijds bleken veel personeelsleden zeer tevreden met de jobinhoud. Het werk werd omschreven als 'gevarieerd, avontuurlijk en spannend' met daaraan gekoppeld een grote mate van autonomie en dit alles in een collegiale sfeer.

Rekrutering, selectie, mobiliteit en uitstroom

De ADIV en dus ook de Directie CI heeft als onderdeel van de Krijgsmacht geen autonomie met betrekking tot het personeelsbeheer en dit in al zijn facetten (aanwerving, vorming …). De Directie CI is voor de werving in grote mate afhankelijk van het DGHR (werving van militair personeel) en van SELOR (voor de werving van burgers). Het Comité stelde evenwel dat een deel van de verantwoordelijkheid ook bij de ADIV zelf ligt: de dienst moet goed uitgewerkte functiebeschrijvingen voorleggen waardoor de wervingen gerichter kunnen verlopen.

Een ander probleem vormt de rotatie bij de militairen. In het kader van de loopbaanuitbouw van officieren binnen Defensie is het de regel dat zij in de loop van hun carrière binnen verschillende eenheden worden ingezet. Dit houdt in dat officieren om de drie jaar en onderofficieren om de vijf jaar van eenheid veranderen.[28] Dit werd soms als een probleem gezien omdat de militairen die bij de ADIV vanuit een andere eenheid aankomen niet altijd op een efficiënte en effectieve wijze kunnen worden ingezet, en dit gelet op de specificiteit van een inlichtingendienst en het inlichtingenwerk. Anderzijds maakt dit systeem de instroom van nieuwe ideeën mogelijk.

De loopbaan van het burgerpersoneel bevat minder wendingen. Het burgerpersoneel kan van directie veranderen, maar dit gebeurt niet vaak. Er werd een uitstroom vastgesteld bij contractuelen die elders (Federale Politie, Justitie, VSSE) een vaste betrekking konden vinden.

[28] Er zijn evenwel uitzonderingen op deze regel.

Vorming, opleiding en kennisbeheer

In tegenstelling tot burgers die als inspecteur of commissaris intreden en die van bij aanvang in het inlichtingenwerk hun loopbaan zullen uitbouwen (en daarvoor dus ook op werden geselecteerd en gevormd), komen militairen die naar de ADIV gemuteerd worden, dikwijls zonder specifieke kennis aan. Dit vormt een belangrijk probleem.

Binnen ADIV bestaat een cel die instaat voor de vorming. Haar belangrijkste taak bestaat erin om voor het burgerpersoneel een loopbaantraject te organiseren en op te volgen.

Voor de opleiding van nieuwe personeelsleden werd een *Basic Inspector Counter Intelligence Course 2018-2019* uitgewerkt waarbij de kandidaten modules dienen te doorlopen, gevolgd door een stage van een jaar.

Ondanks eerdere aanbevelingen[29] stelde het Comité opnieuw vast dat er binnen CI geen formeel kennisbeheer was.[30] Veel kennis bleek geconcentreerd bij individuele personeelsleden en werd niet gedeeld. Het Comité stelde ten slotte vast dat het risico op verlies van kennis en expertise binnen de organisatie werd vergroot door het personeelsverloop (vooral bij de analisten) en dat er geen specifieke procedures waren om kennis- en expertiseverlies op te vangen.

De individuele beoordeling

Het Comité kon vaststellen dat er binnen de ADIV drie evaluatiesystemen naast elkaar bestonden: twee voor de burgers (Statuut Camu/contractuelen versus Statuut 2014) en een derde voor de militairen, wat een ongelijke behandeling veroorzaakt. Vast staat dat militairen geen beslissende zeggenschap hebben over de evaluatie van burgers en *vice versa*. Dit doorkruist de hiërarchische lijnen en kan problematisch zijn.

I.1.5.11. Werkomstandigheden en infrastructuur

Het Vast Comité I moest (opnieuw) vaststellen dat de arbeidsomstandigheden schrijnend en op diverse vlakken onaanvaardbaar waren.

De materiële werkomstandigheden vormden voor het personeel dé prioriteit. Het Comité kon verschillende tekortkomingen vaststellen op vlak van veiligheid,

---

29 Het Vast Comité I beveelde in de Audit 2011 aan om dringend acties te ondernemen om de risico's inzake discontinuïteit van de functie-uitoefening en verlies van kennis te beperken: '*Het is aangewezen dat er binnen de ADIV uitgesproken aandacht wordt betoond voor kennismanagement. Er moeten duidelijke instructies worden uitgewerkt om de aanwezige kennis in kaart te brengen, de relevantie ervan te beoordelen en maatregelen te nemen om ze op te slaan, te bewaren en te verspreiden. Het strekt tot aanbeveling binnen elke divisie een kennisbeheerder aan te stellen die het kennismanagement ondersteunt*', in VAST COMITÉ I, *Activiteitenverslag 2011*, 107.

30 Dit is het proces van het creëren, inventariseren (wie weet wat), delen, gebruiken, en beheren van de kennis en expertise binnen een organisatie).

hygiëne en gezondheid, accommodatie … in die mate dat ze de integriteit van de gebouwen en het personeel ernstig in het gedrang brachten.[31] Voor het verbeteren van de materiële omstandigheden is de ADIV afhankelijk van de Algemene Directie *Material Resources (DGMR); haar* autonomie is op dit vlak zeer beperkt.

Het huisvestingsprobleem van de ADIV en bijgevolg de Directie CI moet worden gezien in het grotere geheel van de nieuw te bouwen infrastructuur voor de Defensiestaf. Het Vast Comité I was desondanks van mening dat dringend werk moest worden gemaakt van betere werkomstandigheden.

I.1.5.12. Ondersteuning en logistiek

Het personeel van de steundiensten binnen de ADIV (personeels- en budgettair beheer, ICT, logistiek …) bleek niet doordrongen van de inlichtingencultuur of de specificiteit van de dienst. Het ontbrak aan kennis over het inlichtingenwerk en ze hadden het bijgevolg moeilijk om de noden van de dienst te vertalen naar de andere Algemene Directies en departementen. Er werd vastgesteld dat de communicatie tussen de Directie CI en de steundiensten niet efficiënt verliep en zelfs weinig ontwikkeld was.

Het Vast Comité I moest ook vaststellen dat de Directie CI weinig communiceerde met de secties van de Generale Staf. Het Comité benadrukte dat deze secties van de Generale Staf de *interface* vormen om te kunnen communiceren met de andere actoren buiten de ADIV. CI-stafmedewerkers gaven te kennen dat de administratieve, logistieke en technische ondersteuning grotendeels was uitgehold. Er werd geklaagd over een gebrek aan autonomie en zware bureaucratie.

I.1.5.13. Informatiebeheer[32]

Voorgaande onderzoeken leerden het Vast Comité I dat het beheer van de informatie bij de ADIV bijzonder problematisch was.[33] Het onderzoek bevestigde deze vaststellingen opnieuw voor wat de Directie CI betreft. Dit kon onder meer worden afgeleid uit de personeelsbevraging dewelke te kennen gaf dat er onder meer een probleem was inzake de toegang tot externe databanken. Ook inzake de snelheid, structuur, volledigheid, gebruiksvriendelijkheid en toegankelijkheid van de

---

31 De minister van Defensie liet optekenen dat er in afwachting van een structurele oplossing instandhoudingswerken werden uitgevoerd.

32 De problematiek van het informatiebeheer is veel ruimer dan hier wordt besproken. Sinds de vaststellingen van de problemen door het Comité rond opslag en beheer van informatie in 2005, werd in 2007 een werk- en investeringsprogramma opgesteld. Rekening houdend met de budgettaire beperkingen konden de investeringen pas in 2013 beginnen. Ook werd een Information Management Cell opgericht in 2013 om het informatiebeheer te verbeteren. Deze cel werkte een meta-databeheersmodel uit, maar het ontbrak aan middelen om het beheermodel te laten functioneren. Hierover: Senaat 2017-18, 29 november 2017, Vr. nr. 6-1674.

33 Hierover bijvoorbeeld VAST COMITÉ I, *Activiteitenverslag 2016*, 35 ('II.3. Toezichtonderzoek over de informatiepositie van de twee inlichtingendiensten voor de aanslagen in Parijs').

informatie en documentatie, scoorde CI slecht. Wat betreft de eigen CI-databank deden zich drie belangrijke problemen voor: een achterstand in de verwerking van data, gebrekkige linken met de brondocumenten en de creatie van individuele folderstructuren.

I.1.5.14. Partnerschappen

De Directie CI heeft talrijke nationale en internationale partners (Belgische administraties, buitenlandse partnerdiensten, private partners …). Toch konden er weinig synergieën worden vastgesteld. Het Comité verwees daarbij naar de vaststellingen én aanbevelingen van de Parlementaire Onderzoekscommissie Terroristische aanslagen.[34] Uiteraard dient bij het uitwerken van synergiën rekening te worden gehouden dat door deze synergieën de specificiteit van de opdrachten van de Directie CI niet in het gevaar komen.

I.1.5.15. Feedback

Al in 2010[35] beveelde het Comité aan dat bij de ADIV een feedbackmechanisme zou worden ingebouwd voor alle geleverde producten. Enerzijds moesten de diensten duidelijk maken onder welke voorwaarden, hoe en naar wie ze inlichtingen willen of kunnen verspreiden en welke 'ambitie' daarbij vanwege de dienst mag verwacht worden (beschrijvende, verklarende of voorspellende inlichtingen). Het Comité benadrukte hierin ook de rol van de klanten. Zij moeten aangeven wat ze verwachten en welke hun (inlichtingen-)behoeften zijn. Het Comité diende ook in dit onderzoek vast te stellen dat er weinig of geen sprake was van *feedback*.

I.2. DE ACTIVITEITEN VAN DE ADIV IN EEN BUITENLANDSE OPERATIEZONE

Een belangrijk deel van het werk van de ADIV is gericht op de productie van inlichtingen over de politiek-militaire situatie in het buitenland. Daarom betoonde het Comité reeds eerder belangstelling voor de rol van deze dienst in buitenlandse operatiegebieden als Afghanistan en Libanon.[36] In 2018 bestudeerde

---

34 Parlementair onderzoek belast met het onderzoek naar de omstandigheden die hebben geleid tot de terroristische aanslagen van 22 maart 2016 in de luchthaven Brussel-Nationaal en in het metrostation Maalbeek te Brussel, met inbegrip van de evolutie en de aanpak van de strijd tegen het radicalisme en de terroristische dreiging, derde tussentijds verslag, *Parl. St.* Kamer 2016-17, nr. 54K 1752/007.

35 Onder meer in: VAST COMITÉ I, *Activiteitenverslag 2011*, 104-105 ('IX.2.2.1. Aanbevelingen inzake organisatorische voorwaarden noodzakelijk voor een goede inzet van de middelen').

36 VAST COMITÉ I, *Activiteitenverslag 2013* ('II.1. De rol van de Algemene Dienst Inlichting en Veiligheid bij de opvolging van het conflict in Afghanistan'), 7-25 en *Activiteitenverslag 2007* ('II.2.2. De opvolging van radicaal islamisme door de ADIV'), 22.

het Comité opnieuw de ontplooiing van de ADIV – en bij uitbreiding het ISTAR-bataljon (zie *infra*) – in een bepaalde[37] operatiezone.[38] De ADIV leverde er steun aan de Belgische militaire commandanten ter plaatste en stond, overeenkomstig de aanbevelingen van de parlementaire onderzoekscommissie Rwanda[39], in voor de *force protection* van de Belgische militairen. De ADIV voerde eveneens ondersteunende opdrachten uit voor de Belgische ambassade en droeg bij tot de veiligheid van de expats. Via zijn analysebureaus in België ten slotte, werkte de ADIV mee aan de totstandkoming van de Belgische strategische visie met betrekking tot de conflictzone.

Voor het onderzoek baseerde het Comité zich onder meer op de studie van tal van documenten[40], op briefings van de ADIV en op contacten met personeelsleden van de militaire inlichtingendienst. Het boog zich verder over de samenwerking tussen de diverse afdelingen van de ADIV onderling en over de samenwerking met buitenlandse partners op het terrein. Aangezien de informatie die uit het onderzoek voortkwam, geclassificeerd is, kan het Comité hier niet verder op ingaan. Hieronder worden slechts drie elementen kort belicht: de juridische context van de inzet van de ADIV, de werking van en de controle op het ISTAR-bataljon en enkele algemene conclusies.

I.2.1. JURIDISCHE CONTEXT VAN DE ONTPLOOIING EN ACTIVITEITEN IN DE ZONE

De inzet van de militaire eenheden in de zone kaderde binnen een niet-internationaal gewapend conflict. Dit betekende dat het recht dat geldt ten tijde van gewapende conflicten van toepassing was. De inzet van Belgische troepen gebeurde in overeenstemming met een resolutie van de Veiligheidsraad van de Verenigde Naties en werd goedgekeurd door de Ministerraad.

De bevoegdheid van de ADIV om steun te verlenen aan operaties staat omschreven in artikel 11 § 1, 1°, d) W.I&V: '*§. 1. De Algemene Dienst Inlichting en Veiligheid heeft als opdracht: 1° 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, alsook de inlichtingen die betrekking hebben op elke activiteit die […]: d) de vervulling van de opdrachten van de strijdkrachten; […] en er de bevoegde ministers onverwijld over inlichten alsook de regering, op haar verzoek, advies verlenen bij de omschrijving van haar binnen- en buitenlands beleid inzake veiligheid en defensie*'.

37 Om veiligheidsredenen besloot het Vast Comité I om de locatie niet te vermelden.
38 Het onderzoek werd begin maart 2018 geopend en begin juli 2018 afgerond.
39 *Parl. St.* Senaat 1997-1998, 6 december 1996, nr. 1-611/7.
40 Het Operationeel Order van de Chef Defensie (CHODOPORDER), briefings van de verschillende afdelingen, rapporten geproduceerd door ingezette eenheden ….

Aangezien de dienst niet alle in dit kader mogelijke opdrachten kan uitvoeren, worden er in het zogenaamde 'Inlichtingenstuurplan' (PDR) prioriteiten bepaald. Het land waarin de conflictzone gelegen was, kreeg de hoogste prioriteit in het PDR 2015-2018.

De concrete activiteiten van de ADIV bij buitenlandse operaties worden verder nader bepaald door zogenaamde operatieorders van de CHOD (CHODOPORDER). Ten slotte zijn er ook *Fragmentary Orders* (FragO). Deze bepalen de inzet van specifieke ADIV-eenheden zoals bijvoorbeeld *Contact Teams* die tijdelijk ter plaatse worden gestuurd. Al deze documenten bepalen het kader en de limieten waarbinnen de verschillende detachementen (met inbegrip van deze van de ADIV) hun opdrachten kunnen uitvoeren. Volledigheidshalve kan worden aangestipt dat de Nationale Veiligheidsraad eveneens bijzondere directieven zou kunnen uitvaardigen in het kader van de inzet van middelen van de ADIV in het buitenland. Tot op heden is dit nog niet gebeurd.

I.2.2. HET ISTAR-BATALJON

Al in 2013 nam het Vast Comité I 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.[41] Het Comité benadrukte daarin dat de oprichting van het bataljon tegemoet kwam aan een stijgende behoefte aan *battlefield intelligence*, en dit gelet op het toenemend aantal buitenlandse opdrachten. Het Comité herhaalde dat de organieke Wet van 30 november 1998 slechts twee inlichtingendiensten erkent. Het wees zowel het Parlement, de minister van Defensie als de CHOD op het feit dat dit bataljon gedeeltelijk inlichtingenactiviteiten ontwikkelt. Aangezien er op korte termijn geen wettelijke of structurele oplossingen voorhanden bleken, werd een voorlopige oplossing uitgewerkt door middel van een protocolakkoord tussen de ADIV en de CHOD.[42] Hierin worden de taken en opdrachten van het ISTAR-bataljon inzake HUMINT- en analysecapaciteiten vastgelegd. Daarnaast wordt de organisatie van een technische en juridische controle uitgewerkt. Die taak berust bij de ADIV. Het Vast Comité I is aangewezen om een – zij het onrechtstreeks, want via de rapporten van de ADIV – toezicht uit te oefenen over de activiteiten van het bataljon.

Het Comité kon vaststellen dat, overeenkomstig de aanbevelingen van de parlementaire onderzoekscommissie 'Terroristische Aanslagen' en zijn eigen aanbevelingen, de elementen van het ISTAR-bataljon die in de betrokken operatiezone

41 In 2013 werd de Begeleidingscommissie van de Senaat in kennis gesteld van het juridisch standpunt van het Comité hieromtrent (VAST COMITE I, *Activiteitenverslag 2013*, 92).

42 Protocolakkoord van 24 mei 2018 tussen de CHOD en de ADIV betreffende de HUMINT- en de analysecapaciteiten van het ISTAR Bn.

aanwezig waren, maar bij de ADIV waren gedetacheerd voor de duur van hun inzet, en hierdoor administratief werden beschouwd als organieke elementen van de ADIV.

I.2.3. CONCLUSIES

Behoudens het feit dat de ADIV een bepaalde formele voorwaarde voor de inzet van een collectemethode niet had nageleefd, stelde het Comité geen onwettigheden vast. Alle ontplooide personeelsleden getuigden van professionalisme en inzet. De activiteiten van de ADIV hebben toegelaten om essentiële informatie in te winnen bij evenementen of incidenten waarbij Belgen of Belgische of Europese belangen betrokken waren. Het Vast Comité I heeft eveneens vastgesteld dat de samenwerking tussen de directies van de ADIV berustte op een intens informeel overleg.

De werk- en veiligheidsomstandigheden maakten het voorwerp uit van analyses. Het Comité detecteerde alsnog enkele kwetsbaarheden die een mogelijk risico voor de veiligheid van de operaties of het personeel konden vormen. Met betrekking tot het controleniveau moest het Vast Comité I vaststellen dat gedurende de eerste rotatie van elementen van het ISTAR-bataljon, de ADIV een door de reglementen voorziene controle niet had uitgevoerd.

I.3. DE INFORMATIEPOSITIE VAN DE INLICHTINGENDIENSTEN VOORAFGAAND AAN DE AANSLAG IN LUIK

I.3.1. CONTEXTUALISERING

Op 29 mei 2018 bracht Benjamin Herman twee politieagentes om het leven in Luik. Beiden werden met een mes aangevallen en vervolgens neergeschoten. De dader bracht daaropvolgend een auto tot stilstand, waarbij ook de passagier om het leven kwam. Herman verschanste zich in een school waar hij iemand gijzelde. In het vuurgevecht dat daarop volgde, raakten meerdere agenten gewond en werd hijzelf omgebracht.

De dader was sinds zijn jeugd bekend bij Justitie. Hij zat op het moment van de feiten een gevangenisstraf van lange duur uit omwille van misdrijven van gemeen recht. Benjamin Herman doorliep verschillende penitentiaire instellingen en zou in de loop van 2018 vrijkomen. De dag voor de feiten kreeg hij penitentiair verlof als voorbereiding op zijn definitieve invrijheidsstelling. Hij vond onderdak bij een kennis. Achteraf bleek dat ook de persoon bij wie hij had aangeklopt om te overnachten, werd gedood.

De parlementaire Begeleidingscommissie verzocht de Vast Comités I en P begin juni 2018 een toezichtsonderzoek te openen.[43] Er waren immers aanwijzingen dat Benjamin Herman in de loop van 2017 tekenen van radicalisering vertoonde in de gevangenis van Lantin. De Begeleidingscommissie specificeerde halfweg juni 2018 haar vraag voor wat het Vast Comité I betrof en verzocht om een toezichtonderzoek '*naar de informatiepositie van de VSSE en de informatie-uitwisseling tussen de VSSE en haar partners met betrekking tot de dader en eventuele mededaders of medeplichtigen van de incidenten te Luik*'.[44]

Daarbij waren – voor de inlichtingen- en veiligheidsdiensten[45] – onderstaande vragen aan de orde:

- Was de dader bij de VSSE en/of de ADIV bekend vóór de aanslag, welke informatie was er over hem beschikbaar en welke dienst lag aan de basis van deze informatie?
- Met welke diensten werd er informatie uitgewisseld of werd er overleg gepleegd?
- Kwam de dader ter sprake op lokale of nationale vergaderingen (Local Task Force (LTF), National Task Force (NTF)[46], of nog, de Lokale Integrale Veiligheidscel (LIVC)[47])?
- Werden de VSSE en/of de ADIV door de partnerdiensten gecontacteerd aangaande betrokkene vóór 29 mei 2018?

---

43 Ook verzocht de Commissie aan beide Comités een gezamenlijk onderzoek te openen naar de rol van het OCAD bij de opvolging van de dader. Hierover: 'II.4. 'De informatiepositie van het OCAD voorafgaand aan de aanslag in Luik'.

44 Het Vast Comité P voerde op zijn beurt een onderzoek naar de informatie-uitwisseling bij de politiediensten. Het gemeenschappelijk eindverslag van beide Comités werd goedgekeurd op 16 juli 2018.

45 De toezichtbevoegdheid van beide Vaste Comités strekt zich niet uit tot andere diensten dan politie-, inlichtingen- en veiligheidsdiensten. De Comités kunnen wel personen van andere diensten (zoals het DG EPI) uitnodigen om deze te horen wanneer ze dat noodzakelijk achten (artt. 24 en 48 W.Toezicht). De enquêtediensten hadden een contact met de administratieve cel van het Kabinet van de minister van Justitie (SAT Justitie) teneinde inzicht te krijgen in de manier waarop de informatie over gedetineerden ter beschikking wordt gesteld. Ook vonden vergaderingen plaats met de Cel Extremisme (Dienst CelEx) van het DG EPI en met een vertegenwoordiger van het directoraat-generaal, met de bedoeling achtergrondinformatie te krijgen over de manier waarop extremistische gevangenen worden opgevolgd.

46 Een LTF is een overlegplatform, ingericht op gedeconcentreerd niveau, waarbinnen politie- en inlichtingendiensten informatie en inlichtingen over gewelddadige radicalisering uitwisselen en coördinatieafspraken maken over het inwinnen van de informatie (uit: Ministeriële Omzendbrief GPI 78 van 31 januari 2014 betreffende de informatieverwerking ten voordele van een geïntegreerde aanpak van terrorisme en gewelddadige radicalisering door de politie, *BS* 17 februari 2014). Ze werken onder de coördinatie van de *National Task Force*.

47 De LIVC-R is een multidisciplinair, gemeentelijk overlegplatform met socio-preventieve actoren in de bestrijding van gewelddadige radicalisering doordat zij personen die zich in een radicaliseringsproces bevinden vroeg detecteren en geïndividualiseerde opvolgtrajecten uitwerken voor hen.

– In het bijzonder voor de VSSE: hoe verliep de samenwerking met het Directoraat-generaal Penitentiaire Inrichtingen (DG EPI) in uitvoering van het Protocolakkoord?

I.3.2. DE OPVOLGING VAN EXTREMISTISCHE GEDETINEERDEN

I.3.2.1. Een verscheidenheid aan actoren

Bij de opvolging van gedetineerden met een extremistisch gedachtengoed of gedetineerden die veroordeeld zijn in het kader van terrorisme, zijn voor verschillende diensten opdrachten weggelegd. Ze werken samen door onderling informatie uit te wisselen en/of door te overleggen om de stand van zaken of te nemen acties te bepalen.

In dat kader is een belangrijke rol weggelegd voor het DG EPI. De gedetineerden komen dagelijks in contact met het penitentiair personeel en met de lokale directies. Voor elke gedetineerde wordt een persoonlijk dossier bijgehouden en bijgewerkt wanneer zich een feit voordoet. Op het hoofdbestuur van het DG EPI is de Cel Extremisme (Dienst CelEx) belast met een bijzondere opvolging van de gedetineerden die een radicaal profiel hebben.

Ook de VSSE heeft interesse voor deze personen, en dit zowel tijdens hun gevangenschap als na hun vrijlating. Binnen de VSSE is sinds 2015 een Cel Gevangenissen opgericht die in nauw contact staat met het DG EPI.[48] Ook de buitendiensten (provinciale posten) van de VSSE vervullen in deze een rol, en dit door via hun contacten met de gevangenisautoriteiten informatie in te winnen over de gevangenen die de aandacht trekken van de VSSE.

De politie die een gevangenis op haar grondgebied heeft, is er in het kader van haar opdracht van bestuurlijke politie toe gehouden om samen te werken met de gevangenisautoriteiten. Ze staat in voor de evaluatie van het risico van de overbrenging van gevangenen (bijv. uithalen van gevangenen) alsook voor de basispolitiezorg, waaronder de wijkwerking. Artikel 20 WPA voorziet in het toezicht door de politie op de veroordeelden die een strafuitvoeringsmodaliteit genieten.[49]

---

48 Sinds het ontstaan van de Cel Gevangenissen verviervoudigde de omvang van dit bureau van drie personen waarvan één analist in 2015 tot twaalf medewerkers, waarvan een drietal analisten.

49 De gemeenschappelijke omzendbrief van de ministers van Justitie en Binnenlandse Zaken en het College van procureurs-generaal COL 11/2013 verduidelijkt dat de erin beschreven politionele toezichtsopdrachten niet verplicht moeten worden uitgevoerd in de gevallen van uitgaansvergunning en penitentiair verlof. In deze laatste gevallen is de opdracht van de politiediensten beperkt tot de uitoefening van het algemeen politioneel toezicht.

Het Coördinatieorgaan voor de dreigingsanalyse (OCAD) komt enkel tussen wanneer een gevangene hetzij in een gemeenschappelijke gegevensbank (GGB)[50] is opgenomen (als *foreign terrorist fighter*, *home grown terrorist* of haatpredikant) of wanneer er elementen zijn – aangebracht door zijn steundiensten – die op een terroristische of extremistische dreiging wijzen.

Ten slotte kunnen ook de gerechtelijke instanties – meer in het bijzonder de parketten – een rol spelen wanneer zij van de verschillende diensten informatie krijgen over activiteiten van gevangenen die een strafrechtelijk karakter vertonen of wanneer deze bij dergelijke activiteiten betrokken zijn, of nog wanneer er gerechtelijke acties moeten worden ondernomen.

I.3.2.2. Een verscheidenheid aan databanken

De databank SIDIS Suite, die wordt beheerd door het DG EPI, verwerkt 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 afdeling tot bescherming van de maatschappij (internering) of een gemeenschapsinstelling voor minderjarigen verblijven. Dit alles om een adequaat beheer van de detentie en van de inrichtingen te vergemakkelijken. De databank maakt de noodzakelijke informatie-uitwisseling en gegevensstromen tussen politie, parket, inlichtingendiensten, justitiehuizen … mogelijk. SIDIS Suite bevat informatie over de duur van de opsluiting, vingerafdrukken, het penitentiair traject en regime, bezoekers, verloven … De VSSE, de Federale Gerechtelijke Politie, DGA/DAO, DGJ/DJO, de Communicatie- en informatiedienst van het arrondissement (SICAD) en de politiezones met een gevangenis of een gerechtsgebouw op hun grondgebied hebben toegang tot de gegevens.[51,52] De politiediensten hebben evenwel geen toegang tot alle gegevens.

---

50 Zie art. 44/11/3*bis* WPA dat in de oprichting van gemeenschappelijke gegevensbanken voorziet. Zie hierover *in extenso*: 'Hoofdstuk VI. De controle van de gemeenschappelijke gegevensbanken'.

51 De gerechtelijke signaleringen van vrije of onder voorwaarden in vrijheid gestelde personen maken het voorwerp uit van COL 11/2013 en van de Omzendbrief FTF van 2015. Inzake penitentiair verlof verleend door de minister van Justitie, voorziet COL 11/2013 niet dat de gevangenis actief informatie moet sturen aan de politiezones.

52 Over SIDIS Suite en de manier waarop diensten buiten DG EPI toegang hebben, zie ook het antwoord van de minister van Justitie in de Kamercommissie Justitie d.d. 20 juni 2018, *Parl. St.* Kamer, CRABV, 54, COM 930. Er moet opgemerkt worden dat de toegang tot SIDIS Suite niet voor alle diensten identiek is. In zijn hoedanigheid van Bevoegde toezichthoudende autoriteit formuleerde het Vast Comité I, samen met het Vast Comité P, over een voorontwerp van wet inzake de toegang tot Sidis Suite voor het OCAD, in oktober 2018 een advies (www.comiteri.be, Advies 007/008 – Leesrecht SIDIS SUITE/OCAD). Het Vast Comité I formuleerde tevens een advies over het leesrecht in Sidis Suite voor de VSSE, de ADIV en de veiligheidsoverheden (www.comiteri.be, Advies 006/2018, Leesrecht SIDIS SUITE).

Daarnaast houdt het DG EPI ook een 'CelEx'-lijst bij.[53,54] Deze lijst – gebaseerd op de nota 'Specifieke instructies extremisme' van het DG EPI – is opgesteld ter attentie van de gevangenisdirecties maar ook van alle personeelsleden opdat zij voortdurend aandachtig zouden zijn voor tekenen van radicalisering en extremisme. De opname in deze lijst heeft meer toezicht op de gevangene tot gevolg. De CelEx-lijst omvat vier categorieën van gevangenen.[55] Zodra een persoon op deze lijst komt, wordt een bericht gestuurd aan de partnerdiensten (VSSE, DJSoc Terro, OCAD) teneinde deze informatie te delen, maar ook om te vernemen of die persoon al gekend is bij de inlichtingen- en politiediensten. In bepaalde gevallen gaat er eveneens een bericht naar verschillende diensten wanneer een gedetineerde zich buiten de gevangenis begeeft. Benjamin Herman bevond zich niet op de CelEx-lijst.

Tweemaal per maand wordt op federaal niveau een vergadering georganiseerd van de Werkgroep Gevangenissen van het Plan Radicalisme, waarbij het DG EPI (CelEx), de VSSE, het OCAD en de Federale Politie (DJSOC/terro) overleg plegen, onder meer over de samenstelling van de CelEx-lijst. De VSSE liet optekenen dat er geen formele procedure bestaat over de plaatsing (en de verwijdering) van personen op deze 'lijst' en dat de adviserende rol van de partnerdiensten van het DG EPI eerder informeel is en gegroeid vanuit de dagelijkse praktijk van de samenwerking. De VSSE stelde voorstander te zijn van een formalisering van de procedures en een verbreding van het *ownership* dat op het ogenblik van het onderzoek nog volledig bij het DG EPI lag.

Ten slotte moet worden gewezen op het feit dat de VSSE zich niet beperkt tot het opvolgen van de gedetineerden die op de CelEx-lijst voorkomen. De Cel Gevangenissen werkt daarnaast met 'targetlijsten' van gedetineerden per gevangenis. Ten tijde van het onderzoek genoten ongeveer 500 gedetineerden de aandacht van de VSSE omwille van een potentieel verband met terrorisme (toegang tot wapens, financiering van terrorisme met drugsgeld …). Dat er met twee 'lijsten' wordt gewerkt, heeft onder andere te maken met het feit dat de VSSE de namen van bepaalde gedetineerden niet wil delen omwille van brongevaar of de regel van de derde dienst, of om lopende inlichtingen- of gerechtelijke onderzoeken niet in gevaar te brengen. Bovendien moet rekening gehouden worden met

---

53 Afkorting van 'Cellule/Cel Extremisme', die de lijst opstelt en bijhoudt. De lijst bevatte begin juli 2018 234 namen (zie antwoord van de minister van Justitie, *Parl. St.* Kamer, CRAVB, 54, COM 910 d.d. 4 juni 2018, 34: *'er zouden ongeveer 250 geradicaliseerden in onze gevangenissen opgesloten zitten*').

54 Het DG EPI spreekt eerder over het 'CelEx-rapport' dan over de CelEx-lijst.

55 (a) degenen die veroordeeld of in verdenking gesteld zijn voor terroristische misdrijven; (b) degenen waarvan de daden worden gelijkgesteld met terroristische misdrijven; (c) de *(foreign) terrorist fighters* en *home grown terrorists* van de OCAD-lijst, of hun opsluiting gemotiveerd is door hun FTF-karakter of niet (veel gemeen recht); en ten slotte (d) bevat de lijst een vierde restcategorie D. De centrale Cel Extremisme evalueert met de steun van haar partners of gevangenen moeten worden ondergebracht in deze categorie. De bevoorrechte partners van de cel zijn het OCAD, DJSOC Terro en de VSSE.

het feit dat de VSSE en het DG EPI een verschillende finaliteit hebben; de VSSE kan in een vroeg stadium overgaan tot het inwinnen van inlichtingen over bepaalde gedetineerden, zonder dat er voor het DG EPI al voldoende aanleiding is om ze op de CelEx-lijst op te nemen. Benjamin Herman stond ook niet op deze targetlijsten.

I.3.3. DE INFORMATIE WAAROVER DE INLICHTINGENDIENSTEN BESCHIKTEN[56]

Benjamin Herman was niet gekend in de databanken van ADIV. Weliswaar bleek dat de ADIV aanwezig was op en bestemmeling was van een verslag van een vergadering van een LTF op 22 februari 2015 in Marche-en-Famenne, waarin Benjamin Herman vermeld werd. Er was echter geen enkel militair aanknopingspunt, zodat het niet abnormaal was dat de naam van betrokkene niet werd ingevoerd in de databank van de ADIV.

Bij de VSSE kwam Benjamin Herman in zeven documenten voor.[57] Uit de beschikbare nota's blijkt dat de gegevens die de VSSE over Benjamin Herman had, eerder vaag en beperkt van inhoud waren. De laatste informatie van eigen collecte dateerde van 1 februari 2017. Daarin werd gesteld dat Benjamin Herman volgens een bron radicaliseerde en steeds meer contact zocht met een persoon die activiteiten van proselitisme ontplooide in de gevangenis. De analysenota's die volgden, hernamen deze en eerdere informatie. Zo bijvoorbeeld werd in mei 2017 een analysenota verspreid naar de Federale Politie, het OCAD en het DG EPI.

I.3.4. ONDERLINGE INFORMATIESTROMEN

Er vonden op diverse tijdstippen overlegvergaderingen plaats tussen verschillende diensten (LTF, Werkgroep Gevangenissen) waarbij de naam van de betrokkene ter sprake kwam.

I.3.4.1. De Local Task Force (LTF)

Benjamin Herman werd vernoemd in twee verslagen van de LTF-vergaderingen Luxemburg (februari 2015 en maart 2017).

Op de vergadering van 2015 waren verschillende politiediensten en de ADIV aanwezig; het OCAD, de VSSE en het parket waren niet aanwezig. Het proces-

---

56 Over de informatie waarover de politiediensten beschikten wordt gerapporteerd door het Vast Comité P (www.comitep.be).

57 Het ging om vijf operationele rapporten (OR) van de collectediensten dewelke niet rechtstreeks extern worden verspreid maar door de analysediensten verwerkt, één synthesefiche (FS) en twee 'Notes aux autorités' (NA) waarmee de autoriteiten werden geïnformeerd.

verbaal werd verzonden naar de aanwezige personen en de VSSE, maar niet naar het OCAD.[58] Dat verslag bevat een verwijzing naar Benjamin Herman die samen met twee anderen intensief zou bidden, maar vermeldt ook dat er geen medegedetineerden onder druk werden gezet om daaraan deel te nemen.[59]

In de LTF-vergadering van maart 2017 werd een lijst van meer dan 50 opgevolgde personen doorgenomen. Verschillende politiediensten, de VSSE en het OCAD, alsmede het parket waren aanwezig; de ADIV niet. Het verslag, waarin Benjamin Herman voorkomt, werd verstuurd naar alle diensten. In de kolom 'Persoon' komt de naam van betrokkene niet expliciet voor, wel die van een andere persoon die zich in de gevangenis van Marche-en-Famenne bevond, en zich aldaar dreigend en arrogant gedroeg en van een harde jihadist wilde doorgaan. Er wordt vermeld dat deze persoon opgesloten werd naar aanleiding van misdrijven van gemeen recht die hij – onder andere – samen met Benjamin Herman pleegde.[60] Deze informatie was afkomstig van een informatierapport (RIR) van de lokale politiezone Famenne-Ardenne. Benjamin Herman was weliswaar zelf niet het voorwerp van de RIR. Tijdens dergelijke vergaderingen is het naar luid van de respondenten gebruikelijk dat een persoon slechts wordt vermeld wanneer de betrokken diensten iets nuttigs over hem te zeggen of toe te voegen hebben. Benjamin Herman trok in dat opzicht geenzins de aandacht. De op de vergadering aanwezige inspecteur van de VSSE, maakte ten behoeve van zijn hiërarchie een intern verslag op. In dit interne verslag komt de naam van Benjamin Herman niet voor. Hieromtrent bevraagd, stelde de VSSE dat de interpretatie was dat het om feiten van gemeen recht ging, hetgeen niet tot de aandachtsfeer van de dienst behoort. Er was voor de VSSE dus geen aanleiding om de naam van Benjamin Herman op basis van de LTF-lijst specifiek in een intern verslag op te nemen.

I.3.4.2. Werkgroep Gevangenissen van het Plan Radicalisme

Benjamin Herman bevond zich niet op de CelEx-lijst. Tijdens de tweewekelijkse besprekingen van de Werkgroep Gevangenissen van het Plan Radicalisme tussen de VSSE, het DG EPI (CelEx), het OCAD en de Federale Politie (DJSOC/terro) kwam zijn naam nooit ter sprake. De VSSE maakte van deze vergaderingen enkel een verslag voor intern gebruik.[61]

---

58 De verslagen van de Local Task Forces dienden op dat ogenblik niet aan het OCAD te worden gestuurd. Het OCAD was enkel bestemmeling van relevante informatie met betrekking tot *foreign terrorist fighters*.

59 Deze informatie is dezelfde als deze vervat in een politioneel informatierapport (RIR) van een maand voordien.

60 Benjamin Herman bevond zich op 13 maart 2017 nog in de gevangenis van Lantin en werd pas enkele dagen later naar Marche-en-Famenne overgeplaatst.

61 De VSSE stelde dat de resultaten van de besprekingen in het verleden voldoende werden afgedekt in de zeer frequente e-mailwisseling tussen de diensten, maar dat een verdere formalisering – in de vorm van een officieel verslag – recent tot de normale gang van zaken behoort.

Begin augustus 2017 was er tussen verschillende diensten – de VSSE, het DG EPI, DJSOC/Terro en het OCAD – weliswaar e-mailverkeer over een persoon X die zich in de gevangenis van Leuze (Henegouwen) bevond. De VSSE maakte hierop een analysenota over deze persoon X. Daarin werd ook Benjamin Herman vermeld en wordt er gesteld dat in zijn hoofde (summier) sprake is van onder andere radicalisering.[62] De dag van verzending van de nota vindt er een contact plaats tussen de VSSE en de Cel Extremisme, echter niet met betrekking tot Benjamin Herman maar met betrekking tot persoon X. In het daaropvolgende e-mailverkeer tussen de VSSE en het DG EPI komt Benjamin Herman wel ter sprake. Het DG EPI vraagt of de betrokkene – naast anderen – 'best op de CelEx-lijst wordt geplaatst', daarbij weliswaar opmerkend dat er sinds 2017 klaarblijkelijk geen verdere radicalisering meer was opgemerkt.[63] De VSSE antwoordt dat het DG EPI 'de administratieve beslissing zelf neemt, op basis van de door de VSSE aangereikte inlichtingen'. De VSSE voegt eraan toe dat ook wanneer personen niet op de CelEx-lijst staan, deze toch nog worden opgevolgd door de VSSE.

In de daaropvolgende overlegvergaderingen werd klaarblijkelijk niet meer op Benjamin Herman teruggekomen. Tot op het ogenblik dat hij eind mei 2018 de feiten pleegde, werd door de politie- en inlichtingendiensten niets nieuws meer vernomen.

I.3.5. DE EVALUATIE VAN HET PROTOCOL DG EPI/VSSE

Reeds in 2014 werd door het Vast Comité I een toezichtonderzoek opgestart naar de wijze waarop de VSSE het 'protocolakkoord tot regeling van de samenwerking tussen de Veiligheid van de Staat en het (toenmalige) Directoraat-generaal Uitvoering Straffen en Maatregelen' uitvoerde.[64] Het Vast Comité I kon op dat moment nog geen exacte cijfers over de uitwisseling van gegevens voorleggen. Het huidige onderzoek kon de intense contacten tussen beide diensten kwantitatief staven.[65]

---

62 De analysenota werd verzonden naar het DG EPI, DJSOC/Terro en het OCAD. In de nota wordt de CelEx-lijst niet vermeld.

63 Het opnemen van een gevangene op de CelEx-lijst heeft bepaalde gevolgen voor betrokkene. Het DG EPI moet de opname op de lijst dus nauwkeurig motiveren. Daarbij kan zich een probleem voordoen wanneer DG EPI ageert op basis van 'soft' informatie of informatie die geclassificeerd is en bijgevolg niet zomaar kan worden gebruikt om een beslissing te motiveren.

64 VAST COMITÉ I, *Activiteitenverslag 2016*, 57-62 ('De VSSE en het samenwerkingsprotocol met de strafinrichtingen').

65 Het aantal uitgaande mails van de VSSE naar de CelEx schommelde tussen januari 2017 en juni 2018 tussen de 100 en 270; het aantal binnenkomende mails voor dezelfde periode schommelde tussen de 200 en 450. Een stijgende lijn was voor beide fluxen merkbaar doorheen de tijd.

Uit het toenmalige onderzoek bleek dat er geen zware tekortkomingen of uitingen van ontevredenheid konden worden vastgesteld over de feitelijke samenwerking. Deze vaststelling kon worden bevestigd.

In zijn aanbevelingen wees het Comité erop dat er omzichtig moest worden omgesprongen met het gebruik van de diverse lijsten met de bedoeling ervoor te zorgen dat de finaliteit van deze lijsten duidelijk werd vastgesteld en gerespecteerd. Een belangrijke opmerking in verband met de wisselwerking tussen de lijsten van het DG EPI en van de VSSE, was de vaststelling dat de opname op de CelEx-lijst vaak tot gevolg had dat een gedetineerde hiervan op de hoogte was: hij ondervindt er immers de dagelijkse consequenties van. Dit bemoeilijkt een discrete opvolging door de VSSE.

Ook een uitwisseling van de informatie was bij de evaluatie van het protocol voorwerp van onderzoek en kwam opnieuw aan bod (in het bijzonder de verspreiding van ruwe informatie). De VSSE verspreidde de interne, operationele rapporten waarin Benjamin Herman ter sprake kwam, niet. De politiediensten deden dit wel met de door hen opgestelde RIR's terwijl die evenzeer ruwe informatie bevatten.[66]

I.3.6. CONCLUSIES VAN DE VASTE COMITÉS I EN P

I.3.6.1. Wat de informatiepositie van de diensten betreft

Er moet worden vastgesteld dat de informatie waarover de politie-, inlichtingen- en veiligheidsdiensten alsook het OCAD over Benjamin Herman beschikten, numeriek zeer beperkt, summier en weinig alarmerend was. De term 'radicalisering' komt in relatie tot Benjamin Herman voor het eerst (en meteen het laatst) voor in een operationeel rapport van de VSSE van februari 2017. De informatie is bijzonder summier; de target was immers niet Benjamin Herman, maar wel een andere persoon. Hijzelf vertoonde bepaalde religieuze gedragingen dewelke niet als extremistisch werden aangemerkt. Bekeringsijver (proselitisme) kon niet worden vastgesteld. Dat betrokkene, los van zijn criminele verleden van gemeen recht, een extremistische of terroristische dreiging zou vormen, kon niet worden afgeleid.

Indien Benjamin Herman inderdaad al plannen zou gehad hebben om tijdens zijn penitentiair verlof een aanslag te plegen, dan bleek dat niet uit de opvolging

66 De VSSE verspreidt enkel geanalyseerde informatie ('inlichtingen') op basis van de informatie die het zelf collecteert of die het van andere bronnen/partners verkrijgt. Niet elk collecterapport leidt automatisch en onmiddellijk tot een analysenota die aan de autoriteiten wordt gestuurd; de manier waarop de collecte-informatie in analysenota's wordt verwerkt en het tijdstip van het opmaken van een analysenota, hangt af van onder andere de kwaliteit van de ruwe informatie en de hoeveelheid ervan. In casu werd de informatie van de collectenota's inderdaad verwerkt in analysenota's en aldus verspreid.

van betrokkene door de diensten, noch vanuit de gevangenis. In de periode tot de aanslag kwam zijn naam niet meer naar boven.

Er zit weinig variatie in de informatie in het bezit van de politiediensten en de VSSE, en bijgevolg ook in de informatie die het OCAD van beiden verkreeg. Dit is te verklaren doordat de diensten een beperkt rechtstreeks zicht hebben op gedetineerden.

De verschillende lijsten – OCAD-lijst, CelEx-lijst, targetlijsten van gedetineerden van de VSSE – sluiten niet volledig op elkaar aan. Wel werd aangetoond dat de informatie werd gedeeld. De minister van Justitie gaf aan dat hij plannen ontwikkelde om de CelEx-lijst om te vormen en in de gemeenschappelijke gegevensbank van het OCAD op te nemen om aldus de verschillen tussen de lijsten weg te werken.[67]

I.3.6.2. Wat de uitwisseling van gegevens betreft

De verschillende diensten hadden elk afzonderlijk informatie over betrokkene en deelden deze met het OCAD. Daarbij viel een verschil op in de manier van werken tussen de politiediensten en de VSSE. De DJSOC van Federale Politie deelde de informatierapporten (RIR's) opgesteld door federale of lokale politiediensten mee aan het OCAD en dit na een interne kwaliteitscontrole, maar zonder er een analyse aan toe te voegen. De VSSE maakte de interne operationele rapporten (OR) van de collectediensten niet rechtstreeks over, maar analyseert deze en stuurt de verwerkte informatie (analysenota's) naar het OCAD. Het verschil heeft onder meer te maken met de verschillende logica en nagestreefde finaliteit van de documenten: de politionele logica waarbij de basisinformatie ongeschonden moet blijven *versus* de inlichtingenlogica waarbij de analyse en het samenleggen van informatie uit meerdere bronnen een hoofdrol speelt. De VSSE stuurde deze analysenota's ook naar de Federale Politie.

De informatie die het OCAD verkreeg, werd in de interne databank opgeslagen dewelke niet toegankelijk is voor andere diensten. Dit is wel het geval voor personen die in de gemeenschappelijke gegevensbank TF[68] of haatpropagandisten worden opgenomen, maar aangezien er in hoofde van Benjamin Herman geen verband kon worden gelegd met enige extremistische of terroristische dreiging, werd de informatie niet in deze databank verwerkt en was ze niet algemeen consulteerbaar.

---

67 Zie hierover het antwoord van de minister van Justitie in de Kamercommissie Justitie d.d. 20 juni 2018, waarin hij stelt dat '*een KB wordt opgesteld dat de CelEx-lijst zal opnemen in de gemeenschappelijke databank van het OCAD*', in *Parl. St.* Kamer, CRABV, 54, COM 930, 5. De VSSE suggereerde dat de herziening van het Actieplan Radicalisering in gevangenissen van maart 2015 hiervoor de aanzet kan vormen.

68 Zie hierover 'Hoofdstuk VI. De controle van de gemeenschappelijke gegevensbanken'.

Verder blijkt de wel zeer belangrijke positie en mogelijke rol van het DG EPI in het geheel van de inlichtingengaring over gevangenen.[69]

I.3.6.3. Wat betreft de rollen van de diensten

De Vaste Comités I en P zijn van mening dat de verschillende diensten hebben gehandeld zoals het hoort. De informatie waarover ze beschikten was schaars en weinigzeggend, maar werd wel uitgewisseld. Er kon niet uit worden afgeleid dat Benjamin Herman extreem-radicale of terroristische plannen had of een bedreiging van die aard vormde. Voor het OCAD was er geen aanleiding om over betrokkene een individuele dreigingsanalyse op te maken. Geen enkele dienst kon op basis van wat hij wist voorzien dat Benjamin Herman een aanslag zou plegen.

Het beheer van de CelEx-lijst door het DG EPI valt buiten de bevoegdheid van de Vaste Comités P en I, die er zich dan ook niet kunnen over uitspreken.

Alhoewel het niet tot het voorwerp van de toezichtonderzoeken behoorde, kregen de Vaste Comités P en I kennis van de interne nota die binnen de gevangenisadministratie drie dagen voor de feiten werd opgemaakt (25 mei 2018). De inhoud van deze nota bevestigde wat eerder werd vermeld. Ook in deze nota was niet Benjamin Herman de rechtstreekse target, maar wel (verschillende) andere personen. Benjamin Herman speelde geen hoofdrol, en er was geen enkele aanduiding van een extremistische of terroristische bedreiging of plan. De nota was enkel ter informatie bedoeld voor de gevangenisdirectie. Het was duidelijk dat zelfs indien deze nota vooraf door de andere diensten zou gekend zijn geweest, dit hoe dan ook niet had kunnen leiden tot de conclusie dat Benjamin Herman een bedreiging vormde of plannen had om een aanslag te plegen.[70]

I.4. DE INFORMATIEPOSITIE VAN HET OCAD VOORAFGAAND AAN DE AANSLAG IN LUIK

I.4.1. DE OPENING VAN EEN GEMEENSCHAPPELIJK TOEZICHTONDERZOEK

In de nasleep van de aanslag in Luik eind mei 2018 door Benjamin Herman[71], verzocht de parlementaire Begeleidingscommissie de Vaste Comités I en P tevens

69 De VSSE stelde dat het belang van CelEx niet voldoende kon worden benadrukt. De dienst pleitte reeds geruime tijd voor een versterking van CelEx, gekoppeld aan het aanwerven van 'lokale coördinatoren radicalisme'.

70 Het is duidelijk dat indien er niet de aanslag was geweest, er in principe en gelet op de inhoud geen reden zou geweest zijn om de VSSE speciaal op de hoogte te brengen van de inhoud van de nota.

71 Hierover 'I.3. De informatiepositie van de inlichtingendiensten voorafgaand aan de aanslag in Luik'.

een gemeenschappelijk onderzoek te voeren naar de informatiepositie van het OCAD.[72] De dienst werd volgende vragen voorgelegd:
- Welke informatie bezat het OCAD over de dader vóór 29 mei 2018 (tijdstip van de aanslag)? Was de dader als geradicaliseerde gekend? Welke informatie ontving het OCAD van zijn partners/steundiensten?
- Heeft het OCAD met zijn partners/steundiensten informatie uitgewisseld? Werd er over de dader informatie via een databank ter beschikking gesteld? Werd er over betrokkene overleg gepleegd?
- Heeft het OCAD over de dader een dreigingsevaluatie of risicoanalyse opgesteld?

De twee enquêtediensten begaven zich gezamenlijk naar het OCAD om na te gaan over welke informatie de dienst beschikte, en hadden tevens een onderhoud met de directeur en de leden van het coördinatieorgaan.

I.4.2. INFORMATIEBRONNEN

Er is enkel in de tussenkomst van het OCAD voorzien wanneer een gevangene hetzij in de gemeenschappelijke gegevensbank (GGB) wordt opgenomen (*(foreign) terrorist fighter, home grown terrorist* of haatprediker) of wanneer er elementen zijn – aangebracht door de steundiensten van het OCAD – die op een terroristische of extremistische dreiging wijzen die binnen de bevoegdheid van het OCAD valt.

Aangaande Benjamin Herman beschikte het OCAD slechts over beperkte informatie. Het betrof:
- drie informatierapporten (RIR's) van de federale gerechtelijke politie van Luxemburg (2015), de federale gerechtelijke politie van Luik (2016) en een laatste opgesteld door de politiezone Famenne-Ardenne (2017);
- twee analysenota's van de Veiligheid van de Staat (2017);
- het verslag van de *local task force* van Neufchâteau van maart 2017.[73]

Informatie afkomstig uit het gevangeniswezen, kan het OCAD via meerdere kanalen bereiken: rechtstreeks vanuit de gevangenissen – bijvoorbeeld tijdens de vergaderingen over de CelEx-gevangenen – of nog via andere berichten[74], maar ook onrechtstreeks via de politiediensten (in een RIR), hetzij via de VSSE (in een

72 Krachtens artikel 53, eerste lid, 6° van de Toezichtwet van 18 juli 1991 vervullen de Vaste Comités I en P gezamenlijk hun controleopdrachten betreffende het OCAD en diens steundiensten.

73 Een eerder LTF-verslag uit 2015 werd niet aan het OCAD verstuurd; het OCAD was op dat ogenblik enkel bestemmeling van relevante informatie met betrekking tot *foreign terrorist fighters*.

74 Bijv. e-mailberichten specifiek wanneer het om gevangenen op de CelEx-lijst gaat.

analysenota), hetzij via een LTF[75] … Op het ogenblik van het onderzoek was het DG EPI nog geen steundienst van het OCAD.[76, 77]

I.4.3. DE BIJ HET OCAD BESCHIKBARE INFORMATIE

De Comités konden vaststellen dat de informatie waarover het OCAD kon beschikken, identiek was aan deze van de politie- en inlichtingendiensten. Daarin kwam Benjamin Herman nooit 'rechtstreeks' voor, maar steeds in relatie tot en in de marge van andere personen die meer direct de aandacht van de diensten hadden getrokken. Over de inzichten van de dader was er, behoudens het feit dat hij een praktiserend moslim was (in de zin dat hij deelnam aan gebeden), niets bekend. Het OCAD kon uit de beschikbare gegevens niet afleiden dat hij een dreiging vormde of zou kunnen vormen.

Wel werd Benjamin Herman als entiteit opgenomen in de interne databank van het OCAD, waarin bovenvermelde documenten werden opgenomen. Deze databank is evenwel niet toegankelijk voor andere diensten.[78] Zoals opgemerkt (I.3), sluiten de verschillende lijsten (OCAD-lijst, CelEx-lijst, targetlijsten met gedetineerden van de VSSE) niet volledig op elkaar aan.

De beschikbare informatie bevatte geen afdoende elementen die beantwoorden aan vastgestelde criteria voor de opname van betrokkene in de gemeenschappelijke gegevensbank en waarvan het OCAD de operationeel beheerder is (de geconsolideerde databank *terrorist fighters* en haatpropagandisten). Om dezelfde reden maakte het OCAD geen interne documenten op met betrekking tot Benjamin Herman, en ook geen dreigingsanalyse. Beide Comités konden zich hierin vinden en concludeerden dat de informatie niet van die aard was dat een dreigingsanalyse zich opdrong. Het gegeven uit 2017 over de radicalisering van

---

75 Het OCAD merkte op dat het, net als de DJSOC/Terro en de VSSE, rechtstreeks informatie en vragen vanuit het DG EPI kreeg, conform de afspraken die zijn gemaakt tussen deze diensten in de Werkgroep Gevangenissen. Het OCAD komt evenwel niet tussen in zaken die raken aan de operationele bevoegdheden van de betrokken diensten.

76 Het Koninklijk besluit van 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 (*BS* 12 september 2018) bracht daar verandering in.

77 Er is geen gegarandeerde feedback naar het DG EPI toe: indien de politiediensten of de VSSE intern of extern (bijvoorbeeld naar OCAD) over een gevangene rapporteren of berichten, dan weet het DG EPI dat niet noodzakelijkerwijze, noch weet het DG EPI of de door hem gegeven informatie op een of andere manier tot iets geleid heeft.

78 Indien de gemeenschappelijke gegevensbank zou worden uitgebreid en er ook personen zouden worden in opgenomen die '*in de gevangenis radicaliseren en mensen die na een veroordeling wegens terreur de gevangenissen verlaten*', zoals klaarblijkelijk het plan is van de ministers van Justitie en van Binnenlandse Zaken (Zie antwoord van de minister van Justitie, *Parl. St.* Kamer, CRAVB, 54, COM 910 d.d. 4 juni 2018, 34), dan zou dit euvel uit de weg worden geholpen en zouden ook diensten extern aan het OCAD deze informatie kunnen raadplegen.

betrokkene[79], was te summier om ermee aan het werk te gaan en sindsdien had Benjamin Herman de aandacht niet meer getrokken.

I.5. DE VERMEENDE TOEZEGGING DOOR EEN INLICHTINGENDIENST AAN EEN DERDE

In 2018 ontving het Vast Comité I een klacht waarbij de betrokkene beweerde dat hem een bepaalde toezegging was gedaan als informant. Daarop deed het Comité de vereiste verificaties bij de betrokken inlichtingendienst. Het Comité concludeerde dat geen enkel bewijs kon worden gevonden van een dergelijke toezegging.

I.6. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2018 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2018 WERDEN OPGESTART

I.6.1. INTERNATIONALE GEGEVENSUITWISSELING OVER *FOREIGN TERRORIST FIGHTERS*

Al in 2016 werd, tijdens een internationale vergadering met verschillende Europese toezichthouders[80], beslist een gelijkaardig toezichtonderzoek op te starten in alle deelnemende landen over de internationale samenwerking tussen de diverse inlichtingendiensten met betrekking tot de strijd tegen de *foreign terrorist fighters* (FTF). Dit initiatief kreeg nadien de uitdrukkelijke steun van de voorzitter van de Begeleidingscommissie. Het ligt daarbij in de bedoeling dat elke toezichthouder, met zijn eigen perspectief en bevoegdheid maar vanuit eenzelfde filosofie en met een zekere gemeenschappelijke aanpak, dit thema bestudeert.

Het opzet van het Belgische luik van het onderzoek[81] bestaat erin om een zo duidelijk en volledig mogelijk beeld te krijgen op de formele (maar ook informele) bilaterale of internationale informatie-uitwisseling tussen de VSSE en de ADIV enerzijds en buitenlandse diensten, werkgroepen of samenwerkingsverbanden anderzijds en dit met betrekking tot de problematiek van de FTF.

---

79 Zie 'I.3. De informatiepositie van de inlichtingendiensten voorafgaand aan de aanslag in Luik'.

80 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.

81 Het onderzoek werd opgestart eind augustus 2016, nadat het initiatief eerder werd voorgelegd aan en goedgekeurd door de Begeleidingscommissie van de Kamer van Volksvertegenwoordigers.

De uiteindelijke finaliteit van het onderzoek is te komen tot een beoordeling over de informatie-uitwisseling en desgevallend tot aanbevelingen om deze te optimaliseren zodat de informatiepositie van de betrokken diensten kan worden verbeterd, zonder dat daarbij de fundamentele rechten van de burger worden uitgehold.

De afgelopen drie jaar werd regelmatig samengekomen om methoden, *best practices*, juridische en praktische problemen te bespreken en de ervaringen in de nationale onderzoeken uit te wisselen. Er werden daarbij geen geclassificeerde gegevens gedeeld. Begin november 2018 werd door de deelnemende toezichtorganen een gemeenschappelijke verklaring en perscommuniqué opgesteld.[82] Het Belgische luik van het onderzoek werd afgerond begin 2019.

I.6.2. DE UITVOERING VAN VEILIGHEIDSSCREENINGS DOOR 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.

De rol die de inlichtingendiensten spelen in het kader van betrouwbaarheidsonderzoeken is niet altijd dezelfde. Soms beperkt deze zich tot het doorgeven aan andere overheden van persoonsgegevens die ze in hun bezit hebben. Soms gaan ze actief op zoek naar bijkomende gegevens. Soms verlenen ze een gemotiveerd advies en in enkele specifieke gevallen nemen ze (alleen of als onderdeel van een veiligheidsoverheid) ook de uiteindelijke beslissing omtrent het al dan niet toekennen of intrekken van de vergunning of toelating.

In casu lag een klacht aan de oorsprong van het toezichtonderzoek. Een medewerker op de nationale luchthaven van Brussel zag zijn toegangsbadge ingetrokken na een negatief advies[83] van de Nationale Veiligheidsoverheid (NVO). Hij diende beroep in bij het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen alsook een beroep tot nietigverklaring en tot schorsing voor de Raad van State. Het Beroepsorgaan verklaarde de klacht onontvankelijk – want ingediend tegen de beslissing van de FOD Mobiliteit en Transport en niet tegen het advies van de NVO. Ook de Raad van State verwierp de klacht. Daarop richtte de klager zich naar het Vast Comité I, zonder evenwel het voorwerp van klacht te definiëren. Hij verklaarde niet te begrijpen waarom een negatief advies werd genomen waardoor hij zijn werk verloor alsook zijn pilotenlicentie geschorst zag.

---

82 Zie bijlage D. 'Versterking van het toezicht op de internationale gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten'.

83 Dat luidde als volgt: *'overwegende dat betrokkene contacten met een radicale familiale omgeving heeft; overwegende dat die contacten een mogelijk veiligheidsrisico met zich meebrengen'*.

Het Comité achtte het legitiem om, vertrekkende vanuit die individuele klacht, een breder toezichtonderzoek te openen naar de wijze waarop de inlichtingendiensten veiligheidsscreenings uitvoeren.[84]

Omwille van andere prioriteiten, konden de eerste onderzoeksverrichtingen pas worden opgestart eind 2017. Van januari tot mei 2018 werden interviews georganiseerd met de verantwoordelijken van de secties die bij beide inlichtingendiensten de veiligheidsscreenings behandelen, alsook met enkele van hun medewerkers. De interviews vonden plaats in meerdere sessies, waarbij bijkomende verduidelijkingen en bijzonderheden werden verschaft. Er vond tevens een omstandige juridische analyse plaats van de voor dit onderzoek relevante wetgeving, en er werden cijfergegevens en documenten bij de diensten opgevraagd.

In november 2018 werd aan zowel de VSSE als de ADIV een ontwerpverslag toegezonden; in december ontving het Comité opmerkingen van de diensten en paste op basis hiervan zijn verslag aan waar nodig. Het toezichtonderzoek werd in maart 2019 gefinaliseerd.

I.6.3. 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.[85] De kerntaak bestaat er in punctuele of strategische evaluaties te maken. Deze taak berust bij analisten en bij – vanuit de zogenaamde 'ondersteunende diensten' gedetacheerde – experten. De ondersteunende diensten vormen voor het coördinatieorgaan de belangrijkste informatiebron. Het zijn de VSSE, de ADIV, de geïntegreerde politie, de Administratie der Douane en Accijnzen van de FOD Financiën, de Dienst Vreemdelingenzaken van de FOD Binnenlandse Zaken, de FOD Mobiliteit en Vervoer en de FOD Buitenlandse Zaken (art. 2, 2° W.OCAD). Het betreft zeer uiteenlopende diensten, elk met een eigen cultuur en grootte.

---

84 'Toezichtonderzoek over de manier waarop de VSSE en de ADIV veiligheidsverificaties uitvoeren, de gegevens evalueren nodig bij het toekennen van veiligheidsattesten of het formuleren van veiligheidsadviezen, dit in toepassing van artikelen 22*bis* tot 22*sexies* van de Wet van 11 december betreffende de classificatie en de veiligheidsmachtigingen, -attesten en –adviezen (W.C&VM)'. Het onderzoek werd geopend op 13 februari 2017.

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

Eerder, in 2010, voerde het Vast Comité I samen met het Vast Comité P een gemeenschappelijk toezichtonderzoek uit naar de informatiestromen tussen het OCAD en de ondersteunende diensten, met bijzondere aandacht voor de twee inlichtingendiensten en de Federale en Lokale Politie.[86]

Op de gemeenschappelijke plenaire vergadering van december 2017 werd besloten een toezichtonderzoek te openen naar de 'andere' ondersteunende diensten.[87] 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 vier[88] overige ondersteunende diensten en dit aan de hand van een uitgebreide bevraging.

In de loop van 2018 werden diverse onderzoeksverrichtingen uitgevoerd. Zo vonden op basis van een gestructureerde, omstandige vragenlijst onder meer interviews plaats met de bij het OCAD gedetacheerde vertegenwoordigers van de Dienst Vreemdelingenzaken (FOD Binnenlandse Zaken), de FOD Mobiliteit, de FOD Buitenlandse Zaken alsook de Administratie der Douane en Accijnzen (FOD Financiën). Ook de *points of contact* bij de diverse steundiensten zelf, werden bevraagd. Op diverse momenten vond overleg met de onderzoeksequipe van het Vast Comité P plaats.

Het gemeenschappelijk toezichtonderzoek zal worden gefinaliseerd in de tweede helft van 2019.

I.6.4. DE WERKING VAN DE AFDELING I/H VAN DE ADIV DOORGELICHT

Een gerechtelijk onderzoek van het Federaal Parket, op het terrein gevoerd door de Dienst Enquêtes van het Vast Comité I, brachten een aantal structurele dysfuncties aan het licht bij de werking van de Afdeling I/H (*Human intelligence*) van de ADIV. Deze afdeling vormt een onderdeel van de Directie I(intelligence) van de militaire inlichtingendienst en heeft als opdracht om netwerken van bronnen en informanten op te richten ten einde de ADIV toe te laten inlichtingen te verza-

86 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').

87 Toezichtonderzoek betreffende de ondersteunende diensten van het OCAD met uitsluiting van de geïntegreerde politie en de inlichtingendiensten.

88 Gemotiveerd vanuit de noodzaak om zo snel als mogelijk een regeling voor de informatiestromen vanuit betrokken diensten aan het OCAD en omgekeerd tot stand te brengen, werden 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) toegevoegd als 'steundienst' (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. Deze steundiensten vielen buiten de scope van het onderzoek.

melen over buitenlandse fenomenen. Een aantal van die dysfuncties werden reeds in de loop van een eerder toezichtonderzoek aangekaart.[89] Onder meer de opdrachtsomschrijving, het strategisch beheer, de vaardigheden en kwaliteit van het personeel, de *tradecraft* … werden daarbij geproblematiseerd. Ook in het onderzoek naar de werking van de Directie Counterintelligence (I.1), 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 elkaar zouden kunnen gaan tegenwerken.

Begin mei 2018 werden respectievelijk de Voorzitter van de Begeleidingscommissie, de minister van Defensie en de ADIV op de hoogte gebracht van het openen van een '*toezichtonderzoek naar de werking van de dienst 'I/H' van de ADIV*'.

Snel volgde een eerste algemene briefing met aansluitend tal van onderzoeksverrichtingen. Het onderzoek werd verder gezet in 2019.

I.6.5. DE INFORMATIEPOSITIE VAN DE INLICHTINGENDIENSTEN OVER DE PAKISTAANSE KERNWETENSCHAPPER KAHN

Halfweg januari 2018 verschijnt een persartikel[90] 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. Op initiatief van een parlementslid gaf de Begeleidingscommissie van de Kamer op 12 juni 2018 aan het Vast Comité I de opdracht de thematiek te bestuderen. Op 2 juli werd het '*toezichtonderzoek 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.

In de tweede helft van 2018 werden diverse onderzoeksopdrachten uitgevoerd. Het onderzoek werd begin 2019 afgerond.

---

89 Zie VAST COMITÉ I, *Activiteitenverslag 2017*, 4-11 ('II.1. Een klacht over drie operaties van de ADIV').

90 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.

I.6.6. PUIGDEMONT EN DE MOGELIJKE ACTIVITEITEN DOOR BUITENLANDSE INLICHTINGENDIENSTEN IN BELGIË

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.[91] 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 geolokalisatie-baken, 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.

In de tweede helft van 2018 werden diverse onderzoeksopdrachten uitgevoerd. Ook dit onderzoek werd begin 2019 afgerond.

---

91 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).*

HOOFDSTUK II
DE CONTROLE OP DE BIJZONDERE EN BEPAALDE GEWONE INLICHTINGENMETHODEN

Dit hoofdstuk bevat nadere cijfers over de inzet door de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) van de 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.

II.1. CIJFERS MET BETREKKING TOT DE BIJZONDERE EN BEPAALDE GEWONE METHODEN

Tussen 1 januari en 31 december 2018 werden door de twee inlichtingendiensten samen 2445 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 2315 door de VSSE (waarvan 1971 specifieke en 344 uitzonderlijke) en 130 door de ADIV (waarvan 102 specifieke en 28 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

Het totaal aantal ingezette methoden steeg in 2018 met meer dan 25% (van 1923 naar 2445). De vastgestelde stijging is vooral te wijten aan de sterk toegenomen inzet van bijzondere methoden door de VSSE. Hierbij springt voornamelijk de toename van de uitzonderlijke methoden in het oog. Ook de ADIV deed in 2018 meer beroep op bijzondere inlichtingenmethoden. De dienst komt daardoor opnieuw aan het cijfer van een aantal jaren voordien.

Hetzelfde beeld zien we bij de gewone methoden van vorderingen gericht aan operatoren om bepaalde communicatiemiddelen te identificeren. De VSSE formuleerde 6482 vorderingen, hetgeen een forse toename betekent. Bij de ADIV is er bijna sprake van een verdubbeling.

	Vorderingen door ADIV	**Vorderingen door VSSE**
2016	216	2203
2017	257	4327
2018	502	6482

In zijn vorig jaarverslag stelde het Comité hierover het volgende: '*Los van het feit dat het quasi onmogelijk is om de cijfers inzake identificaties over de jaren heen te vergelijken, kan het Comité niet om de vaststelling heen dat er sinds de invoering van de versoepelde procedure ex artikel 16/2 W.I&V veel meer identificaties worden verricht. Vanuit zijn algemene toezichtsbevoegdheid zal het Comité aan de VSSE vragen om intern te onderzoeken in welke mate dit hoge aantal vorderingen (mede) wordt veroorzaakt door het versoepelen van de procedure. Daarbij moet o.m. aandacht worden besteed aan de aard van dreigingen die de vorderingen rechtvaardigden en aan de vraag of en in welke mate dergelijke vorderingen gebeuren op verzoek van buitenlandse overheden/partnerdiensten.*'[92] Tegenover zijn parlementaire Begeleidingscommissie herhaalde het Comité dit voornemen.[93] Het Comité bekwam echter geen (ADIV) – of geen afdoend (VSSE[94]) antwoord op zijn vragen ter zake. Daarom heeft het besloten deze thematiek op te nemen in zijn in 2019 geopende *'toezichtonderzoek naar de toepassing en de interne controle door de*

92 VAST COMITÉ I, *Activiteitenverslag 2017*, 42.

93 *Parl. St.* Kamer 2018-19, nr. 54K3375/001 (Activiteitenverslag 2017 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).

94 Naar luid van de VSSE was de toename slechts gedeeltelijk te verklaren door een versoepeling van de procedure door de wetgever. Het aantal aanvragen was tevens hoger omdat ze meer resultaten opleverden (o.m. door het opheffen van het anonieme karakter van de prepaidkaarten). Als laatste reden werd aangehaald dat – alhoewel deze aanvragen niet onder art. 16/2 W.I&V vallen – er voor het opvolgen van targets in *social media* eenzelfde format wordt gehanteerd waardoor deze aanvragen (helaas) ook in de statistieken terechtkomen. De VSSE specifieerde ten slotte dat het aantal aanvragen door vragen van buitenlandse partnerdiensten niet was vermeerderd in verhouding tot het totaal van de aanvragen.

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.'

In wat volgt, beperkt het Comité zich 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.

II.1.1. METHODEN AANGEWEND DOOR DE ADIV

II.1.1.1. Gewone methoden

Identificatie van de gebruiker van telecommunicatie

Bij Wet van 5 februari 2016 werd – in navolging van de aanbevelingen van het Vast Comité I[95] – de identificatie van de gebruiker van telecommunicatie (bijv. gsm-nummer of IP-adres) of van een gebruikt communicatiemiddel, als een gewone methode beschouwd in de mate waarin dit gebeurt via een vordering aan of een rechtstreekse toegang tot de klantenbestanden van een operator. Voorheen vormde dit een specifieke methode. De wijziging gebeurde door de invoeging van een nieuw artikel 16/2 in de Wet van 30 november 1998.[96] De regeling voorziet in een verplichting voor de VSSE en de ADIV om een register bij te houden van alle gevorderde identificaties en van alle via rechtstreekse toegang verkregen identificaties. Er werd ook bepaald dat het Comité maandelijks een lijst van de gevorderde identificaties en van elke toegang moet ontvangen. In de praktijk krijgt het Comité maandelijks alleen het aantal vorderingen. Ook dit item zal worden bestudeerd in het in 2019 geopende toezichtonderzoek (*supra*).

Identificatie van prepaid-kaarthouder

Daarnaast werd bij Wet van 1 september 2016 (*BS* 7 december 2016) een nieuwe gewone methode ingevoerd in datzelfde artikel 16/2 W.I&V: '§ 2. *De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een bank of financiële instelling om over te gaan tot het identificeren van de eindgebruiker van de in artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie bedoelde voorafbetaalde kaart, op basis van de referentie van een elektronische banktransactie die verband houdt met de voorafbetaalde kaart en die voorafgaand meegedeeld is door een operator of verstrekker in toepassing van paragraaf 1.*' De VSSE en de ADIV moeten – net zoals bij

95 VAST COMITÉ I, *Activiteitenverslag 2012*, 69.

96 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).

de identificatie van de gebruiker van telecommunicatie of van een gebruikt communicatiemiddel – een register bijhouden van alle gevorderde identificaties.

Toegang tot PNR-gegevens

Bij Wet van 25 december 2016 (*BS* 25 januari 2017) 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).[97] Het Comité wordt in kennis gesteld van de aanwending van deze methode en kan ze desgevallend verbieden.[98]

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).

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).[99] Bij gebrek aan een uitvoeringsbesluit is deze bepaling nog niet in werking getreden.[100]

De cijfers

Gewone methoden (ADIV)	**Aantal toelatingen**
Identificatie van de gebruiker van telecommunicatie	502
Identificatie van prepaid-kaarthouder	0
Gerichte opzoekingen PNR-gegevens	18
Doorgifte PNR-gegevens o.b.v. hits	Niet aangeleverd
Gebruik van politionele camerabeelden	Niet in werking

97 Zie tevens het protocolakkoord d.d. 13 november 2018 betreffende de samenwerking tussen de Passagiersinformatie-eenheid en de ADIV in het kader van de wet betreffende de verwerking van de passagiersgegevens (Beperkte verspreiding, art. 20 K.B. 24 maart 2000).

98 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.

99 Bij dezelfde wet werd de bestaande specifieke en uitzonderlijke observatiemogelijkheid uitgebreid (artt. 18/4 § 3 en 18/11 § 3 W.I&V).

100 Begin 2019 keurde de Ministerraad ter zake een ontwerp van KB 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).

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)[101]	8
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)	1
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;)	5
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8 W.I&V)	45
Kennisnemen van lokalisatiegegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator (art. 18/8 W.I&V)	43
TOTAAL	102

[101] 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.

II.1.1.3. De uitzonderlijke methoden

De ADIV machtigde in het kader van zijn opdrachten bedoeld in de artikelen 11, § 1, 1° tot 3° en 5°, en § 2 W.I&V volgende uitzonderlijke methoden:

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)[102]	0
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)	1
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)	1
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	12
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	1
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	13
TOTAAL	28

II.1.1.4. De opdrachten en de dreigingen die de inzet van de gewone en bijzondere methoden rechtvaardigen[103]

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 kun-

[102] 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.

[103] Per toelating kunnen meerdere opdrachten en dreigingen aan de orde zijn.

nen 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).**

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).

In acht genomen dat per toelating verschillende dreigingen aan de orde kunnen zijn, werden onderstaande cijfers opgetekend:

AARD VAN DE OPDRACHT	AANTAL 2018
Inlichtingenopdracht	18
Militaire veiligheid	19
Bescherming geheimen	4
Activiteiten buitenlandse diensten in België opvolgen	89

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 2018
Spionage	85
Terrorisme (en radicaliseringsproces)	26
Extremisme	1
Inmenging	18
Criminele organisatie	–
Andere	0

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.[104] Dit gebeurde vooralsnog niet; het Comité herhaalt dan ook zijn aanbeveling.

104 VAST COMITÉ I, *Activiteitenverslag 2017*, 43.

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	6482
Identificatie van prepaid-kaarthouder	0
Gerichte opzoekingen PNR-gegevens)	7
Doorgifte PNR-gegevens o.b.v. hits	Niet aangeleverd
Gebruik van politionele camerabeelden	Niet in werking

Zoals gezegd, zal het Comité de wijze waarop deze methoden worden 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)	236
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)	1
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)	81
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;)	55
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8 W.I&V)	822
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator (art. 18/8 W.I&V)	776
TOTAAL	1971

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)	13
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)	25
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)	5
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	80
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	40
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	181
TOTAAL	344

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 2018
Spionage	815
Terrorisme (en radicaliseringsproces)	1159
Extremisme	312
Proliferatie	5
Schadelijke sektarische organisaties	0
Inmenging	24

AARD DREIGING	AANTAL 2018
Criminele organisaties	0
Activiteiten buitenlandse diensten in België opvolgen	(inbegrepen in bovenstaande cijfers)
TOTAAL	2315

Bovenstaande cijfers tonen aan dat 'terrorisme', wat betreft de inzet van BIM-methoden, de absolute prioriteit blijft voor van de VSSE.

De bevoegdheid van de VSSE wordt niet alleen bepaald door de aard van de dreiging. De dienst mag slechts optreden ter vrijwaring van welbepaalde belangen:

1. De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde zijnde,
   a) de veiligheid van de instellingen van de Staat en het vrijwaren van de 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.

AARD BELANG	AANTAL 2018
De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde	106
De uitwendige veiligheid van de Staat en de internationale betrekkingen	10
De inwendige en uitwendige veiligheid van de Staat samen	1375
De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel	3
Activiteiten van buitenlandse inlichtingendiensten	821
TOTAAL	2315

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.[105] Gelet op andere prioriteiten werd hier van afgezien. 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.'*

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 2018 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[106] en een *a posteriori*-controle.[107] Aangezien de inlichtin-

105 VAST COMITÉ I, *Activiteitenverslag 2017*, 25 voetnoot 40.

106 '*De beoordelingscriteria bedoeld in het eerste lid, 2°, worden voorafgaandelijk aan het Vast Comité I voorgelegd*.'

107 *'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*

gendiensten 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.[108]

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 Privacycommissie/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 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 onderzoeks-gerech-

verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.'

108 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 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.

ten of de strafrechters. Strikt genomen treedt het Comité alsdan niet op als jurisdictioneel orgaan.

WIJZE VAN VATTING	2013	2014	2015	2016	2017	2018
1. Op eigen initiatief	16	12	16	3	1	1
2. Privacycommissie / Gegevensbeschermingsautoriteit	0	0	0	0	0	0
3. Klacht	0	0	0	1	0	0
4. Schorsing door BIM-Commissie	5	5	11	19	15	10
5. Toelating minister	2	1	0	0	0	0
6. Prejudicieel adviesverlener	0	0	0	0	0	0
TOTAAL	**23**	**18**	**27**	**23**	**16**	**11**

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);
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 waar-

van 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	2013	2014	2015	2016	2017	2018
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	0	3	2	1	0	0
4. Bijkomende informatie van BIM-Commissie	0	0	0	0	0	0
5. Bijkomende informatie van inlichtingendienst	0	1	1	4	0	0
6. Onderzoeksopdracht Dienst Enquêtes	50	54	48	60	35	52
7. Horen BIM-Commissieleden	0	0	2	0	0	0
8. Horen leden inlichtingendiensten	0	0	2	0	0	0
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	9	3	3	6	9	4
12. Gedeeltelijke stopzetting methode	5	10	13	4	6	6

AARD VAN DE BESLISSING	2013	2014	2015	2016	2017	2018
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	2	0	4	11	0	0
14. Onbevoegd	0	0	0	0	0	0
15. Wettige toelating / Geen stopzetting methode / Ongegrond	7	4	6	2	1	1
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 2018 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;
- 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;
- De gevolgen van een onwettig(e) (uitgevoerde) methode.

Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode: voorafgaande beslissing van het diensthoofd en kennisgeving BIM-Commissie

Een methode zonder voorafgaande beslissing

In dossier 2018/7250 had de betrokken inlichtingendienst bij een interne controle zelf vastgesteld dat er een onregelmatigheid had plaatsgevonden: er was een vordering voor identificatie- en lokalisatiegegevens gezonden naar een *provider* zonder dat er een beslissing door het diensthoofd was genomen. Daarenboven had de methode betrekking op een journalist zodat de BIM-Commissie haar voorafgaand advies had moeten verlenen. De BIM-Commissie, die op de hoogte werd gebracht, schorste de methode en het Comité bevestigde deze beslissing en liet de door de vordering gecollecteerde gegevens vernietigen.

Geen beslissing van het diensthoofd

Een inlichtingendienst wenste een bepaalde specifieke methode voor een duur van twee maanden in te zetten vanaf een welbepaalde datum. Een agent van die

dienst wijzigde echter de begindatum door die een paar dagen eerder te situeren. Het Comité besloot '*que les "rectifications" effectuées par un agent de la VSSE n'ont pas été contresignées par l'administrateur général lui-même et n'ont en conséquence aucune valeur légale*'.[109] De gegevens die werden ingewonnen vóór de door het diensthoofd voorziene startdatum, waren dus onwettelijk. Daarenboven werd de methode niet automatisch stopgezet op het einde van de voorziene termijn; de methode werd nog twee dagen aangehouden. Ook die gegevens waren niet wettelijk verkregen (2018/6794).

Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging

Gebrek in de motivering van de beslissing

Wanneer de betrokken inlichtingendienst de BIM-Commissie meldt dat een gedeelte van de initieel vermelde motivering van een specifieke methode niet met de werkelijkheid overeenstemde, herziet de commissie haar eerder genomen beslissing en schorst zij de methode (dossier 2018/7684). Het Comité stelde op zijn beurt vast dat de motivering van de kwestieuze BIM-beslissing tal van onjuistheden bevatte. '*Dat de onjuistheden in de motivering van die aard zijn dat zij de motivering zelf fundamenteel en ernstig aantasten. Aangezien daardoor moet worden vastgesteld dat niet is voldaan aan artikel 18/3 W.I&V, dat onder andere stelt dat de beslissing van het diensthoofd de feitelijke omstandigheden die de specifieke methode rechtvaardigen (…) moet vermelden. […] Aangezien de motiveringsverplichting is voorgeschreven op straffe van een onwettigheid.*' De ingewonnen gegevens dienden dan ook te worden vernietigd.

Een verkeerd voorwerp

In dossier 2018/7167 bleek de inlichtingendienst per vergissing een verkeerd telefoonnummer te hebben vermeld, zowel in de beslissing als in de vordering aan de operator. De dienst merkte dit zelf op, schorste de methode en verwittigde de BIM-Commissie. Deze schorste op zijn beurt de methode, waarop het Comité besloot tot de vernietiging van de onwettelijk bekomen gegevens.

De duur van een maatregel

Een inlichtingendienst wenste over te gaan tot de kennisname van communicatie- en lokalisatiegegevens voor een periode van exact één jaar (dossier 2018/7464).

---

109 '*dat de 'rechtzettingen' die werden aangebracht door een agent van de VSSE niet werden ondertekend door de administrateur-generaal zelf en bijgevolg geen enkele wettelijke waarde hebben*'. (vrije vertaling)

Gelet op de aard van de dreiging was dit de maximaal toegelaten periode. Maar de wet bepaalt dat dit jaar geldt te rekenen vanaf de beslissing van het diensthoofd (art. 18/8 § 2, eerste lid, 3° W.I&V). De begindatum is dus niet zomaar vrij te kiezen indien men over gegevens van een volledig jaar wil beschikken. Gevolg was dat de methode moest 'ingekort' worden zodat het begin zich situeerde bij de beslissing van het diensthoofd en het einde precies één jaar voordien.

In dossier 2018/7493 stelde zich identiek hetzelfde probleem: een inlichtingendienst wenste informatie te bekomen over een telefoonnummer en dit voor een termijn van negen maanden. Gelet op de dreiging (spionage) was die termijn toegelaten. Alleen moest deze gerekend worden vanaf de genomen beslissing (art. 18/8 § 2, 2°, W.I&V). De dienst had dit nagelaten zodat het vergaren van telefoniegegevens gedurende een periode van zes dagen niet door een wettige methode was gedekt.

In een ander dossier (2018/7470) was het probleem dat de beslissing zelf niet expliciet vermeldde voor welke termijn men bepaalde gegevens wou bekomen. '*[Q]ue la méthode précise une période en se référant à la période d'une autre méthode*'.[110] In die andere BIM-methode was wel een periode bepaald zodat het Comité zekerheid had over de voorgenomen duur. Daarenboven is de vermelding van de termijn niet op straffe van nietigheid voorgeschreven: '*Considérant qu'en vertu de l'art. 18/3, § 2, alinéa 1er, 5° de la L.R&S, la décision du dirigeant du service mentionne la période pendant laquelle la méthode spécifique peut être appliquée, à compter de la notification de la décision à la Commission; Considérant cependant que seules les mentions visées aux 1° à 4°, 7°, 9°, 10°, 11° et 14° de l'article 18/3, § 2, alinéa 1er, de la L. R&S sont prescrites sous peine d'illégalité*'[111]; De methode was dan ook wettig, doch het Comité voegde volgende bedenking toe:'*Considérant, in fine, que le procédé consistant à ne pas mentionner de période propre à la méthode, mais à faire référence à celle d'une autre méthode en cours, non simultanée de surcroit, ne permet pas au Comité permanent R de contrôler de facto, d'une part, le principe de proportionnalité devant être respecté pour toute méthode et, d'autre part, le respect de l'article 18/8 de la L. R&S; Considérant que le procédé critiqué nuit par conséquent au principe général de bonne administration et doit être évité*'.[112]

---

110 *'Dat de methode een termijn preciseerde door te verwijzen naar de termijn van een andere methode'*. (vrije vertaling)

111 '*Overwegende dat krachtens art. 18/3, § 2, eerste lid, 5°, W.I&V, de beslissing van het diensthoofd de periode vermeldt gedurende dewelke de specifieke methode mag worden toegepast, te rekenen vanaf de kennisgeving van de beslissing aan de Commissie; Overwegende evenwel dat enkel de in 1° tot 4°, 7°, 9°, 10°, 11° en 14° van artikel 18/3, § 2, eerste lid W.I&V bedoelde vermeldingen op straffe van nietigheid zijn voorgeschreven*; (vrije vertaling).

112 *'Overwegende, in fine, dat het procédé bestaande uit het niet vermelden van de periode eigen aan de methode, maar het verwijzen naar deze van een andere, bovendien niet gelijklopend, lopende methode het Comité niet toelaat de facto enerzijds het proportionaliteitsprincipe dat moet voldaan zijn bij elke methode, en anderzijds de naleving van artikel 18/8 W.I&V, te controleren;*

Het voorwerp van de methode

Het hierboven beschreven dossier 2018/7464 vertoonde nog een andere lacune. De beslissing maakte geen melding van het gsm-nummer waarop de methode betrekking zou hebben. '*Considérant qu'en vertu de l'art. 18/3, § 2, alinéa 1er, 2° de la L. R&S, la décision du dirigeant du service doit mentionner, sous peine d'illégalité, l'objet sur lequel la méthode spécifique peut être appliquée; qu'en l'espèce, l'objet n'est pas mentionné*'.[113]

Wettelijkheid van de uitvoering van een wettige methode

Verschil tussen de beslissing van het diensthoofd en de vordering

In vier beslissingen bleek de toelating van het diensthoofd om een specifieke of uitzonderlijke methode in te zetten volkomen wettig, maar stelde er zich een probleem op het vlak van de uitvoering in die zin dat de vordering van de gegevens niet conform was aan het initiële mandaat.

Zo had de BIM-Commissie in dossier 2018/6951 opgemerkt dat er een verschil was tussen de beslissing van het diensthoofd om tot een kennisname van communicatiemiddelen over te gaan en de eigenlijke vordering aan de operator: beide documenten viseerden gedeeltelijk een andere periode. Het Comité besliste dan ook dat de gegevens die betrekking hadden op de dagen die niet vervat lagen in de initieel voorziene periode, onwettelijk waren verkregen.

Ook in dossier 2018/7107 was een verschil tussen de beslissing van het diensthoofd en de vordering aan de operator aan de orde. Ook hier besliste het Comité dat alle verzamelde gegevens die buiten de beslissing van het diensthoofd vielen, dienden vernietigd te worden.

In dossier 2018/7769 machtigde het diensthoofd de collecte van gegevens van een bepaald bankrekeningnummer. De navolgende vordering aan de bankinstelling was echter veel ruimer: de dienst vorderde alle bankrekeningnummers, bankkluizen en financiële instrumenten van de target. Het Comité stelde dan ook vast dat alleen de vordering van de gegevens van het bankrekeningnummer wettig was.

In het kader van een specifieke methode ontving een inlichtingendienst van een andere instantie ongevraagd gegevens over de inhoud van gesprekken en niet alleen de gewenste metadata (dossier 2018/7650). De inlichtingendienst hield de gegevens over de inhoud van de gesprekken apart en verwittigde de BIM-Commissie. Deze besliste tot een exploitatieverbod. Het Comité kwam tot het volgende besluit: '*Considérant, après une enquête menée conformément à l'article 43/5 §§ 1er*

Overwegende dat deze werkwijze bijgevolg schade toebrengt aan het algemeen beginsel van goed bestuur en moet worden vermeden'. (vrije vertaling).

113 *'Overwegende dat ingevolge art. 18/3, § 2, eerste lid, 2°, W.I&V, de beslissing van het diensthoofd, op straffe van onwettigheid, het voorwerp moet bevattten waarop de specifieke methode kan worden toegepast;* in voorliggend geval, werd het voorwerp niet vermeld'. (vrije vertaling).

et 2 de la L.R&S, qu'il apparaît que dans le réquisitoire adressé à [X] en exécution de la décision précitée du dirigeant du service, il n'est fait aucune mention d'une interception téléphonique en application de l'article 18/17, § 1er, de la L.R&S et que la mise en œuvre de cette méthode repose exclusivement sur une erreur de la [X]; que cela exonère [le service de renseignement] de toute responsabilité; que de surcroît, [ce service] a sollicité immédiatement [X] d'interrompre cette méthode dès qu'[il] en a eu connaissance; Considérant que les données de communications téléphoniques interceptées ont été communiquées illégalement [aux services de renseignements] à défaut de décision valable.'[114]

De gevolgen van een onwettig(e) (uitgevoerde) methode

In het hierboven vermelde dossier 2018/7250, waarbij de door een onwettige vordering gecollecteerde gegevens moesten vernietigd worden, bleek daarenboven dat de methode aanleiding had gegeven tot het opstellen van twee inlichtingenrapporten. Het Comité beveelde hierover het volgende: '*que les deux rapports, non référencés, ainsi que tout autre document y faisant référence, traitant des résultats du réquisitoire […] ne puissent pas être exploités et soient détruits*'.[115]

II.3. CONCLUSIES EN AANBEVELINGEN

Het Vast Comité I formuleert volgende algemene conclusies en aanbevelingen:
- ADIV richtte zich bij de inzet van BIM-methoden zoals steeds meer op de dreiging van 'spionage', gevolgd door 'terrorisme' en 'inmenging'; voor de VSSE was de aard van de dreiging hoofdzakelijk 'terrorisme', gevolgd door 'spionage' en 'extremisme'.
- Het aantal door de VSSE ingezette bijzondere methoden blijft ook in 2018 sterk stijgen. De stijging manifesteert zich verhoudingsgewijs vooral op vlak van de uitzonderlijke methoden.
- Ook de ADIV deed in 2018 meer beroep op bijzondere inlichtingenmethoden en keert daarmee een dalende trend van afgelopen jaren. De ADIV zet evenwel nog steeds beduidend minder BIM's in dan de VSSE.

---

114 '*Overwegende dat, na een onderzoek uitgevoerd conform artikel 43/5 §§ 1 en 2 W.I&V, blijkt dat in de vordering geadresseerd aan [X] in uitvoering van bovengenoemde beslissing van het dienst-hoofd, op geen enkele wijze melding wordt gemaakt van een telefoontap in toepassing van artikel 18/17, § 1, W.I&V en dat de uitvoering van deze methode integraal gebaseerd is op een vergissing van de […]; dit ontheft [deze dienst] van alle verantwoordelijkheid; bovendien heeft de [inlichtingendienst] onmiddellijk aan [X] verzocht de methode te onderbreken van zodra ze hiervan kennis kreeg; Overwegende dat de onderschepte telefoniegegevens bij gebrek aan een geldige beslissing onwettig werden verstrekt aan de [inlichtingedienst]'.* (vrije vertaling).

115 '*dat de twee rapporten, zonder referte, alsook elk ander document dat daarnaar verwijst, gebruik makend van de resultaten van de vordering […] niet mag worden geëxploiteerd en moeten worden vernietigd.*' (vrije vertaling).

- Hetzelfde beeld zien we bij de gewone methoden van vorderingen gericht aan operatoren om bepaalde communicatiemiddelen te identificeren: de VSSE formuleerde in 2018 6482 vorderingen, de ADIV 502. Het Comité kan niet om de vaststelling heen dat er sinds de invoering van de versoepelde procedure *ex* artikel 16/2 W.I&V opnieuw veel meer identificaties worden verricht. Het Comité bekwam geen (ADIV) of geen afdoend (VSSE) antwoord op zijn vragen hierover. Daarom werd besloten de thematiek op te nemen in een in 2019 geopend toezichtonderzoek.
- Anders dan voor de inzet van bijzondere methoden beschikt het Comité niet over de cijfers met betrekking tot de geviseerde dreiging en de te verdedigen belangen wat betreft de gewone methoden *ex* artikel 16/2 W.I&V. Het Comité beveelt de diensten aan ook deze gegevens te registreren en ter beschikking te stellen van het Vast Comité I.
- Het Comité diende slechts in 11 dossiers een onwettigheid vast te stellen. Daarmee blijft het aantal door het Comité genomen beslissingen dalen, en dit ondanks de significante stijging van het aantal ingezette BIM-methoden. Bovendien zijn – op één na – alle vattingen het gevolg van een schorsing door de BIM-Commissie. Zoals uit de analyse van de rechtspraak blijkt, bleek in een aantal cases de toelating om een BIM in te zetten volkomen wettig, doch stelde er zich problemen op vlak van de uitvoering in die zin dat de vordering van de gegevens niet conform was aan het initiële mandaat. Andere onwettigheden betroffen het gebrek aan motivering, het ontbreken van een voorafgaande beslissing door het diensthoofd of nog, een verkeerd voorwerp van de methode, waarbij het Comité besloot tot vernietiging van de onwettelijk bekomen gegevens.

HOOFDSTUK III
HET TOEZICHT OP BUITENLANDSE INTERCEPTIES, BEELDOPNAMEN EN IT-INTRUSIES

Bij Wet van 30 november 1998 kreeg de ADIV een beperkte interceptiebevoegdheid: '*het onderscheppen, het afluisteren, de kennisname of de opname, […] om redenen van militaire aard, van militaire radioverbindingen uitgezonden in het buitenland.*'

In 2003 werd die mogelijkheid aanzienlijk uitgebreid, zowel wat betreft de aard van de communicatie als wat betreft de dreiging. Sindsdien mag de ADIV zijn intercepties richten op '*elke vorm van communicatie uitgezonden in het buitenland zowel om redenen van militaire aard in het kader van de opdrachten gedefinieerd in artikel 11, § 2, 1° en 2° van deze wet als om redenen van veiligheid en bescherming van onze troepen en van deze van onze geallieerden tijdens operaties in het buitenland en van onze onderdanen die in het buitenland gevestigd zijn, zoals gedefinieerd in hetzelfde artikel 11, § 2, 3° et 4°.*' Gelet op deze verruimde bevoegdheid, werd een specifieke controletaak toevertrouwd aan het Vast Comité I (zie verder).

In 2010 werd de Wet opnieuw gewijzigd[116]: naast het '*het onderscheppen, het afluisteren, het kennisnemen of het opnemen*' kon de ADIV voortaan ook communicatie '*zoeken*'. Voorafgaand aan het onderscheppen, het afluisteren, het kennisnemen of het opnemen moet de ADIV immers in staat zijn het ganse elektromagnetische spectrum en de *cyberspace* te bewaken, bijvoorbeeld om nieuwe (exploitatie)mogelijkheden te zoeken en te identificeren of om over voldoende informatie te beschikken om met zekerheid vast te stellen dat bepaalde intercepties toegestaan zijn.

In 2017 werden de bevoegdheden van de ADIV voor een derde maal verruimd, net zoals de controletaak van het Vast Comité I.[117] In een eerste onderdeel

116 Deze mogelijkheid werd ingevoerd door de zgn. BIM-Wet. Deze wet maakte het voor de VSSE en de ADIV ook mogelijk om binnenlandse communicaties af te luisteren en op te nemen (art. 18/17, § 1 W.I&V en Hoofdstuk II). Er moet een duidelijk onderscheid worden gemaakt tussen 'intercepties als bijzondere inlichtingenmethode' en de 'veiligheidsintercepties' beschreven in dit hoofdstuk, zowel wat betreft het toepassingsgebied als wat betreft de controle.

117 VAST COMITÉ I, *Activiteitenverslag 2017*, 46-47.

wordt die wetswijziging kort in herinnering gebracht. In een tweede onderdeel wordt de wijze waarop het Comité in 2018 zijn specifieke controletaak in deze heeft waargenomen, samengevat.

III.1. DE BEVOEGDHEDEN VAN DE ADIV EN DE CONTROLETAAK VAN HET VAST COMITÉ I[118]

In 2017 breidde de bevoegdheid van de ADIV in het kader van de veiligheidsintercepties uit. De intercepties kunnen sindsdien voor communicaties '*uitgezonden of ontvangen in het buitenland*'. Vóór de wetswijziging was dit beperkt tot communicaties die waren '*uitgezonden in het buitenland*'. Daarenboven geldt deze mogelijkheid nu voor *quasi* alle opdrachten van de ADIV.[119] Daarbij is het niet onbelangrijk te vermelden dat de opdrachtomschrijvingen zelf, ook werden verruimd door dezelfde wetswijziging).[120]

Daarnaast voerde de wet twee andere methoden in, te weten de 'intrusie in een informaticasysteem'[121] en de 'opname van bewegende beelden'.[122]

De wijze waarop het Comité deze methoden kan controleren, wijzigde ook op sommige vlakken.

De controle *voorafgaand* aan de intercepties, intrusies of beeldopnames gebeurt op basis van jaarlijks opgestelde lijsten.[123] Dit betekent dat er naast een jaarlijks interceptieplan, nu ook een intrusie- en beeldplan dient te worden opgesteld door de ADIV. In deze plannen stelt de ADIV een lijst op van '*organisaties of instellingen die het voorwerp zullen uitmaken van interceptie van hun communicaties, intrusies in hun informaticasystemen of opnames van vaste of bewegende beelden tijdens het komende jaar. Deze lijsten verantwoorden voor iedere organisatie of instelling de reden waarom zij het voorwerp is van een interceptie, intrusie of opname van vaste of bewegende beelden in verband met*

118 Zie artt. 44 t.e.m. 44/5 W.I&V.

119 '*[I]n het kader van de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5 W.I&V'.*

120 Indien een ingreep op een communicatienetwerk noodzakelijk is om de interceptie van in het buitenland uitgezonden of ontvangen communicatie mogelijk te maken, kan de ADIV de medewerking van een netwerkoperator of de verstrekker van een elektronische communicatiedienst vorderen (art. 44/5 W.I&V).

121 In dit kader kan de ADIV '*overgaan tot de intrusie in een informaticasysteem dat zich in het buitenland bevindt, er de beveiliging van opheffen, er technische voorzieningen in aanbrengen teneinde de door het informaticasysteem opgeslagen, verwerkte of doorgestuurde gegevens te ontcijferen, te decoderen, op te slaan en te manipuleren en het informaticasysteem te verstoren en te neutraliseren*' (art. 44/1 W.I&V).

122 In dit kader kan de ADIV '*in het buitenland middelen gebruiken voor de opname van vaste of bewegende beelden*' (art. 44/2 W.I&V).

123 Dit impliceert niet dat het Vast Comité I de bevoegdheid heeft om de door de minister goedgekeurde lijst al dan niet goed te keuren.

de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°, en vermelden de voorziene duur' (art. 44/3 W.I&V). De ADIV moet die lijsten in de maand december voor toelating aan de minister van Defensie zenden. Deze heeft tien werkdagen om zijn beslissing mee te delen aan de ADIV[124] die op zijn beurt de lijsten, voorzien van de toelating van de minister, overzendt aan het Vast Comité I.[125]

Het toezicht *tijdens* de interceptie, intrusie of opname gebeurt '*op elk ogenblik door middel van bezoeken aan de installaties waar de Algemene Dienst Inlichting en Veiligheid deze intercepties, intrusies en opnames van vaste of bewegende beelden uitvoert'*.

Het toezicht *na* de uitvoering van de methode werd aanzienlijk verscherpt. Het gebeurt '*aan de hand van maandelijkse lijsten van landen of van organisaties of instellingen die effectief het onderwerp hebben uitgemaakt van een afluistering, intrusie of opname van beelden gedurende de voorafgaande maand'* en die '*de reden verantwoorden waarom de interceptie, intrusie of opname van beelden werd uitgevoerd in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°*'. Deze lijsten moeten ter kennis van het Vast Comité I worden gebracht. De *ex post*-controle gebeurt ook aan de hand van '*het nazicht van logboeken die permanent op de plaats van de interceptie, de intrusie of de opname van vaste of bewegende beelden door de Algemene Dienst Inlichting en Veiligheid worden bijgehouden*'. Deze logboeken moeten steeds toegankelijk zijn voor het Vast Comité I.

Wat kan het Vast Comité I nu ondernemen indien het een onregelmatigheid vaststelt? Artikel 44/4 W.I&V bepaalt dat het Comité, *'[o]ngeacht de andere bevoegdheden aan dit Comité toegekend op basis van de wet van 18 juli 1991, het recht [heeft] de aan de gang zijnde intercepties, intrusies of beeldopnames te doen stopzetten wanneer blijkt dat ze de wettelijke bepalingen of de [ministeriële] toelating niet respecteren. Het beveelt dat de gegevens die onwettig werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd, volgens de door de Koning te bepalen nadere regels.'* Er werd evenwel nog geen dergelijk KB getroffen. Het Comité beveelt aan om dit zo spoedig mogelijk te doen. Het Comité moet zijn beslissing alleszins omstandig motiveren en meedelen aan de minister en aan de ADIV.

---

124 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.

125 Voor intercepties, intrusies of opnames die niet opgenomen zijn in de jaarlijkse lijsten, maar die *'onontbeerlijk en dringend blijken te zijn*', wordt de minister zo spoedig mogelijk en uiterlijk op de eerste werkdag die volgt op de aanvang van de methode ingelicht. Indien de minister niet akkoord gaat, kan hij deze methode laten stopzetten. Deze beslissing wordt door de ADIV zo spoedig mogelijk meegedeeld aan het Vast Comité I.

III.2. HET IN 2018 VERRICHTE TOEZICHT

III.2.1. HET TOEZICHT VOORAFGAAND AAN DE INTERCEPTIE, INTRUSIE OF OPNAME

Het Vast Comité I formuleerde een aantal belangrijke opmerkingen bij het 'Interceptieplan 2017'. De belangrijkste opmerkingen betroffen de prioriteitsverschillen tussen enerzijds het Inlichtingenstuurplan[126] 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 2018', dat eind april 2018 aan het Comité werd bezorgd, heeft de ADIV de organisaties die het voorwerp kunnen uitmaken van intercepties, nader omschreven. Het Comité diende slechts enkele kleine opmerkingen te formuleren bij het plan.

Het Vast Comité I werd midden februari 2018 ook in het bezit gesteld van het – eerdere summiere – beeld- en intrusieplan. 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

Eind 2018 bezocht het Comité de installaties van waaruit de intercepties gebeuren. Bij die gelegenheid controleerde het Comité of er geen verschillen waren tussen de in het interceptieplan goedgekeurde targets en de op dat moment uitgevoerde intercepties. Er werd geen enkele onregelmatigheid vastgesteld.

III.2.3. HET TOEZICHT NA DE UITVOERING VAN DE METHODE

Het Comité ontving negen '*maandelijkse lijsten*[127] *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°'.*

126 Een plan opgesteld door de Directie Intelligence van de ADIV met daarin de op te volgen landen en de prioritisering.

127 Deze negen rapporten hadden betrekking op de twaalf maanden van het jaar.

De controle van de maandelijkse intrusie- en beeldopnamelijsten zal gebeuren in het kader van het 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*.'

Zoals vereist, verrichtte het Comité ook een nazicht van de logboeken die in het kader van de intercepties dienen bijgehouden te worden. Er vielen slechts enkele onregelmatigheden van administratieve aard te noteren.

Ten slotte heeft het Comité voor het eerst een controle uitgevoerd op de analyseproducten die in het kader van een internationale SIGINT-samenwerking werden opgesteld.

III.2.4. VASTSTELLINGEN EN CONCLUSIES

Tijdens werkvergaderingen en inspecties kon het Comité vaststellen dat de ADIV alles in het werk stelde om de aangevatte hervormingen op het niveau van de nationale en internationale samenwerking en op technisch vlak, verder te zetten.

Om zijn doelstellingen te bereiken en de wettelijke opdrachten te kunnen uitoefenen, dient de ADIV te kunnen beschikken over voldoende menselijke en technische middelen in het domein van de SIGINT. Ook in 2018 werd vastgesteld dat de aanwerving van personeel dat kan instaan voor vertalingen, daarbij een prioriteit dient te vormen.

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

Zoals boven[128] vermeld, nam het Vast Comité I eerder 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.[129] 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 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

128 Zie 'Hoofdstuk I.2. De activiteiten van de ADIV in een buitenlandse operatiezone'.

129 Protocolakkoord van 24 mei 2018 tussen de CHOD en de ADIV betreffende de HUMINT- en de analysecapaciteiten van het ISTAR Bn.

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 verslag betreffende iedere onderzoeksopdracht. Het Comité ontving in 2018 enkele van deze verslagen. De analyse van deze verslagen zal het voorwerp uitmaken van verder onderzoek.

IV.2. CONTROLE OP DE SPECIALE FONDSEN

Het Rekenhof houdt namens de Kamer van Volksvertegenwoordigers toezicht op het gebruik van de financiële middelen door overheidsdiensten. Het Rekenhof controleert de wettigheid, de rechtmatigheid en de doelmatigheid van alle uitgaven. Dat geldt in principe ook voor alle uitgaven van de inlichtingendiensten. Echter, omwille van de gevoeligheid van de materie wordt een deel van het budget van de VSSE en de ADIV (met name de 'speciale fondsen' met uitgaven voor bijvoorbeeld operaties en informanten) niet onderzocht door het Rekenhof. Voor de VSSE wordt de controle van deze uitgaven verricht door de directeur algemeen beleid van de minister van Justitie. Halfweg 2018 uitte het Rekenhof het voornemen om vanaf het afsluiten van de rekening van 2018 een periodieke controle te doen van deze fondsen.

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 gebeurt sinds 2010 in aanwezigheid van de voorzitter van het Vast Comité I. In 2018 was de voorzitter effectief aanwezig bij deze vier controles.

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.

Voorheen bestonden twee richtlijnen die een verplichting inhielden voor de VSSE om de minister van Justitie in kennis te stellen wanneer politici het voorwerp uitmaakten van inlichtingenactiviteiten: een ministeriële richtlijn van 25 mei 2009 – opgesteld naar aanleiding van de aanbevelingen van het Vast

Comité I in het kader van een eerder toezichtonderzoek[130, 131]– en een interne instructie van 27 maart 2012. De richtlijn van 25 mei 2009 stelde dat de minister van Justitie op de hoogte moest worden gebracht telkens de naam van een zetelend federaal parlementslid werd vernoemd in een verslag. Het toepassingsgebied van de interne instructie van 27 maart 2012 was zowel enger als ruimer dan dat van de ministeriële instructie: ze had enerzijds alleen betrekking op vermeldingen in verslagen van de buitendiensten van de VSSE, maar anderzijds op alle ministers en politieke mandatarissen, ook deze van de Gemeenschappen en Gewesten.[132]

Vanaf 1 januari 2018 wordt binnen de VSSE een nieuwe als 'vertrouwelijk' geclassificeerde dienstnota van 13 december 2017 toegepast. 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 mandatarissen die bijdragen aan de totstandkoming van een dreiging en een trimestrieel overzicht van het geheel van documenten waarin melding wordt gemaakt van politieke mandatarissen.

De minister van Justitie stemde eerder in met het '*principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991*'.[133] In het kader van de meldingsplicht werd het Comité door de VSSE van beide types van rapporten op de hoogte gesteld.

Ondanks herhaaldelijk verzoek mocht het Comité van de ADIV geen informatie in die zin ontvangen.

Het Vast Comité I neemt zich voor deze dossiers steekproefsgewijs aan een legaliteitstoets te onderwerpen.

---

130 VAST COMITÉ 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.).

131 De aanbeveling luidde als volgt: *'Meer in het algemeen wenst het Vast Comité I dat de Veiligheid van de Staat klare en eenduidige richtlijnen uitwerkt met betrekking tot de inwinning, de verwerking, de raadpleging (met inbegrip van de eventuele interne afscherming), de opslag en de archivering van gegevens van bepaalde categorieën van personen die bijzondere verantwoordelijkheden dragen of droegen. Bij de uitwerking van deze richtlijnen en bij de concrete opvolging van de (gewezen) politieke mandatarissen dient de Veiligheid van de Staat rekening te houden met de krijtlijnen uitgetekend in het arrest van het Europees Hof voor de Rechten van de Mens in de zaak Segerstedt-Wiberg and others'*.

132 Hierover uitvoerig: VAST COMITÉ I, *Activiteitenverslag 2013*, 37 e.v. ('II.4. De opvolging van politieke mandatarissen door de inlichtingendiensten'). Zie ook VAST COMITÉ I, *Activiteitenverslag 2013*, 25 e.v. ('II.2. Geheime nota's over de Scientology-kerk in de pers') en 31 e.v. ('II.3. Een informant binnen het Vlaams Belang').

133 *'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'.

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.

Decennialang doken allerhande theorieën op over de oorzaak van de crash.[134] In een publicatie van Susan Williams, onderzoekster aan de University of London[135], werden verschillende hypothesen van de crash van het VN-vliegtuig onderzocht; de auteur besloot dat alles wijst in de richting van een bewuste interventie door een of meerdere vliegtuigen. Daarbij vielen ook namen van Belgen die toen in de regio actief waren. Williams pleitte ervoor om de waarheid aan het licht te brengen door de '*intelligence, security and defence archives*' van landen die betrokken waren in het toenmalig conflict in Congo, zoals de VS, het Verenigd Koninkrijk, Frankrijk, Duitsland, Zuid-Afrika maar ook België, open te stellen.

Voormalig secretaris-generaal van de VN Ban Ki-Moon pikte de idee op en stelde een nieuw onderzoek in, onder leiding van *Eminent Person* Mohamed Chande *Othman*. Op 24 december 2017 keurde de Verenigde Naties hieromtrent een Resolutie goed.[136] Daarin worden 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. Othman wou ook van de door de lidstaten aangeduide onafhankelijke personen weten welke moeilijkheden ze ondervonden bij hun onderzoek (bijv. het weigeren van toegang tot bepaalde archieven).

Op 16 april 2018 duidden de ministers van Justitie en Defensie toenmalig voorzitter van het Vast Comité I, Guy Rapaille 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. De Voorzitter van de Begeleidingscommissie werd van deze aanstelling in april 2018 op de hoogte gebracht. De voorzitter van het Comité nam het luik van de geclassificeerde informatie uit de archieven van de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid voor zijn rekening, Quanten onderzocht de archieven van Defensie. Eind september 2018 legden zij hun verslag neer bij de VN. Ze concludeerden dat *'after a thorough and meticulous*

134 Onder meer door het onderzoek van G. BJÖRKDAHL (J. BORGER, *The Guardian*, 17 Aug 2011, 'Dag Hammeskjöld: evidence suggests UN chief's plan was shot down').

135 S. WILLIAMS, *Who killed Hammarskjöld? The UN, the cold war and white supremacy in Africa*, Hurst Publishers, Londen, 2016.

136 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).

analysis of these archives, is that they do not contain any direct information related to the death of Dag Hammerskjöld. Although, some elements which may shed an additional light on the proposed research, have been selected'.

Begin november 2018 kreeg de Algemene Vergadering van de Verenigde Naties van Othman een eerste tussentijdse verslag.[137] Hieruit bleek onder meer dat Zuid-Afrika noch het Verenigd Koninkrijk experten aanduidden. Wat het Belgische luik betreft, werd vermeld dat beide experten *'provided a comprehensive interim report indicating the sustantial work undertaken by them. The interim report confirms that full access*[138] *was given by Belgium to all files and archives kept by the Ministry of Defence, the State security Service (VSSE) and the General Intelligence and Security service (GISS, military intelligence service). The report observes that the mandate has not covered a review of the archives of non-state actors or private organisations. The interim report from Belgium identifies information relevant to the presence of foreign paramilitary and intelligence personnel in and around the Congo at the relevant time, as well as to the capacity of the arial forces of Katanga*.'[139]

Ingevolge de opruststelling 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.

---

137 Zie: www.hammarskjoldinquiry.info/pdf/ham_187_EP_interim_report_081118.pdf. Het rapport werd op 3 december 2018 mondeling toegelicht (Oral briefing by Mr. Miguel de Serpa Soares, Under-Secretary-General for Legal Affairs and United Nations Legal Counsel). De thematiek vormt opnieuw het onderwerp van publicaties begin 2019 (E. GRAHAM HARRISON et al., *The Observer*, 12 Jan 2019, 'Man accused of shooting down UN chief').

138 Wel stelde het Belgische verslag dat '*the searching of archives of the military intelligence service GISS and of het Ministry of Defence has yielded less useful documentation than at the State Security Service, can be called somewhat astonishing. […] It should be noted that, at this stage, all GISS sub-archives have not yet been fully investigated*.'

139 Zie: www.hammarskjoldinquiry.info/pdf/ham_187_EP_interim_report_081118.pdf.

HOOFDSTUK V
HET VAST COMITÉ I ALS BEVOEGDE TOEZICHTHOUDENDE AUTORITEIT IN HET KADER VAN DE VERWERKING VAN PERSOONSGEGEVENS

V.1. NIEUWE EUROPESE RECHTSINSTRUMENTEN MET BELANGRIJKE GEVOLGEN OP NATIONAAL VLAK

Op 4 mei 2016 werden in het Publicatieblad van de Europese Unie twee belangrijke rechtsinstrumenten gepubliceerd in verband met de verwerking van persoonsgegevens: de Algemene Verordening Gegevensbescherming 2016/679 (AVG)[140] en de Richtlijn 2016/680 (Richtlijn).[141] Beide instrumenten regelen de wijze waarop publieke en private actoren dienen te handelen wanneer zij persoonsgegevens verzamelen, opslaan, bewaren en doorgeven: wanneer is een verwerking rechtmatig en eerlijk? Welke rechten heeft de betrokkene en wat zijn de uitzonderingen op deze rechten? Wie is de verwerkingsverantwoordelijke en de verwerker? Kunnen persoonsgegevens worden doorgegeven naar derde landen? Wie is de toezichthoudende autoriteit? Welke sancties zijn mogelijk bij overtredingen? …

De AVG, die in werking trad op 25 mei 2018, en de Richtlijn gaven aanleiding tot enkele belangrijke wetswijzigingen op national vlak. Zo werd de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens opgeheven en werd de Commissie voor de bescherming van de persoonlijke levenssfeer (de Privacycommissie) bij Wet

140 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.

141 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.

van 3 december 2017 vervangen door de Gegevensbeschermingsautoriteit (GBA).[142] Daarnaast werd een geheel nieuwe Gegevensbeschermingswet gestemd.[143]

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'. Dergelijke verwerkingen vallen buiten het Unierecht en worden dus niet gevat door de AVG of de Richtlijn, maar de wetgever heeft er voor geopteerd om de diensten die dergelijke verwerkingen uitvoeren, tot op zekere hoogte toch te onderwerpen aan dezelfde gegevensbeschermingsregels.

Dit was voorheen eigenlijk ook reeds het geval: de Privacywet van 1992 was slechts ten dele van toepassing op de verwerkingen door de VSSE, de ADIV, de veiligheidsoverheden, de veiligheidsofficieren en het Vast Comité I en zijn Dienst Enquêtes. Dat bepaalde gegevensbeschermingsregels van toepassing waren op deze diensten mag overigens niet verwonderen. Immers, België is gebonden door Verdrag nr. 108 van de Raad van Europa van 28 januari 1981 voor de bescherming van individuen met betrekking tot de automatische verwerking van persoonlijke gegevens.[144] Dit Verdrag is wat België betreft ook van toepassing op diensten die gegevens verwerken inzake nationale veiligheid. Daarenboven geldt in België ook het Aanvullend Protocol bij dit Verdrag.[145] Daarin staan specifieke regels met betrekking tot onafhankelijke toezichtorganen en informatie-uitwisseling over de landsgrenzen heen.

In wat volgt, wordt vooreerst de nieuwe rol van het Vast Comité I toegelicht. Deze rol staat omschreven in de Wet tot oprichting van de Gegevensbeschermingsautoriteit (GBA-Wet), in de Gegevensbeschermingswet (GBW) en in de Toezichtwet (W.Toezicht) waarin een aantal wijzigingen werden aangebracht. Het Comité werd, in eerste instantie op informele wijze en nadien formeel, betrokken bij de totstandkoming van deze nieuwe regeling.[146] Zoals verder zal blijken, werden door het Parlement nog enkele wijzigingen aangebracht aan de tekst. Niettemin zal de nieuwe regeling op een aantal belangrijke punten nog moeten gewijzigd of aangevuld worden. In een tweede deel wordt kort stilgestaan bij het Vast Comité

142 Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (GBA-Wet), *BS* 10 januari 2018.

143 Voluit: Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (GBW), *BS* 5 september 2018.

144 Https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/verdrag_108.pdf.

145 Https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanvullend_protocol_verdrag_108.pdf.

146 Het advies dat het Comité verleende op vraag de Kamercommissie Justitie is terug te vinden de website van het Comité (www.comiteri.be). Op 26 juni 2018 lichtte de voorzitter van het Comité zijn advies mondeling toe op een zitting van de bevoegde Kamercommissie. Zie i.v.m. dit advies ook 'Hoofdstuk VII. Adviezen'.

I als verwerker van persoonsgegevens. Ten slotte worden de eerste activiteiten van het Comité als 'Bevoegde toezichthoudende autoriteit' (BTA) toegelicht.

V.2. NIEUWE OPDRACHTEN VOOR HET COMITÉ ALS BEVOEGDE TOEZICHTHOUDENDE AUTORITEIT

De nieuwe opdrachten van het Comité en de wijze waarop deze moeten worden uitgeoefend, blijken uit diverse bepalingen uit de Gegevensbeschermingswet en de Toezichtwet. Ze worden hieronder samengevat weergegeven. Vooreerst wordt echter gepreciseerd voor welke verwerkingen het Comité bevoegd is en hoe het Comité zich verhoudt tot de andere Bevoegde toezichthoudende autoriteiten.

V.2.1. TEN AANZIEN VAN WELKE VERWERKINGEN VAN WELKE DIENSTEN EN PERSONEN?

Het Vast Comité I is bevoegd voor de controle op alle of bepaalde persoonsgegevensverwerkingen door tal van diensten, overheden en personen. Ze staan opgesomd in Titel 3 van de Gegevensbeschermingswet.

- Ondertitel 1. heeft specifiek betrekking op alle verwerkingen door de VSSE en de ADIV (artt. 73 en 95 GBW);
- Ondertitel 3. viseert elke verwerking van persoonsgegevens in het kader van veiligheidsmachtigingen, -attesten en -adviezen bedoeld in de Wet van 11 december 1998 door de Nationale Veiligheidsoverheid (NVO) en elk overheidslid van deze overheid, de andere veiligheidsoverheden zoals bedoeld in de artikelen 15, tweede lid en 22*ter* W.C&VM en de veiligheidsofficieren bedoeld in artikel 13, 1°, W.C&VM of hun verwerkers (artt. 107 en 128 GBW)[147];
- Ondertitel 4. handelt over elke verwerking van persoonsgegevens door het OCAD en zijn verwerkers, '*uitgevoerd in het kader van de opdrachten als bedoeld in de wet van 10 juli 2006, en door of krachtens bijzondere wetten*' (artt. 139 en 161 GBW). De verwerkingen door de ondersteunende diensten van het OCAD worden hier dus niet geviseerd;
- Ondertitel 5. handelt over elke verwerking van persoonsgegevens door de Passagiersinformatie-eenheid (PIE) in het kader van de finaliteiten bedoeld in

[147] Deze ondertitel is ook van toepassing op elke verwerking van persoonsgegevens door het Beroepsorgaan in het kader van de beroepsprocedures bedoeld in de Wet van 11 december 1998 tot oprichting van het Beroepsorgaan. Echter, in dit kader vervult het Comité niet de rol van Bevoegde toezichthoudende autoriteit (art. 128 § 2 GBW).

artikel 8, § 1, 4°, van de Wet van 25 december 2016 of met andere woorden verwerkingen met het oog op '*het toezien op activiteiten bedoeld 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*' (artt. 169 en 184 GBA);[148, 149]

– Ondertitel 6. ten slotte viseert de verwerkingen door de BIM-Commissie (art. 185 GBW).

Op elk van deze diensten of personen rusten specifieke verplichtingen inzake dataprotectie. Ze zijn grotendeels gelijklopend. Toch zijn er enkele verschillen. Zo bijvoorbeeld is wat betreft de BIM-Commissie alleen bepaald dat het Vast Comité I de BTA is. De regels die de BIM-Commissie dient te respecteren bij de verwerking van persoonsgegevens en de rechten van de burger, werden slechts zeer summier omschreven in de Gegevensbeschermingswet. Wel zijn de enkele algemene bepalingen uit de Toezichtwet ook op de BIM-Commissie van toepassing.

V.2.2. WELKE 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) – de opvolger van de Privacycommissie – 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 dat er in bepaalde gevallen moet of kan worden samengewerkt of dat er informatie moet worden uitgewisseld. Zo bepalen de artikelen 98 en 131 GBW dat de andere BTA's het Vast Comité I moeten informeren over inbreuken op de reglementering inzake de verwerking van persoonsgegevens door de inlichtingendiensten of veiligheidsoverheden van zodra zij er kennis van

148 Hierover: Protocolakkoord d.d. 13 november 2018 betreffende de samenwerking tussen de Passagiersinformatie-eenheid en de ADIV in het kader van de wet betreffende de verwerking van de passagiersgegevens (Beperkte verspreiding, art. 20 KB 24 maart 2000).

149 Zie in verband met de relatie tussen de functionaris voor de gegevensbescherming van het PIE en het Vast Comité I ook artikel 27 van het K.B ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, houdende diverse bepalingen betreffende de Passagiersinformatie-eenheid en de functionaris voor de gegevensbescherming, *BS* 29 december 2017.

nemen. Ook moeten zij met het Comité overleggen wanneer zij gevat worden in een dossier dat mogelijk gevolgen heeft voor de verwerking van persoonsgegevens door een van deze instanties.[150] Verder dienen de BTA's in bepaalde gevallen onderzoeksverslagen uit te wisselen (*infra*).

Belangrijker is evenwel 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 zal worden waargenomen door de Gegevensbeschermingsautoriteit. Tevens moeten de BTA's een protocol afsluiten met het oog op de verwezenlijking van de vereiste samenwerking.

De wetgever voorzag ten slotte 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.

V.2.3. WELKE NIEUWE OPDRACHTEN?

V.2.3.1. Onderzoeken voeren

Wie kan een onderzoek initiëren?

Het Comité kan op eigen initiatief of op verzoek van een bevoegde overheid onderzoeken instellen naar de verwerkingen van persoonsgegevens door de inlichtingendiensten (en de hierboven vermelde personen en overheden[151]) en hun verwerkers (art. 33 W.Toezicht). Het '*waakt [daarbij] over de […] bescherming van de fundamentele rechten en vrijheden van de natuurlijke personen met betrekking tot deze verwerking*.' (artt. 95 en 128 GBW; zie ook art. 144 GBW).

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

150 Voor de andere door het Vast Comité I te controleren diensten werd geen gelijkaardige bepaling opgenomen in de GBW. Het betreft duidelijk een vergetelheid van de wetgever.

151 Art. 33 W.Toezicht verwijst alleen naar de inlichtingendiensten en niet naar de andere personen en overheden ten aanzien van wie het Comité de bevoegde gegevensbeschermingsautoriteit is. Het Comité gaat er van uit dat het om een vergetelheid gaat.

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).[152] 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.[153]

Daarnaast bepaalt artikel 51/1 GBW dat het Comité *'[i]n zijn hoedanigheid van gegevensbeschermingsautoriteit [op]treedt […] uit eigen beweging, ofwel op verzoek van een andere gegevensbeschermingsautoriteit, ofwel op verzoek van elke betrokkene'*. Deze bepaling opent dus de mogelijkheid voor de GBA, het COC of het Vast Comité P om het Vast Comité I te vatten. Een vatting door de GBA of door het COC zal bijvoorbeeld aan de orde zijn wanneer bij de GBA (art. 11 § 5 GBW) of bij het COC (art. 45 § 6 GBW) een verzoek of een klacht aanhangig wordt gemaakt waarbij de verwerkingsverantwoordelijke melding maakt van het feit dat hij gegevens van bijvoorbeeld een inlichtingendienst of van het OCAD verwerkt.[154] In dat geval mag de GBA of het COC de zaak niet zelf behandelen maar moet ze doorverwezen worden naar het Vast Comité I. Het Comité zal dan de nodige verificaties verrichten.

Over welke onderzoeksbevoegdheden en -mogelijkhden beschikt het Vast Comité I

De controle op de gegevensverwerkingen verloopt '*volgens de nadere regels vastgelegd in de wet van 18 juli 1991*' (art. 95 GBW; zie ook artt. 106, 5°, 161 en 174 GBW). Met andere woorden, het Comité kan alle bevoegdheden die het in het kader van zijn traditionele toezichtopdracht mag inzetten, ook hier hanteren.

Daarenboven mag het Comité, indien nodig, samenwerken met de andere Belgische toezichthoudende autoriteiten, zonder dat hierbij afbreuk mag gedaan worden '*aan de fysieke integriteit van personen, of aan de opdrachten van de inlichtingen- en veiligheidsdiensten en de wet van 11 december 1998*' (art. 96 GBW) of mits dit gebeurt '*met inachtneming van de wet van 11 december 1998*' en '*zonder dat dit afbreuk doet aan de belangen bedoeld in artikel 5 van de wet van 11 december 1998 tot oprichting van een beroepsorgaan*' (art. 129 GBW).

---

152 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).

153 Deze verificaties gebeuren kosteloos (artt. 80, 114, 146 en 174 GBW).

154 Art. 11 GBW maakt in zijn eerste paragraaf alleen melding van gegevens van de twee inlichtingendiensten en van het OCAD. In de rest van de bepaling en in het gelijkaardige art. 45 GBW wordt melding gemaakt van '*gegevens verwerkt die rechtstreeks of onrechtstreeks afkomstig zijn van de overheden bedoeld in titel 3*'. Dit lijkt meer aan te sluiten bij de bedoeling van de wetgever.

Ten slotte legt de Gegevensbeschermingswet in twee gevallen (de andere gevallen zijn duidelijk vergeten) een medewerkingsplicht op aan de gecontroleerde diensten (artt. 97 en 130 GBW).

De beslissingen van het Vast Comité I

In een nieuwe Afdeling 4 van Hoofdstuk III van de Toezichtwet worden de beslissingen omschreven die het Vast Comité I kan nemen in zijn hoedanigheid van gegevensbeschermingsautoriteit (art. 51/3 W.Toezicht). Het kan:
- logbestanden en andere gegevens indien een inlichtendienst of de BIM-Commissie over een rechtstreekse toegang of bevraging beschikt van een gegevensbank van een private of publieke actor (artt. 13 en 47 GBW);
- besluiten dat de verwerking is uitgevoerd in overeenstemming met de bepalingen van de reglementering inzake de verwerking van persoonsgegevens;
- de betrokken dienst of diens verwerker waarschuwen dat een voorgenomen verwerking van persoonsgegevens de reglementering kan schenden;
- de betrokken dienst of diens verwerker berispen wanneer een verwerking geresulteerd heeft in een schending van een dataprotectieregel;
- de dienst of de verwerker gelasten om een verwerking in overeenstemming te brengen met de betrokken bepalingen, in voorkomend geval, op een nader bepaalde manier en binnen een nader bepaalde termijn;
- een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod, opleggen;
- het rectificeren of wissen van persoonsgegevens gelasten;
- het dossier overzenden aan de procureur des Konings van Brussel, die het Comité informeert van het gevolg dat aan het dossier gegeven wordt.

De kennisgeving of verslaggeving door het Vast Comité I

Diverse regels bepalen welke persoon, diensten of instanties het Comité op welke wijze moet informeren van het resultaat van zijn controles.

Zo moet het verslag van op eigen initiatief of op verzoek van een bevoegde overheid opgestarte onderzoeken naar de bevoegde minister of overheid en naar de Kamer van Volksvertegenwoordigers worden gezonden (art. 33, derde lid W.Toezicht). De besluiten van het onderzoek worden, naar gelang van het geval, ter kennis gebracht van de leidinggevende ambtenaar van de inlichtingendienst of van de directeur van het OCAD (art. 34, laatste lid W.Toezicht) of – ook hier vergat de wetgever te voorzien in een globale regeling – van een andere betrokken persoon of dienst.

In geval van een onderzoek op klacht van een burger, antwoordt het Comité deze enkel dat '*de nodige verificaties werden verricht*'.[155] De leidinggevende amb-

[155] Zie ook de artt. 80, 114, 146 en 174 GBW. In een 'gewoon' klachtonderzoek kan het Comité in geval van afsluiten van het onderzoek het resultaat '*in algemene bewoordingen*' meedelen (art. 34 W.Toezicht).

tenaar 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).

Indien een andere toezichthoudende autoriteit aan de basis ligt van het opstarten van een onderzoek (bijv. artt. 11 § 5, 45 § 6 en 51/1 GBW) stuurt het Comité zijn '*antwoord*' naar deze andere autoriteit die op zijn beurt de betrokkene informeert maar enkel over '*de resultaten van de verificatie die betrekking hebben op persoonsgegevens die niet van de inlichtingendienst of het OCAD afkomstig zijn*'.[156]

Verder bepalen de artikelen 96 en 128 GBW dat *'[i]n het kader van de uitoefening van het toezicht bedoeld in artikel 95, […] het Vast Comité I in algemene termen het resultaat hiervan mee[deelt] aan de andere bevoegde toezichthoudende autoriteiten*'. Voor onderzoeken naar de andere instanties werd geen gelijkaardige verplichting ingevoerd. Daarenboven werd alleen voor onderzoeken naar de inlichtingendiensten gepreciseerd dat de andere BTA de onderzoeksresultaten van het Comité niet aan de betrokkene mogen bekendmaken (art. 95 GBW).

Ten slotte moet rekening worden gehouden met artikel 51/4 W.Toezicht. Ingevolge deze bepaling moet de betrokken inlichtingendienst op de hoogte gebracht worden wanneer het onderzoek betrekking heeft op een verwerker van deze dienst. Deze bepaling stelt ook het volgende: *'Wanneer het er kennis van neemt, informeert het Vast Comité I eveneens de betrokken dienst van de schendingen van de reglementering inzake de verwerking van persoonsgegevens door andere verwerkingsverantwoordelijken'.*

V.2.3.2. Adviezen verlenen

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.[157] 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.

---

156 Indien het verzoek of de klacht enkel betrekking heeft op persoonsgegevens afkomstig van een inlichtingendienst of het OCAD, antwoordt de GBA of het COC, na ontvangst van het antwoord van het Vast Comité I, dat de nodige verificaties werden verricht.

157 Hierover 'Hoofdstuk VII. Adviezen'.

V.2.3.3. Afhandelen van door de Dienst Enquêtes I doorgemelde misdrijven

Wanneer een lid van de Dienst Enquêtes I kennis heeft van een misdaad of van een wanbedrijf maakt hij daarvan proces-verbaal op dat aan de procureur des Konings wordt gezonden (art. 46 W.Toezicht). Die regel geldt niet voor de misdrijven omschreven in de artikelen 226, 227 en 230 GBW.[158] In die gevallen informeert de dienst zo snel mogelijk het Vast Comité I dat '*de opvolging volgens de nadere regels bepaald in artikel 54*[159] *[W.Toezicht] verzekert*'.

V.2.3.4. 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.[160] 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[161]).

V.2.3.5. Beslissen over het ontslag van een Data Protection Officer

Elke door het Comité gecontroleerde dienst is verplicht een functionaris voor gegevensbescherming (DPO) aan te stellen, die onafhankelijk moet kunnen opereren. Hij kan dan ook niet gestraft worden voor het uitoefenen van zijn functie. Hij kan alleen van zijn functie ontheven worden indien hij een zware fout heeft begaan of de voorwaarden noodzakelijk voor het uitoefenen van zijn functie niet langer vervult. Hij kan deze beslissing aanvechten bij het Vast Comité I (artt. 91, 124 en 157 GBW[162]).

---

158 Dezelfde uitzondering werd ook ingebouwd wanneer de enquêtedienst een misdrijf als bedoeld in art. 13/1 W.I&V vaststelt.

159 Naar alle waarschijnlijkheid betreft het een vergissing en moet verwezen worden naar art. 51/3 W.Toezicht.

160 Niet elke dienst moet alle hier vermelde gegevens bijhouden of ter beschikking stellen. Waarschijnlijk was dat niet de bedoeling van de wetgever. Dit geldt zeker wat betreft de BIM-Commissie die blijkbaar geen informatie moet meedelen aan het Vast Comité I.

161 Voor de PIE werd geen gelijkaardige bepaling opgenomen. Naar alle waarschijnlijkheid betreft het een vergetelheid van de wetgever.

162 *Idem.*

V.2.3.6. Het opstellen van een jaarlijks verslag

Ingevolge artikel 35 § 3 W.Toezicht brengt het Vast Comité I '*jaarlijks verslag uit 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*'. Een kopij van dit verslag wordt gericht aan de bevoegde ministers en aan de twee inlichtingendiensten[163], die over de mogelijkheid beschikken om het Vast Comité I attent te maken op hun bemerkingen.

V.3. HET VAST COMITÉ I ALS VERWERKER VAN PERSOONSGEGEVENS

In de Gegevensbeschermingswet werd een bepaling opgenomen die het Vast Comité I toelaat '*voor zover noodzakelijk voor de uitoefening van hun [zijn] opdrachten, persoonsgegevens van alle aard, inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook de genetische en biometrische gegevens, de gegevens over de gezondheid, de gegevens die het seksuele gedrag of de seksuele gerichtheid betreffen en deze met betrekking tot strafrechtelijke vervolgingen en tot inbreuken of veiligheidsmaatregelen die hiermee samenhangen*' te verwerken '*in het kader van haar opdrachten bedoeld in de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, en in bijzondere wetten*' (art. 185 § 1 GBW).

Om de vertrouwelijkheid en de doeltreffendheid van de uitvoering van deze opdrachten te garanderen, is de toegang van de betrokkene tot deze persoonsgegevens beperkt tot wat voorzien is in de bijzondere wetten. Wel heeft de betrokkene het recht te vragen om eventuele onjuiste persoonsgegevens te laten verbeteren of verwijderen.

Ten slotte bepaalt artikel 185 § 4 GBW dat het Comité '*in het kader van [zijn] opdrachten als toezichthoudende autoriteit niet onderworpen [is] aan het toezicht van de Gegevensbeschermingsautoriteit bedoeld in de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit.*'

Bovenstaande regeling heeft alleen betrekking op verwerkingen die verband houden met de nationale veiligheid. Andere verwerkingen, zoals het beheer van zijn eigen personeelsbeheer vallen onder de gewone dataprotectieregels.

---

[163] Ook hier maakt de tekst van de wet ten onrechte geen melding van de andere in Titel 3 van de Gegevensbeschermingswet vermelde personen en overheden.

Een laatse opmerking betreft het feit dat de Dienst Enquêtes I wat betreft zijn gerechtelijke opdrachten, onder het toezicht valt van het COC in zijn hoedanigheid van Bevoegde toezichthoudende autoriteit.

V.4. ACTIVITEITEN VAN HET VAST COMITÉ I ALS BEVOEGDE TOEZICHTHOUDENDE AUTORITEIT

V.4.1. VOORBEREIDENDE WERKZAAMHEDEN

In 2018 heeft het Comité tal van voorbereidingen getroffen om zijn nieuwe taak en verplichtingen waar te kunnen nemen.

Vooreerst werd een Data Protection Officer (DPO) aangesteld voor alle verwerkingen van het Comité die buiten de 'nationale veiligheid' vallen (bijvoorbeeld verwerkingen in het kader van het personeelsbeheer en logistiek).

Verder werden diverse vergaderingen gehouden met de drie andere bevoegde toezichthoudende overheden. Op de agenda stonden de redactie van een protocol waarin onder meer het 'één-loketmechanisme' voor de burger zal uitgewerkt worden, praktische werkafspraken en de uitwisseling van *best practices*.

Met het Vast Comité P werden de eerste 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.

V.4.2. ACHT DPA-ADVIEZEN

Het Comité verleende in 2018 alleen of samen met het Vast Comité P, acht adviezen bij ontwerpen van wet of ontwerpbesluiten. Deze adviezen zijn integraal te consulteren op de website van het Comité. Hier wordt volstaan met een opsomming van de verleende adviezen:

- Advies 001/VCI-BTA/2018 van 26 september 2018 met betrekking tot '*ontwerpen van Koninklijke besluiten aangaande de uitvoering van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens, waarin de verplichtingen worden opgenomen voor respectievelijk de busvervoersmaatschappijen en het HST-vervoer en HST-ticketverdelers*';
- Advies 002/VCI-BTA/2018 van 26 september 2018 met betrekking tot '*het voorontwerp van wet betreffende de organisatie van de penitentiaire diensten en het statuut van het penitentiair personeel*', waarin bepalingen werden opgenomen inzake de screening van kandidaat-penitentiaire beambten;

- Advies 003/VCI-VCP-BTA/2018 van 26 september 2018 in verband met datzelfde voorontwerp, gegeven samen met het Vast Comité P aangezien het ontwerp stelde dat de screening van kandidaat-penitentiaire beambten mede moest gebaseerd zijn op gegevens afkomstig van het OCAD;
- Advies 004/VCI-BTA/2018 van 1 oktober 2018 in verband met '*het voorontwerp van wet houdende wijziging van de wet van 21 december 2013 houdende het Consulair Wetboek en de wet van 10 februari 2015 met betrekking tot geautomatisseerde verwerkingen van persoonsgegevens die noodzakelijk zijn voor de Belgische paspoorten en reisdocumenten*';
- Advies 005/VCI-VCP-BTA/2018 van 1 oktober 2018 in verband met datzelfde voorontwerp, gegeven samen met het Vast Comité P aangezien in het ontwerp tevens sprake was van het OCAD;
- Advies 006/VCI-BTA/2018 van 24 oktober 2018 met betrekking tot het '*voorontwerp van wet houdende diverse bepalingen inzake informatisering van justitie en modernisering van het statuut van rechters in ondernemingszaken*' waarin sprake was van een leesrecht voor de inlichtingendiensten in SIDIS-suite;
- Advies 007/VCI-VCP-BTA/2018 van 24 oktober 2018 met betrekking tot datzelfde voorontwerp, gegeven samen met het Vast Comité P aangezien er sprake was van een leesrecht in SIDIS-suite voor het OCAD;
- Advies 008/VCI-BTA/2018 van 16 november 2018 met betrekking tot het '*voorwetsontwerp houdende diverse bepalingen in strafzaken*' waarin nieuwe inlichtingenmethoden en beschermings- en ondersteuningsmaatregelen werden opgenomen.

V.4.3. TWEE INDIVIDUELE DPA-KLACHTEN

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 twee werden afgehandeld in 2018. In beide dossiers werden de vereiste verificaties uitgevoerd. De klagers werden hiervan in kennis gesteld.[164]

[164] '*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 wijzigde de Wet van 5 augustus 1992 op het politieambt (WPA): er werd een wettelijke basis gecreëerd voor de oprichting van gemeenschappelijke gegevensbanken in het kader van de voorkoming en opvolging van het terrorisme en het extremisme dat tot terrorisme kan leiden.[165] De achterliggende idee bestond erin om verschillende diensten de mogelijkheid te bieden om hun gegevens en informatie te delen teneinde doeltreffender te zijn in het kader van de strijd tegen deze fenomenen.

Zich baserend op deze nieuwe mogelijkheid, richtten de ministers van Binnenlandse Zaken en Justitie in 2016 de gemeenschappelijke gegevensbank '*foreign terrorist fighters*' (GGB FTF) op.[166] De doelstelling ervan was bij te dragen tot de analyse, de evaluatie en de opvolging van personen met banden met deze problematiek.

In 2018[167] werd deze gemeenschappelijke gegevensbank (GGB) 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[168] ook een aparte gemeenschappelijke gegevensbank opgericht voor '*haatpropagandisten*' (GGB HP). Deze wijzigingen en toevoegingen zullen in het eerste deel van dit hoofdstuk worden toegelicht (VI.1).

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 politio-

---

165 Wet van 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme, *BS* 9 mei 2016.

166 KB van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank '*Foreign Terrorist Fighters*' en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de wet op het politieambt, *BS* 22 september 2016.

167 KB van 23 april 2018 tot wijziging van het bovenvermeld KB van 21 juli 2016 en tot omvorming van de gemeenschappelijke gegevensbank '*Foreign Terrorist Fighters*' naar de gemeen-schappelijke gegevensbank '*Terrorist Fighters*', *BS* 30 mei 2018 (KB TF).

168 KB 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 (KB HP).

nele informatie (COC) en aan het Vast Comité I. Deze toezichtsopdracht wordt besproken in een tweede deel (VI.2).

Beide instanties brachten ook een gezamenlijk advies uit over twee 'voorafgaandelijke aangiften' die in 2018 werden ingediend door de bevoegde ministers. Zoals vereist, regelen deze aangiften in detail de werking van de nieuwe en van de verruimde databank. Een derde onderdeel vat de in deze context geformuleerde adviezen samen (VI.3).

VI.1. DE IN 2018 DOORGEVOERDE WIJZIGINGEN

VI.1.1. DE EVOLUTIE VAN *FOREIGN TERRORIST FIGHTERS* NAAR *TERRORIST FIGHTERS*

De gegevensbank werd in die zin gewijzigd dat ze voortaan is samengesteld uit inlichtingenfiches van zowel '*foreign terrorist fighters*' (dit is de oorspronkelijke categorie uit 2016) alsook van de '*homegrown terrorist fighters*' (de in 2018 toegevoegde categorie).

Behoudens twee aanpassingen die verder worden besproken, bracht het KB van 23 april 2018 geen wijzigingen aan aan het functioneren van de in 2016 opgerichte gemeenschappelijke gegevensbank.[169]

Deze uitbreiding werd noodzakelijk geacht gelet op de vele aanslagen sinds 2016 in Europa van djihadistische aard of gelieerd aan extreem-rechts maar die niet onmiddellijk een band hadden met een djihadistische conflictzone. De aanpassing maakt het dus ook mogelijk om persoonsgegevens en informatie van '*homegrown terrorist fighters*' in de gegevensbank op te nemen.

Het gaat om alle fysieke personen met een aanknopingspunt in België en waarbij minstens aan één van volgende criteria is voldaan:

a) er bestaan ernstige aanwijzingen dat deze persoon de intentie heeft om geweld te gebruiken tegen personen of materiële belangen om ideologische of politieke redenen met het doel zijn doelstelling door middel van terreur, intimidatie of dreigingen te bereiken;
b) er bestaan ernstige aanwijzingen dat hij of zij doelbewust steun levert, onder meer logistiek, financieel of met opleidings- of rekruteringsdoeleinden, aan de personen geviseerd in a), of aan de personen die geregistreerd staan als FTF en waarvoor er ernstige aanwijzingen bestaan dat zij de intentie hebben om een gewelddadige actie uit te voeren (art. 6, § 1, 1°/1 KB TF).

De gegevens van personen die aan deze vereisten voldoen, kunnen worden opgenomen in de gegevensbank. Hetzelfde geldt voor personen voor wie er ernstige

[169] Voor een uitgebreide bespreking van de werking van de gemeenschappelijke gegevensbanken, zie VAST COMITE I, *Activiteitenverslag 2016*, 127-139 (www.comiteri.be).

aanwijzingen bestaan dat ze aan deze criteria zouden kunnen voldoen, en dit met als doel om bijkomende persoonsgegevens of informatie te verzamelen die al of niet bevestigen dat de betrokkene beantwoordt aan de criteria van *terrorist fighters*.

VI.1.2. DE OPRICHTING VAN EEN GEMEENSCHAPPELIJKE GEGEVENSBANK VOOR HAATPROPAGANDISTEN (HP)

Met het KB van 23 april 2018 (KB HP) werd een nieuwe GGB 'haatpropagandisten' in het leven geroepen.

Deze gegevensbank is complementair aan de GGB TF en focust meer bepaald op de radicaliserende invloed die vaak aan de basis ligt van het plegen van terroristische acties of van extremisme dat kan leiden tot terrorisme. Het doel daarbij is om gegevens en informatie over vectoren van radicalisering (natuurlijke personen, rechtspersonen, feitelijke verenigingen) en de door hen aangewende middelen, samen te brengen.[170] De gedeelde gegevens en informatie moeten bijdragen tot de analyse, de evaluatie en de opvolging van deze entiteiten.[171]

De GGB HP is in de eerste plaats gericht op natuurlijke of rechtspersonen, ongeacht hun nationaliteit, hun verblijfplaats of hun zetel, die aan onderstaande cumulatieve voorwaarden voldoen:

a) ze berokkenen schade aan de beginselen van de democratie of de mensenrechten, de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat. Het is daarbij niet noodzakelijk dat de schade zich reeds heeft voorgedaan; potentiële schade is voldoende;
b) ze rechtvaardigen het gebruik van geweld (fysiek en psychisch geweld, intra- en extrafamiliaal geweld, homofoob geweld, cyberaanvallen …) of dwang als actiemethoden. De haatpropagandist geeft blijk van zijn intentie om schade te berokkenen en van de rechtvaardiging tot het gebruik van geweld of dwang door middel van concrete acties of kanalen. Deze intentie moet openbaar verwoordigd worden (bijv. door middel van een publicatie);
c) ze verspreiden deze overtuiging naar anderen met de bedoeling om een radicaliserende invloed uit te oefenen. De haatpropagandist wil het radicaliseringsproces ondersteunen of ertoe bijdragen;
d) er is een aanknopingspunt met België.

---

170 Bijvoorbeeld een Internetsite, traktaten, berichten op radio of TV, radio- of televisiekanalen, culturele of propgandacentra, lokalen ….

171 Deze datatbank vervangt de '*Joint Information Box*' (JIB) die werd beheerd door het OCAD. De JIB maakte het voorwerp uit van een gemeenschappelijk toezichtonderzoek I en P (VAST COMITÉ I, *Activiteitenrapport 2015*, 7-11).

Personen over wie ernstige aanwijzingen bestaan dat ze voldoen aan deze criteria worden voor maximum zes maanden opgenomen in de GGB HP. Wanneer deze termijn verstrijkt, worden de gegevens verwijderd, tenzij de entiteit blijkt te beantwoorden aan de criteria.

De werking van deze gegevensbank is identiek aan deze van de GGB TF. Ook de belangrijkste protagisten zijn dezelfde: de ministers van Binnenlandse Zaken en Justitie zijn de verwerkingsverantwoordelijken, de Federale Politie werd aangeduid als beheerder (art. 3 KB HP) en het OCAD als operationeel verantwoordelijke (art. 4 KB HP). Ook de functie van consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer werd opgenomen (art. 5 KB HP). Er werd evenwel niet gepreciseerd welke persoon of dienst deze opdracht moet waarnemen.

VI.1.3. HET DOORZENDEN VAN DE INFORMATIEKAART AAN DE LIVC-R

Een andere wijziging die in 2018 werd doorgevoerd, was het resultaat van de oprichting van de lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme (LIVC-R).[172] De LIVC-R vormt een platform waar specialisten van het lokale bestuur en lokale sociaalpreventieve organisaties samenzitten om tot een casusgerichte aanpak te komen van geradicaliseerden. Het opzetten van een LIVC-R behoort tot de bevoegdheid van de burgmeester. Artikel 4 van de Wet van 30 juli 2018 geeft de korpschef van de Lokale Politie (of de door hem aangestelde vertegenwoordiger) de toelating om aan de leden van de LIVC-R de informatiekaart van een persoon wiens casus wordt besproken, mee te delen. Deze informatiekaart vormt een uittreksel van de inlichtingenfiche en bevat persoonsgegevens en informatie die strikt beperkt zijn tot informatie die de bestemmeling nodig heeft (artt. 44/11/3 *quater* WPA en 11 KB FTF).

VI.1.4. EEN RECHTSTREEKSE TOEGANG VOOR DE NATIONALE VEILIGHEIDSOVERHEID

Bij de KB's van 23 april 2018 werd aan de Nationale Veiligheidsoverheid een rechtsstreekse toegang tot de gegevensbanken toegekend, en dat in het kader van zijn bevoegdheid tot toekenning van veiligheidsmachtigingen, -attesten en -adviezen.

---

172 Wet van 30 juli 2018 tot oprichting van de lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme, *BS* 14 september 2018.

VI.1.5. EEN NIEUWE RICHTLIJN M.B.T. DE INFORMATIEUITWISSELING

Op 22 mei 2018 vaardigden de ministers van Binnenlandse Zaken en Justitie een omzendbrief uit betreffende de informatieuitwisseling rond en de opvolging van *terrorist fighters* en haatpropagandisten. Deze richtlijn – die de classificatie 'Beperkte verspreiding' kreeg – regelt in detail de werking van de gemeenschappelijke gegevensbanken en bepaalt de rol van alle actoren, zoals de politie- en inlichtingendiensten, het OCAD, de Lokale Task Force, de LIVC-R …

VI.2. DE CONTROLEOPDRACHT

VI.2.1. HET VOORWERP VAN CONTROLE

Het COC en het Vast Comité I controleerden gezamenlijk de uitvoering van bepaalde aanbevelingen die ze in 2017 hadden geformuleerd. Daarnaast werd ook beslist om de wijze waarop de informatie aan de burgemeesters en aan derden werd verstrekt door respectievelijk de korpschefs van de Lokale Politie en de basisdiensten, aan een controle te onderwerpen.[173]

VI.2.2. DE OPVOLGING VAN DE IN 2017 GEFORMULEERDE AANBEVELINGEN

VI.2.2.1. Een wettelijke basis voor de verwerking van HTF en HP

Het COC en het Vast Comité I stelden in hun rapport van 2017 vast dat er gegevens worden verwerkt van 'haatpropagandisten' en '*homegrown terrorist fighters*' zonder dat hiervoor het KB FTF was gewijzigd of zonder dat er een nieuw Koninklijk besluit was genomen. Aan deze lacune werd verholpen door de in mei 2018 gepubliceerde KB's.

Toch werden de noodzakelijke 'voorafgaandelijke aangiften' niet verricht. Na het versturen van herinneringsbrieven aan de verwerkingsverantwoordelijken, werden bovenstaande aangiften eind november 2018 alsnog ontvangen (zie *infra*, VI.3).

VI.2.2.2. De aanwijzing van een veiligheidsconsulent

Na een nieuwe vraag van beide controleinstanties in 2018, stelden de ministers dat ze nog niet waren overgegaan tot de aanstelling van een consulent voor de

[173] Het rapport werd door beide instanties op 20 december 2018 goedgekeurd.

veiligheid en de bescherming van de persoonlijke levenssfeer en dit in afwachting van de aanpassing van het wetgevend kader inzake de bescherming van de persoonlijke levenssfeer.[174,175]

VI.2.2.3. De implementatie van een mechanisme voor het melden van veilgheidsincidenten

Vanuit zijn bevoegdheid als beheerder van de gegevensbank, meldde de Federale Politie dat in 2018 een procedure werd geïmplementeerd die elke gebruiker de mogelijkheid biedt een veiligheidsincident te melden. De Federale Politie voegde daaraan toe dat een procedure wordt uitgewerkt binnen het Stuurcomité van de GGB om de eventuele veiligheidsincidenten die door een gebruiker zouden worden veroorzaakt, te kunnen opvolgen en beheren.

Het COC en het Vast Comité I waren verheugd over dit initiatief. Ze herinnerden er echter aan dat de informaticabeveiliging een bevoegdheid is van professionals en dat het niet voldoende is om enkel de veiligheidsincidenten te behandelen die werden veroorzaakt/opgespoord/gemeld door de gebruikers, voor wie informaticabeveiliging niet de *core business* is.

In dit verband was het ontbreken van een veiligheidsconsulent – die de hoofdrol speelt in de beveiliging van informatiesystemen – zorgwekkend.

VI.2.2.4. De ontwikkeling van een bijkomende informaticatool

Personen waarvoor er enkel 'ernstige aanwijzingen' bestaan dat ze behoren tot een van de vijf FTF-categorieën van de gegevensbank, mogen worden opgenomen in de gegevensbank voor een maximumduur van zes maanden. Wanneer er tijdens deze termijn geen enkele bijkomende informatie is die de registratie binnen een van de vijf categorieën rechtvaardigt, moeten de namen van die personen worden gewist. Het COC en het Vast Comité I beveelden daarom een systeem van automatische notificatie aan. Ingevolge deze aanbeveling werd een verwittigingssysteem geïnstalleerd.

Daarnaast beschikte het OCAD niet over een informaticatool voor de opvolging van de bewaartermijnen en de verwijdering van gegevens van personen die voorkomen (of voorkwamen) in één van de vijf FTF-categorieën. In 2017 had het OCAD verduidelijkt dat dergelijke technische tool (nog) niet prioritair was. Hierover bevraagd in 2018, gaf de Federale Politie te kennen dat zolang het OCAD niet beslist een entiteit te wissen, zijn gegevens exploiteerbaar blijven in de GGB. Dit betekent dat indien het OCAD nalaat om op eigen initiatief op te treden, een per-

174 Intussentijd hadden alle diensten intern al wel een consulent aangewezen.

175 Het COC en het Vast Comité I konden deze rechtvaardiging niet onderschrijven. Beide instanties voeren immers een controle uit op basis van de geldende (en niet de toekomstige) regelgeving. Het COC en het Vast Comité I handhaafden dus hun eerdere aanbeveling.

soon voor onbepaalde tijd in de gemeenschappelijke gegevensbank kan bewaard blijven, wat in strijd is met de verplichting om (minimaal) driejaarlijks te onderzoeken of de registratie van een entiteit nog aangewezen is. Daarom bleef de aanbeveling om een informaticatool te ontwikkelen weerhouden.

VI.2.2.5. Informatiekaarten en mededelingen aan derden

De burgemeester is volgens de wet bestemmeling van de informatiekaarten van FTF'ers die hun verblijfplaats of woonplaats in zijn gemeente hebben, zijn gemeente regelmatig bezoeken of er regelmatig activiteiten organiseren. In 2017 had het OCAD geen enkel zicht op de wijze waarop aan deze verplichting was voldaan, wat het COC en het Vast Comité I ertoe aanzette de ontwikkeling van een IT-opvolgingstool aan te bevelen die moet toelaten de opvolging van deze verplichting te controleren.

Wat de mededelingen aan derde diensten betreft, herinnerden het COC en het Vast Comité I er al in 2017 aan dat uit het samenlezen van de artikelen 44/11/3*quater* WPA en 11 § 2 KB (F)TF volgt dat dergelijke mededelingen vooraf moeten worden geëvalueerd door de Federale Politie (in haar hoedanigheid van beheerder van de gegevensbank), het OCAD (in zijn hoedanigheid van operationele verantwoordelijke en dienst bedoeld in art. 44/11/3*ter* § 1 WPA) en de inlichtingendiensten. Het COC en het Vast Comité I benadrukten dat deze evaluatie noodzakelijkerwijs het aspect informatiebeveiliging moet omvatten. Deze vraag werd in 2018 opnieuw voorgelegd aan het OCAD, die de toepassingsmaatregelen die het op zijn niveau genomen had, detailleerde.

Het OCAD vermeldde niet uitdrukkelijk dat de in artikel 44/11/3*quater* WPA bedoelde evaluatie (systematisch en) vooraf wordt uitgevoerd voor wat betreft de doorgifte van (uittreksels) van de informatiekaart aan derde instanties (d.w.z. instanties die niet worden bedoeld door art. 44/11/3*ter* WPA). In dit kader is het belangrijk op te merken dat artikel 11 van het KB (F)TF sinds de vorige controle in 2017 werd gewijzigd door het KB van 23 april 2018 voor wat het extraheren en doorgeven van lijsten betreft.[176, 177] Uit deze wijziging volgt dat het extraheren van lijsten uitdrukkelijk is toegestaan voor diensten die over een rechtstreekse toegang beschikken, maar enkel voor interne behandeling door een personeelslid dat houder is van een veiligheidsmachtiging. Op het moment dat deze extrahering technisch mogelijk zal zijn (dit leek ten tijde van het onerzoek nog niet het geval), zal de doorgifte van lijsten van het OCAD aan deze diensten zijn nut verliezen.

De doorgifte van de lijsten aan andere diensten of instellingen (t.t.z. zij die niet over een rechtstreekse toegang beschikken) is in principe niet toegestaan tenzij

176 Een lijst bevat minimaal de geanonimiseerde gegevens van meerdere FTF (statistieken) en maximaal alle persoonsgegevens opgenomen in de informatiekaarten van deze FTF.

177 Doelstelling van de lijst in het licht van de wettelijke opdracht van de ontvanger, gebruik van de lijst uitsluitend voor die doelstelling, beperkte bewaring van de lijst, beveiliging ….

bepaalde voorwaarden zijn vervuld. Het OCAD heeft bij de controle medio 2018 verduidelijkt dat het op zijn niveau maatregelen heeft genomen met betrekking tot de doorgifte van lijsten. Het COC en het Vast Comité I herinnerden aan hun eerder geformuleerde vaststelling over de noodzakelijke technische beveiliging van de doorgifte indien deze via e-mail gebeurt. Bovendien achtten zij het gepast dat de basisdienst die de doorgifte uitvoert, de ontvanger van de lijst naar behoren zou informeren over de voorwaarden van mededeling van de lijst.[178]

VI.2.2.6. Uitvoering van een spontane controle van de loggings

Het COC en het Vast Comité I concludeerden in 2017 dat '*zelfs als de loggings niet onmiddellijk beschikbaar zijn voor de gebruikende diensten, moeten zij deze, via hun respectievelijke consulent voor de veiligheid en de bescherming van de persoonlijke levenssfeer, opvragen bij de beheerder van de gemeenschappelijke gegevensbank (met name de federale politie). Deze proactieve aanpak zou de betrokken dienst in staat stellen controle uit te oefenen op de legitimiteit van de toegang tot de gemeenschappelijke gegevensbank*'. Met uitzondering van één gecontroleerde dienst werd de aanbeveling om spontaan een controle van de loggings uit te voeren, niet opgevolgd.

VI.2.3. HET GEBRUIK VAN DE FTF-GEGEVENSBANK DOOR PARTNERDIENSTEN EN JUSTITIEHUIZEN

VI.2.3.1. Onvoldoende toegang tot de productieomgeving

Medio 2018 had een aanzienlijk aantal partnerdiensten en Justitiehuizen nog steeds geen toegang tot de productieomgeving van de gemeenschappelijke gegevensbank en gebruikte die bijgevolg niet.[179] Volgens het COC en het Vast Comité I kon deze situatie schadelijk zijn voor enerzijds de volledigheid van de gemeenschappelijke gegevensbank en anderzijds het nemen van een passende maatregel door de betrokken diensten of autoriteiten.

Het COC en het Vast Comité I formuleerden in dit kader volgende verduidelijkingen:

– De Algemene directie van het Crisiscentrum is een dienst die over een rechtstreekse bevraging van de gegevensbank beschikt (of moet beschikken). Indien dit nog niet is gerealiseerd, moeten maatregelen worden genomen om dit recht (deze verplichting) te concretiseren.

178 Dit kan bijvoorbeeld geregeld worden in een protocol.

179 Sommige diensten hadden eenvoudigweg geen toegang op technisch niveau (bijv. de *Administration générale des Maisons de Justice de la Communauté française*).

– In de praktijk hebben niet alle strafinrichtingen, doch slechts enkele diensten op het hoofdbestuur van het DG EPI een rechtstreekse toegang tot de gegevensbanken. Nochtans voorziet de regelgeving in een verplichting voor alle strafinrichtingen om de GGB's te voeden. Indien men deze praktijk wenst te behouden, dient het wetgevend kader in die zin te worden aangepast.

VI.2.3.2. De situatie inzake veiligheidsmachtigingen

Op het ogenblik van de controle beschikten de leden van de diensten die toegang hadden tot de gemeenschappelijke gegevensbank over de vereiste veiligheidsmachtiging. Het COC en het Vast Comité I beveelden in dat verband aan om de (vrij lange) procedures voor de aanvraag van de veiligheidsmachtigingen snel op te starten. Omgekeerd moet systematisch elk verlies van de *need to know* van een personeelslid worden gemeld, zodat wordt vermeden dat toegangsrechten die niet noodzakelijk zijn, worden behouden of dat veiligheidsonderzoeken die ondertussen nutteloos zijn geworden, worden voortgezet.

VI.2.3.3. De aanwijzing van een veiligheidsconsulent binnen elke dienst

Alle diensten die op het ogenblik van de controle beschikten over een rechtstreekse toegang of rechtstreekse bevraging, hadden een veiligheidsconsulent aangesteld.

VI.2.3.4. De tevredenheid van de partnerdiensten

Diverse actoren benadrukten het nuttige en collaboratieve aspect van de gegevensbank. In de praktijk uitten verschillende diensten echter de wens om met een systeem te kunnen werken dat de automatische vergelijking van de in de gemeenschappelijke gegevensbank opgenomen personen met hun eigen gegevensbank, mogelijk maakt. Door de wijziging van artikel 11 van het KB (F)TF in 2018 hebben de diensten die over een rechtstreekse toegang beschikken, nu de mogelijkheid om lijsten uit de gegevensbank te halen, '*en dit enkel voor intern gebruik*'. Deze bepaling werd eveneens gewijzigd om toe te laten dat de basisdiensten, na de vereiste evaluatie, lijsten kunnen meedelen '*aan andere diensten of instellingen*' (d.w.z. diensten of instellingen die niet over een rechtstreekse toegang beschikken).

Op operationeel niveau is deze vraag naar een IT-toepassing logisch en begrijpelijk: automatische vergelijkingen besparen tijd en capaciteit. Geautomatiseerde vergelijkingen vereisen echter enerzijds uitgebreide tests en anderzijds dat alle beslissingen worden genomen na menselijke tussenkomst en validatie. Bovendien moeten maatregelen worden genomen om ervoor te zorgen dat het gebruik van deze lijsten door derden voldoet aan de vereiste veiligheidsvoorwaarden (vertrouwelijkheid, integriteit …).

De Federale Politie voorzag de inproductiestelling van deze functionaliteit voor begin 2019. Het COC en het Vast Comité I zullen dit aspect opvolgen.

VI.2.3.5. Aanpassing van de validatieprocedures ingevolge de wijzigingen van het regelgevend kader

De validatieprocedures die door bepaalde diensten vóór of naar aanleiding van de controle door het COC en het Vast Comité I werden meegedeeld, hadden alleen betrekking op de FTF en moeten worden geactualiseerd voor de HTF en de HP. Bovendien moet het Vlaams Agentschap Jongerenwelzijn overgaan tot de implementatie van het in artikel 8 van het KB TF bedoelde interne validatiesysteem.

VI.2.4. OVER DE INFORMATIE AAN DE BURGEMEESTERS EN DE DOORGIFTE VAN (UITTREKSELS) VAN INFORMATIEKAARTEN OF VAN LIJSTEN AAN DERDE INSTANTIES

Bij gebrek aan een betrouwbaar controlemiddel werd de controle van het COC en het Vast Comité I op de doorgifte van de informatiekaart door de korpschefs van de Lokale Politie aan de burgemeesters uitgesteld. In dat kader beveelden beide instanties het OCAD en de Federale Politie aan om de basisdiensten (en in het bijzonder de politiezones) te sensibiliseren over de noodzaak om systematisch de geïnformatiseerde indicatoren (data van doorgifte van een (update van de) informatiekaart) in te vullen om de toekomstige controle te vergemakkelijken.

Tijdens de periode van het onderzoek werden door het OCAD geen (uittreksels) van informatiekaarten doorgegeven aan derde overheden of aan derde eenheden (d.w.z. volgens de voorbereidende werkzaamheden van de wet, aan instanties die niet onder artikel 44/11/3*ter* WPA vallen).[180]

In juli 2018 gaf het OCAD dat het maandelijks lijsten met de namen van de personen in de gemeenschappelijke gegevensbank naar '*een beperkt aantal diensten*' had doorgegeven zonder te specifiëren om welke diensten het ging. De dienst verklaarde dat de '*zending van de lijsten naar die 'partners' door de vier basisdiensten bij consensus werd goedgekeurd*'.

De regelgeving over het extraheren en de doorgifte van lijsten werd in 2018 gewijzigd. Het extraheren van lijsten is voortaan uitdrukkelijk toegestaan voor diensten die over een rechtstreekse toegang beschikken, maar enkel voor interne behandeling en wanneer die behandeling wordt verricht door een personeelslid

[180] Deze doorgifte zou een voorafgaande gezamenlijke beoordeling hebben vereist van de Federale Politie, het OCAD en de (andere) basisdiensten (art. 44/11/3*quater* WPA). Het OCAD heeft geen verduidelijking verstrekt over eventuele doorgiften door andere basisdiensten in die context (het is overigens niet zeker dat het OCAD over die gegevens beschikt).

dat houder is van een veiligheidsmachtiging. De doorgifte van de lijsten aan andere diensten of instellingen is alleen toegestaan onder bepaalde voorwaarden (*supra*). Het COC en het Vast Comité I zullen de naleving van deze nieuwe regelgeving in het kader van een latere controle verifiëren.

VI.3. TWEE GEMEENSCHAPPELIJKE ADVIEZEN

Ingevolge de wijzigingen die werden aangebracht door de twee KB's van 23 april 2018 en conform artikel 44/11/3*bis* § 3 WPA, legden de ministers van Binnenlandse Zaken en Justitie twee 'voorafgaandelijke aangiften' aan het COC en het Vast Comité I voor advies voor.[181] De belangrijkste opmerkingen worden hieronder samengevat:

- Er werd reeds een aanvang genomen met de verwerking van persoonsgegevens- en informatieverwerking over respectievelijk HTF en HP zonder voorafgaandelijke aanpassing van het juridische kader (art. 44/11/3*bis* § 4, tweede lid, WPA) en zonder dat een voorafgaandeljike aangifte werd ingediend (art. 44/11/3*bis* § 3 WPA). Het COC en het Vast Comité I wezen er op dat de naleving van beide bepalingen één van de hoekstenen vormt waarop de controle op de gmeenschappelijke gegevensbanken berust;
- Hoewel de KB's TF en HP al enkele maanden gepubliceerd waren, bevatte de aangifte geen enkele concrete informatie over de rechtstreekse toegang van de NVO;
- De aangiften lieten ook de mogelijkheid onbesproken om lijsten met persoonsgegevens en informatie uit de gegevensbank te extraheren, terwijl dit een belangrijke wijziging betrof;
- Het COC en het Vast Comité I merkten opnieuw op dat geen melding werd gemaakt van de aanstelling van een veiligheidsconsulent;
- Beide instanties betreurden dat wat de communicatie over de inforamtiekaarten aan de burgemeesters betreft, de aangifte geen preciseringen aanbracht inzake de toepassingsfrequentie van artikel 12 van de KB's TF en HP.[182] Daarenboven maakte de aangifte geen gewag van de Wet van 30 juli 2018 houdende oprichting van de lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme (LIVC-R). Daarin wordt voorgeschreven dat de korpschef en/of zijn vertegenwoordiger van de Lokale Politie de toelating hebben om aan de leden van de LIVC-R de informatiekaart van een persoon wiens casus voorwerp van discussie vormt, mee te delen.

---

181 Deze gezamenlijke adviezen 001/CPR-C.O.C./2018 en 002/CPR-C.O.C./2018 kunnen worden geconsulteerd op www.comiteri.be.

182 Wat moet bijvoorbeeld worden verstaan onder de 'gemeenten die *regelmatig* worden bezocht' door een entiteit, of nog een gemeente waarin een entiteit '*regelmatig* een of meerdere activiteiten organiseert'.

HOOFDSTUK VII
ADVIEZEN

Artikel 33, zevende lid, W.Toezicht bepaalt dat het Comité '*enkel op verzoek van de Kamer van volksvertegenwoordigers of van de bevoegde minister advies [mag] uitbrengen over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin de beleidslijnen van de bevoegde ministers worden geformuleerd.*' In 2018 werd het Comité op basis van deze bepaling slecht éénmaal om een advies verzocht, en dit door de Kamercommissie Justitie (*infra*).

Daarnaast dient het Comité ook advies te verlenen als Bevoegde toezichthoudende autoriteit (BTA) in het kader van de verwerking van persoonsgegevens alsook bij de wettelijke regeling in verband met gemeenschappelijke databanken, maar dan samen met het COC. Deze laatste twee adviesbevoegdheden worden behandeld in Hoofdstuk V en Hoofdstuk VI.

VII.1. ADVIES BIJ HET WETSONTWERP AANGAANDE DE VERWERKING VAN PERSOONSGEGEVENS

Op 14 december 2017 werd het Vast Comité I door Kamercommissie Justitie gevraagd advies te verlenen aangaande het wetsontwerp betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. Het ontwerp, dat bijzonder complex en technisch van aard was en betrekking had op een thema van groot maatschappelijk belang, telde niet minder dan 280 artikelen. Aangezien de tekst tot net voor zijn indiening in het Parlement voorwerp uitmaakte van een politiek debat, waarbij bepaalde opties nog ter discussie stonden en ook bepaalde wijzigingen werden aangebracht, kon het Comité het gehele ontwerp niet in detail bestuderen.

Het Comité was dan ook in de onmogelijkheid om een gedegen advies te formuleren over alle aspecten van de regeling die het aanbelangden. Het Comité wees in het bijzonder op twee elementen: enerzijds de complexiteit en de draagwijdte van de ontworpen regeling – waarbij de vraag zich stelde of een effectieve controle op de verwerking van persoonsgegevens steeds de eerste bekommernis was – en de soms onlogische en onbegrijpelijke redactie van het ontwerp en anderzijds de absolute noodzaak aan een kaderuitbreiding voor het Comité voor

de uitvoering van de talrijke en belangrijke taken die het in het ontwerp kreeg toebedeeld.[183]

Het Comité benadrukte in zijn advies[184] dat het de keuze om gegevens die betrekking hebben op 'nationale veiligheid' niet volledig uit te sluiten van alle beschermingsmechanismen, kon toejuichen. Wel leidde de wijze waarop deze keuze werd ingevuld (onder meer door de creatie van meerdere gegevensbeschermingsautoriteiten) tot een bijzonder complex systeem van toezicht waarbij onvermijdelijk onduidelijkheden zouden ontstaan bij alle betrokken actoren: administratieve overheden, de diverse gegevensbeschermingsautoriteiten en – niet in het minst – de burger voor wie de bescherming bedoeld is.

183 De Wet van 3 december 2017 waarbij de gegevensbeschermingsautoriteit werd opgericht, voorzag in een uitgebreide structuur met zes verschillende entiteiten, maar voor het Comité was nergens sprake van bijkomende middelen op budgettair, personeels- of IT-vlak. Het Comité drong aan op een onmiddellijke uitbreiding van zijn personeelskader. Zoniet zouden niet alleen de andere, eveneens in volume toegenomen opdrachten van het Comité hieronder lijden, maar zouden ook de nieuwe opdrachten nauwelijks kunnen worden uitgevoerd. Dergelijke situatie brengt de onafhankelijke, democratische controle op de inlichtingensector ernstig in het gedrang.

184 Het integrale advies is beschikbaar op www.comiteri.be.

HOOFDSTUK VIII
DE OPSPORINGS- EN GERECHTELIJKE ONDERZOEKEN

Naast zijn medewerking aan de toezichtonderzoeken, voert de Dienst Enquêtes I van het Comité ook onderzoeken naar leden van de inlichtingendiensten die verdacht worden van een misdaad of wanbedrijf. Dit doet de enquêtedienst in opdracht van de gerechtelijke overheden. Deze bevoegdheid staat omschreven in artikel 40, derde lid van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse. Met de Wet van 10 juli 2006 betreffende de analyse van de dreiging werd deze bevoegdheid uitgebreid tot misdaden of wanbedrijven gepleegd door de leden van het Coördinatieorgaan voor de dreigingsanalyse (OCAD). Wat betreft de leden van de andere 'ondersteunende diensten' geldt deze bepaling alleen ten aanzien van de verplichting om relevante inlichtingen aan het OCAD mee te delen (artt. 6 en 14 W.OCAD).

Wanneer zij een opdracht van gerechtelijke politie vervullen, staan de leden en de directeur van de Dienst Enquêtes I onder het toezicht van de procureur-generaal bij het hof van beroep of van de federaal procureur (art. 39 W.Toezicht) en heeft het Vast Comité I geen zeggenschap over hen. De voorzitter van het Vast Comité I moet er echter zorg voor dragen dat de uitvoering van de opdrachten van gerechtelijke politie de uitvoering van de toezichtonderzoeken niet hindert. De reden daarvoor ligt voor de hand: het controleorgaan 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 2018 voerde de Dienst Enquêtes I onderzoeksdaden uit in het kader van zijn gerechtelijke opdracht, meer bepaald in drie opsporingsonderzoeken.

Vooreerst werd een in 2017 opgestarte onderzoek voortgezet. Het werd gevoerd op vordering van het Federaal Parket en betrof de mogelijke betrokkenheid van een lid van een inlichtingendienst bij een misdaad of wanbedrijf tegen de inwendige en uitwendige veiligheid van de Staat. Het onderzoek werd niet afgerond in 2018.

Een tweede zaak betrof een vervolg op een klacht van een privé-persoon tegen een personeelslid van ADIV. In 2014 werd door betrokkene bij het Vast Comité I een klacht ingediend. Hierover werd ook door het Comité in het kader van zijn algemene toezichtsbevoegdheid een onderzoek uitgevoerd.[185]

Ten slotte leverde de Dienst Enquêtes I bijstand in een onderzoek van de Dienst belast met de gespecialiseerde gerechtelijke opdrachten in militair milieu van de Federale Politie naar vermoedelijke feiten van pestgedrag binnen een inlichtingendienst.

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 2018 één melding in die zin.

185 VAST COMITÉ I, *Activiteitenverslag 2015*, 41 ('II.9. Klacht over het verstrekken van persoonlijke informatie door een inlichtingenagent aan een derde').

HOOFDSTUK IX
EXPERTISE EN EXTERNE CONTACTEN

IX.1. EXPERT OP DIVERSE FORA

Leden van het Vast Comité I en van zijn personeel werden in 2018 diverse malen als expert geconsulteerd door binnen- en buitenlandse publieke en private instellingen:

- De griffier nam eind februari 2018 op uitnodiging van het Geneva Centre for the Democratic Control of Armed Forces (DCAF) in Skopje (Macedonië) deel aan het panelgesprek 'Why, When and How to engage in Oversight Fields Visits' in het kader van het DCAF Assistance Program for the Parliament of the Republic of Macedonia. Daar werd onder meer de draft van de 'Guidelines for intelligence oversight for parliamentary committees in the Assembly of the Republic of Macedonia' voorgesteld[186];
- De toenmalige voorzitter van het Comité maakte in februari 2018 deel uit van de jury voor een doctoraatsverdediging aan de Faculté des sciences économiques, sociales, politiques et de communication van de Université catholique de Louvain (UCL)[187];
- Er werd vanuit het Comité meegewerkt aan een verkenning van parlementaire controle van inlichtingen- en veiligheidsdiensten in het buitenland op verzoek van de Nederlandse Tweede Kamer;
- Op 25 mei 2018 organiseerden het Vast Comité I en het Vast Comité P een zitting in het Parlement naar aanleiding van hun 25-jarig bestaan. Naast enkele politici en internationale gastsprekers, werden ook vertegenwoordigers van de gecontroleerde diensten uitgenodigd om hun visie weer te geven.
- Van 24 tot 31 mei 2018 bracht de United Nations Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism, Mevr. Fionnuala Ní Aoláin, een officieel bezoek aan België. Ook het Vast Comité I werd vereerd met een bezoek en kon zijn visie toelichten.[188]

---

186 DCAF, *Guidelines for intelligence oversight for parliamentary committees in the Assembly of the Republic of Macedonia*, Mei 2018, (www.dcaf.ch).

187 A. LELIEVRE, *La communication web des services de renseignement. Etude sémio-pragmatique. Thèse présentée dans le cadre du Doctorat en Information et Communication*, UCL, février 2018.

188 Hierover: Human Rights Council, Report of the Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism – Visit to Belgium, A/HRC/40/52/Add. 5, 27 februari 2019, 33 p.

- Een ere-voorzitter van het Vast Comité I oefent sinds 2011 het voorzitterschap uit van het *Belgian Intelligence Studies Centre* (BISC). Dat centrum stelt zich tot doel de inlichtingen- en veiligheidsdiensten en de wetenschappelijke wereld dichter bij elkaar brengen en een bijdrage te leveren aan de reflectie over inlichtingenvraagstukken. In juni 2018 organiseerde het BISC een studiedag over 'International collaboration regarding intelligence services and intelligence studies'.[189]
- De Directeur van de Dienst Enquêtes I reflecteerde in de Cahiers inlichtingenstudies over de werking van het Vast Comité I sinds 2013[190];
- Begin april 2018 modereerde de voorzitter van het Comité het panelgesprek 'L'Europe et le renseignement' tijdens het colloquium 'Le renseignement et son contrôle', georganiseerd door de Franse Conseil d'Etat en de Commission nationale de contrôle des techniques de renseignement (CNCTR);
- De griffier van het Comité nam deel aan het European Intelligence Oversight Network (EION), waarbij experten vanuit diverse toezichthoudende autoriteiten, NGO's (bijv. Stiftung Neue Verantwortung) als vanuit de academische wereld reflecteerden over 'oversight innovation' en de uitwisseling van informatie tussen nationale toezichthouders;
- In september 2018 vond in Parijs een driedaags colloquium plaats getiteld 'SIGINT intelligence transnational activities and national security in France and Europe – a changing landscape'. Een ere-voorzitter sprak er als *keynote speaker* over 'SIGINT Intelligence, Surveillance, Ethics and Control'. Van de gelegenheid werd gebruik gemaakt om de rol van het Vast Comité I als controleorgaan toe te lichten en het toenemende belang van SIGINT in een inlichtingencontext te accentueren;
- De griffier van het Vast Comité I werd uitgenodigd in het kader van het opleidingsonderdeel 'Intelligence' van de Master in de internationale betrekkingen en de diplomatie (Universiteit Antwerpen) om er de werking van het Comité toe te lichten;
- Het Vast Comité I vormde de gesprekspartner van de *Stiftung Neue Verantwortung* tijdens een gedachtewisseling omtrent 'New challenges and changes to democratic control of intelligence in Belgium and Germany';
- Er werd een beroep gedaan op de juridische expertise van het Comité in een praktijkseminarie bestemd voor politie, magistratuur en advocatuur rond het thema 'classificatie en veiligheidsmachtigingen';
- Het hoofd van de juridische dienst publiceerde in 2018 een wetenschappelijke bijdrage over 25 jaar Belgisch toezicht op de inlichtingen- en veiligheidsdiensten[191];

---

189 Het BISC wijdde zijn 9de cahier aan de ere-voorzitter van het Comité (M. COOLS et al, eds., *Methodologie inlichtingenstudies – Méthodologie des études de renseignement. Liber Amicorum Guy Rapaille*, Gompel&Svacina, Oud-Turnhout, 2018, 280 p.

190 F. FRANCEUS, 'Et demain? Het Vast Comité I sinds 2013', in M. COOLS et al, *o.c.*, 2018, 19-26.

191 W. VAN LAETHEM, 'The Rule of Law and 25 Years of Intelligence Oversight in an Ever-changing World: the Belgian Case' in I. LEIGH en N. WEGGE (eds.), *Intelligence Oversight in the Twenty-First Century. Accountability in a Changing World*, Londen, Routledge, 2018, 208 p.

– De (ere-)voorzitter(s) en raadsheren van het Vast Comité I namen het woord tijdens de tweedaagse 'Conférence européenne des autorités de contrôle du renseignement' (Parijs, 6 en 7 december 2018).

IX.2. SAMENWERKINGSPROTOCOL MENSENRECHTENINSTELLINGEN

De creatie van een nationaal Mensenrechteninstituut, een engagement dat werd aangegaan bij de ondertekening van het Protocol bij het VN-verdrag tegen foltering, werd in België in 2018 nog niet gerealiseerd.[192] De effectieve oprichting van een dergelijk instituut kon pas na ratificatie van het protocol, waarmee – naast het federale Parlement – ook alle deelstaten moesten instemmen. In uitvoering hiervan verschenen de instemmingsaktes van de Vlaamse, Franstalige en Duitstalige Gemeenschap en van het Waals Gewest in het Staatsblad en werd ook de akte van de Verenigde Vergadering van de Gemeenschappelijke Gemeenschapscommissie gepubliceerd.

In afwachting van de effectieve oprichting van het instituut, resulteerde de vergaderingen met diverse instellingen met een mandaat op het gebied van mensenrechten[193] in januari 2015 in een samenwerkingsprotocol.[194] Daarin kwamen alle deelnemende instanties overeen om praktijken en methoden uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen.

De activiteiten van dit platform namen in 2018 de vorm aan van overlegvergaderingen waarin zowel algemene problematieken (bijv. België en de bevordering en bescherming van mensenrechten, de oprichting van de Centrale Toezichtsraad voor het Gevangeniswezen, een voorstelling van de diverse deelnemende instituten …) als de uitwisseling van werkwijzen en methodologieën over concrete individuele dossiers aan de orde waren. In 2018 nam Myria – voorheen het Centrum voor gelijkheid van kansen en voor racismebestrijding – het voorzitterschap over van de Nationale Commissie voor de Rechten van het Kind.

192 Met de Wet van 12 mei 2019 tot oprichting van een Federaal Instituut voor de bescherming en bevordering van de rechten van de mens (*BS* 21 juni 2019) werd de kwestie ook op federaal niveau geregeld.

193 Zoals 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.

194 Samenwerkingsprotocol van 13 januari 2015 tussen de instellingen met een volledig of gedeeltelijk mandaat belast met de eerbiediging van de rechten van de mens.

IX.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)[195] werken daarom samen om het hoofd te bieden aan die uitdagingen door werkwijzen te vinden om het risico op een hiaat in het toezicht te verkleinen.

Sinds 2015 voerden deze toezichthouders gelijktijdig maar elk binnen het kader van zijn mandaat en bevoegdheden, een onderzoek naar de internationale uitwisseling van persoonsgegevens in het kader van de strijd tegen FTF (cf. I.6.1.). Afgelopen jaren werden diverse *expert meetings* georganiseerd waarbij methoden, *best practices*, juridische en praktische problemen werden besproken en ervaringen uitgewisseld.

Begin november 2018 werd door de deelnemende toezichtorganen een gemeenschappelijke verklaring en perscommuniqué opgesteld.[196] In de gemeenschappelijke verklaring werden een aantal manieren opgesomd om in deze vooruitgang te boeken. Immers, om het risico op 'blinde vlekken' in het toezicht te voorkomen, is er nood aan een intensifiëring van de samenwerking tussen de toezichtinstanties. Een waardevolle en noodzakelijke stap naar een nauwere samenwerking op het gebied van het toezicht is het verminderen van de geheimhouding tussen de toezichtinstanties. Nu de inlichtingendiensten frequent gegevens uitwisselen, moet dat ook mogelijk zijn voor de toezichthouders; ook zij moeten vervolgens de uitgewisselde inlichtingen kunnen bespreken. Een andere stap in de goede richting is de ontwikkeling van nieuwe juridische en technische toezichtmethoden met het oog op de feitelijke beoordeling van de internationale gegevensuitwisseling en het bestaan en functioneren van gemeenschappelijke waarborgen voor de bescherming van grondrechten.

IX.4. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

Het Vast Comité I onderhield ook in 2018 nauwe contacten met diverse buitenlandse toezichthouders.

Tijdens een colloquium dat begin april 2018 plaatsvond in de Franse *Conseil d'Etat* – en de *Commission nationale de contrôle des techniques de renseignement*

195 Zie VAST COMITÉ I, *Activiteitenverslag 2015*, 80-81.

196 Zie bijlage D. 'Versterking van het toezicht op de internationale gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten'.

(CNCTR) als mede-organisator optrad – en waarop een vertegenwoordiging van het Vast Comité I aanwezig was, konden de relaties verder worden uitgebouwd. Niet alleen werden de banden aangehaald met de Franse *Délégation parlementaire au renseignement* (DPR), maar werd ook van gedachten gewisseld met de Nederlandse Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD), de Britse *Investigatory Powers Commissioner's Office* (IPCO), het Duitse *Parlamentarisches Kontrollgremium PKgr* …

In juni 2018 werd in Berlijn een werkbezoek georganiseerd tussen een vertegenwoordiging van het Vast Comité I en het Duitse *Parlamentarisches Kontrollgremium*, waarbij langs Belgische zijde de activiteitenverslagen alsook de onderzoeken na de terreuraanslagen in Parijs en Brussel werden toegelicht.

Nog diezelfde maand werd in co-organisatie met de voorzitter van de Kamer van Volksvertegenwoordigers in Brussel een briefing georganiseerd met de Georgische Office of the Personal Data Protection Inspector en vertegenwoordigers van het Georgische Parlement. Ook de Veiligheid van de Staat en het Coördinatieorgaan voor de dreigingsanalyse werd betrokken bij dit initiatief. Het opzet was een beter begrip van onafhankelijk toezicht op de inlichtingendiensten, met in het bijzonder aandacht voor de gehanteerde methodologie, middelen en technieken om aan de vereisten van een efficiënte en effectieve democratische controle te kunnen beantwoorden.

Op verzoek van het Noorse ministerie van Justitie vond op de ambassade van Noorwegen in Brussel in oktober 2018 een ontmoeting plaats met vertegenwoordigers van het Noorse ministerie van Justitie en ambassademedewerkers over de strategische planning in het kader van de samenwerking tussen inlichtingendiensten.

Begin november 2018 vond op de Franse ambassade in Brussel een onderhoud plaats met een parlementaire delegatie, samengesteld uit leden van de *Délégation parlementaire au Renseignement*, de *Commission de vérification des fonds spéciaux* en de *Assemblée nationale*. De gedachtenwisseling vond plaats in het kader van de voorbereiding van een gemeenschappelijk initiatief van de voorzitters van de Assemblée nationale en van de Senaat over '10 ans de controle parlementaire du renseignement: l'exigence démocratique est-elle satisfaite?'

Nog in november 2018 werd in Valetta (Malta) het *International Intelligence Oversight Forum* over 'Latest Challenges to Intelligence Oversight in a Democracy', georganiseerd door de *Special Rapporteur for Privacy* (SRP) van de Verenigde Naties. Hieraan namen zowel vertegenwoordigers van toezichthouders, inlichtingendiensten, universiteiten en NGO's deel. Het 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.

Het Comité werd op 21 en 22 november 2018 uitgenodigd door het Zwitserse toezichtsorgaan *Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten* (Autorité de surveillance indépendente des activités de renseigne-

ment) voor een bezoek in Bern met het oog op het versterken van de banden tussen beide toezichthouders.

Het Vast Comité I organiseerde samen met de *Commission nationale de contrôle des techniques de renseignement* de tweedaagse 'Conférence européenne des autorités de contrôle du renseignement' (Parijs, 6 en 7 december 2018). De conferentie vond plaats achter gesloten deuren; er waren deelnemers uit 15 verschillende Europese landen afgevaardigd (*supra*).

Ten slotte werden, met het oog op het creëren van een normatief kader voor de internationale samenwerking tussen inlichtingendiensten en de toezichthouders, de eerste contacten gelegd met diverse BENELUX-instanties.

IX.5. AANWEZIGHEID IN DE MEDIA

Het Vast Comité I wordt regelmatig gesolliciteerd door de geschreven en gesproken media om toelichting te geven over zijn werkzaamheden dan wel deze van de inlichtingendiensten. Het Vast Comité I ging een aantal maal op deze verzoeken in.

Datum	Onderwerp/titel	Forum
16 januari 2018	Inteligencia estratégica, hoy	Defensa.com
27 januari 2018	Eindelijk controle op kas Staatsveiligheid	De Tijd
27 januari 2018	Militair geheime dienst ontsnapt aan Rekenhof	De Tijd
30 januari 2018	Eddy Testelmans, l'ancien chef des renseignements de l'armée, sous le feu des critiques	La Libre Belgique
13 februari 2018	"Bruxelles est un nid d'espions": la capitale belge est un carrefour mondial de l'espionnage, confirme le patron du Comité R	Sud Presse
1 maart 2018	Belgische terroristen-databank rammelt nog	De Tijd
6 maart 2018	Ex-leden willen dat Comité I rol van Staatsveiligheid onderzoekt	Knack
6 maart 2018	Des anciens du Comité R réclament une enquête sur la Sûreté de l'État	Le Vif
13 maart 2018	Serge Lipszyc, seul candidat à la présidence du Comité R	Le Vif
23 maart 2018	Omstreden benoeming voor adviseur premier	De Standaard
23 maart 2018	Candidate to head security committee draws fire from the opposition	The Brussels Times
28 maart 2018	Adviseur premier Michel aan het hoofd van Comité I	De Standaard

Datum	Onderwerp/titel	Forum
13 april 2018	België opent geheime archieven om mysterieuze dood VN-baas op te helderen	De Morgen
18 april 2018	Comment la Belgique a rendu la liberté au commanditaire présumé des attentats de Paris et de Bruxelles	Paris Match
19 april 2018	La Chambre désigne un collaborateur de Charles Michel à la tête du Comité R	Sudinfo.be
19 april 2018	Kamer keurt omstreden benoeming van adviseur premier goed	De Standaard
24 mei 2018	Guy Rapaille, président du Comité R: "Il a fallu attendre les attentats pour obtenir plus de moyens"	Rtbf.be
24 mei 2018	Contrôler la police et les renseignements: Guy Rapaille invité de Jeudi en Prime	Rtbf.be
25 mei 2018	Belgische militairen zetten in 2016 voet aan de grond in Syrië	Vrt.be
5 juni 2018	Ça roule entre le FBI et la Belgique	Le Soir
6 juni 2018	Wat vertellen Belgische archieven over dood Dag Hammarskjöld in 1961?	Mo.be
6 juni 2018	Rekenkamer: "Privacycommissie, Comité P en andere aan Kamer verbonden instellingen moeten gesaneerd worden"	Het Laatste Nieuws
12 juni 2018	Guy Rapaille (Comité I): 'Russische inmenging bij onze verkiezingen? Dat valt te vrezen, ja'	Knack
13 juni 2018	"Gare à l'action des services turcs et marocains"	Le Soir
13 juni 2018	Bélgica investiga si sus servicios de inteligencia conocían el supuesto espionaje del CNI a Puigdemont	Público
13 juni 2018	Belgique: interrogations sur un possible espionnage de Puigdemont par l'Espagne sans préavis	Le Point
13 juni 2018	België laat schaduwoperatie tegen Puigdemont onderzoeken	De Tijd
13 juni 2018	Guy Rapaille: "Une ingérence russe lors des élections est à craindre"	Le Vif
13 juni 2018	Le renseignement belge s'inquiète d'une possible ingérence de la Russie lors des élections	Sudinfo.be
13 juni 2018	Steven Vandeput confirme un risque d'actions de désinformation russes en Belgique: "on se prépare"	Rtbf.be

Datum	Onderwerp/titel	Forum
14 juni 2018	Militaire veiligheidsdienst draait vierkant	De Standaard
14 juni 2018	Dysfonctionnements au sein du service de renseignement militaire	Rtbf.be
15 juni 2018	Comité I-voorzitter Guy Rapaille spreekt	Apache
16 juni 2018	Guy Rapaille, président du Comité R: "La Belgique doit craindre l'ingérence russe"	Le Soir – Le Vif
24 juni 2018	Elections en Turquie: la propagande passe aussi par les mosquées	La Libre Belgique
25 juli 2018	À Bruxelles, une incroyable histoire de faux papier et d'espions russes	Le Monde
30 augustus 2018	Les services de renseignement doivent pouvoir déplaire au politique. Entretien avec Guy Rapaille	Le Vif
11 september 2018	Guy Rapaille "Les services de renseignement doivent pouvoir déplaire aux politiques"	Rtbf.be
11 september 2018	Au bout du jour: interview de Monsieur Rapaille	Rtbf.be
12 november 2018	Filip Dewinter, espion …pour la Chine?	La Libre Belgique
12 november 2018	Filip Dewinter vraagt onderzoek van Comité I	De Standaard
2 december 2018	Guy Rapaille: "La transparence des services de renseignements a été parfaite"	Le Soir
21 december 2018	Elk bedrijf moet info geven aan Staatsveiligheid	De Tijd
21 december 2018	Les entreprises doivent fournir des informations sur demande de la Sûreté de l'État	Rtbf.be

HOOFDSTUK X
HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN

Het Beroepsorgaan is een 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, ten slotte, de veiligheidsadviezen. Daarnaast kan het Beroepsorgaan ook optreden als 'annulatierechter' tegen beslissingen van publieke of administratieve overheden om in een bepaalde sector of voor een bepaalde plaats of evenement veiligheidsattesten of -adviezen aan te vragen.[197]

Het Beroepsorgaan is samengesteld uit de voorzitter van het Vast Comité I, de voorzitter van het Vast Comité P en, sinds midden 2018 (zie X.2.2.), de voorzitter van 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 en door de administratie van het Vast Comité I.

De activiteiten van het Beroepsorgaan hebben een directe impact op zowel de budgettaire als personele middelen van het Vast Comité I. Immers, alle werkingskosten worden gedragen door het Vast Comité I, dat daarnaast niet enkel én de voorzitter én de griffier levert, doch ook het nodige administratief personeel dat moet instaan voor de voorbereiding, de behandeling en de afhandeling van de beroepen. Deze werkprocessen zijn erg tijdsintensief.

---

197 Zie hierover uitgebreid VAST COMITÉ I, *Activiteitenverslag 2006*, 91-119. De regels die daarin worden toegelicht, houden evenwel geen rekening met de wijzigingen aangaande de veiligheidsadviezen die werden ingevoerd door de wetten van 23 februari 2018 en 13 september 2018. Zij worden hieronder besproken (zie X.2.1.2 en X.2.2).

X.1. EEN BIJWIJLEN ZWARE EN COMPLEXE PROCEDURE

Alhoewel in 2018 een daling van het aantal dossiers werd opgetekend (van 192 naar 158), betekende dit geen verlaging van de werklast aangezien de dossiers steeds complexer worden op het vlak van administratief beheer, de terechtzittingen en de beslissingen. Dit vertaalt zich in een toenemende werklast.

Zo voldoen heel wat dossiers niet aan de vereisten gesteld in de artikelen 2 en 3 van het KB Beroepsorg., waarin respectievelijk staat dat '*alle processtukken aan het beroepsorgaan worden toegezonden bij ter post aangetekende brief*' en dat '*de beroepsakte wordt ondertekend en gedagtekend door de eiser of door een advocaat*'. De griffier zag zich dan ook genoodzaakt de eisers hierop te wijzen met het oog op de regularisatie van de situatie binnen de wettelijke termijn.[198]

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. Deze vertraging kan evident ingaan 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 overgezonden, wordt vaak overschreden. Op die manier wordt het ook voor het Beroepsorgaan moeilijk 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 ook hier bijkomende handelingen moet stellen; soms blijkt het dossier pas te worden samengesteld nadat er beroep is aangetekend;
- De toepassing van artikel 5 § 3 W.Beroepsorg. is vaak problematisch. Deze bepaling laat het Beroepsorgaan toe op verzoek van een inlichtingen- of politiedienst te beslissen om bepaalde stukken uit het dossier te halen dat ter inzage van de eiser of zijn advocaat wordt gegeven. Dit is het geval indien de verspreiding ervan een gevaar kan inhouden voor de bescherming van de bronnen, van de persoonlijke levenssfeer van derden of de vervulling van de wettelijke opdrachten van de inlichtingendiensten of van 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

[198] Omwille van de zeer korte termijnen is het beroep in deze gevallen dan ook vaak laattijdig en dus onontvankelijk.

de vaste rechtspraak van het Beroepsorgaan volgens dewelke de W.Beroepsorgaan een *lex specialis* is t.o.v. de Classificatiewet. Ten slotte zijn er ook gevallen waarin de voorzitter van het Beroepsorgaan ambtshalve elementen uit het dossier moet verwijderen omdat de betrokken dienst manifest nagelaten heeft zich te beroepen op artikel 5 § 3 W.Beroepsorg. en dit ter bescherming van de persoonlijke levenssfeer van derden.

- De beslissingen van de veiligheidsoverheden zijn onvoldoende gemotiveerd en er wordt – anders dan vereist door de wet – geen volledig gemotiveerde beslissing opgesteld indien artikel 22, vijfde lid W.CV&VM toelaat bepaalde elementen weg te laten in de aan de betrokkene ter kennis gegeven beslissing. De veiligheidsoverheid moet middels de motivering duidelijk maken welke concrete feiten een tegenindicatie uitmaken, gegeven 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 ook niet getuigden van zorgvuldigheid en respect voor de beginselen van het administratief recht op formeel vlak (beslissingen zonder data en identiteit van de functionaris die de beslissing neemt; betrokkene wordt nooit gehoord; het gebruik van de taal in bestuurszaken).
- De veiligheidsoverheden lijken bepaalde beslissingen die voortkomen uit een vaste rechtspraak van het Beroepsorgaan moeilijk te aanvaarden (bijvoorbeeld 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) advoca(a)t(en). Gelet op de complexiteit van sommige zaken, wordt hier veel tijd aan besteed. Ten slotte moeten – anders dan vroeger – veel zaken op een tweede of derde zitting worden hernomen, ofwel omdat een verzoeker uitstel vraagt, ofwel omdat in het dossier gewacht wordt op bijkomende informatie of nog, omwille van een wijziging van de zetel van het Beroepsorgaan.

Ook het beslissingsproces zelf vergt meer tijd dan een aantal jaren geleden. Hiervoor zijn twee belangrijke redenen aan te halen. Enerzijds worden er meer procedurele kwesties opgeworpen (bijv. debat over ontvankelijkheid, taalproblematiek, rechten van verdediging, motiveringsplicht …). Anderzijds wordt het Beroepsorgaan vaker geconfronteerd met extreem gevoelige dossiers die verband houden met spionage of de problematiek van de radicalisering en terreurdreiging. Dergelijke dossiers vereisen uiteraard een uiterst zorgvuldige behandeling en een aangepaste motivering. Daarenboven nopen ze soms tot specifieke veiligheidsmaatregelen.

X.2. EVOLUTIE IN HET WETGEVEND KADER

Diverse elementen doen vermoeden dat de werklast van het Beroepsorgaan in de toekomst nog (gevoelig) zal toenemen. Na de aanslagen van Parijs en Brussel had de Regering aangekondigd om het aantal veiligheidsscreenings op te voeren, in het bijzonder met het oog op de verhoging van de veiligheid van kritieke infrastructuren.

Dit voornemen concretiseerde zich eind 2017 door de neerlegging van een wetsontwerp[199] met het oog op de wijziging van de W.C&VM. Het Vast Comité I bracht hierover een advies uit.[200] Het ontwerp werd uiteindelijk begin 2018 goedgekeurd[201] en bracht tevens een kleine wijziging aan de W.Beroepsorg. met zich mee. Ter uitvoering van de wet werden vier Koninklijke besluiten getroffen. Een aantal van de wijzigingen had een invloed op de samenstelling van het Beroepsorgaan. Ook de nieuwe kaderwet met betrekking tot de bescherming van de persoonlijke levenssfeer bevatte regels die van toepassing zijn op (in het bijzonder) het Beroepsorgaan. Deze aanpassingen van het wetgevend kader worden hieronder toegelicht.

X.2.1. WIJZIGINGEN IN DE REGELGEVING OP DE CLASSIFICATIE EN DE VEILIGHEIDS-MACHTIGINGEN, -ATTESTEN EN -ADVIEZEN

X.2.1.1. De bevoegdheid en de rol van de veiligheidsofficier

De wijziging van de W.C&VM breidt de taken van de veiligheidsofficier in het kader van de veiligheidsverificaties (attesten en adviezen) uit en verankert deze functie ook in de schoot van het Openbaar Ministerie.

De veiligheidsofficier krijgt de bevoegdheid toegewezen om '*te zorgen voor de inachtneming van de veiligheidsregels in het kader van een veiligheidsadvies of veiligheidsattest*' op het niveau van de betrokken privaat- en publiekrechtelijke rechtspersonen.

---

199 *Parl. St.* Kamer 2017-2018, nr. 54K2767/001.

200 Dit advies is beschikbaar op de website van het Vast Comité I (www.comiteri.be). Het Comité benadrukte dat het ontwerp geen antwoord bood op de vele problemen die de toepassing van de toen geldende regeling met zich meebrachten (complextiteit, te korte beroepstermijnen …) en dit zowel op het vlak van de betrokken administraties en burgers als van het Beroepsorgaan. Eerder formuleerde het Comité een aantal voorstellen om tegemoet te komen aan voornoemde problemen. Het ontwerp van wet ging daar niet alleen niet op in, het creëerde onvermijdelijk bijkomende problemen voor alle actoren. Het Comité achtte het dan ook aangewezen dat beide wetten van 11 december 1998 (W.C&VM en W.Beroepsorg.) op een coherente wijze zouden worden hervormd.

201 Wet van 23 februari 2018 houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS* 1 juni 2018).

X.2.1.2. De hervorming van de procedure inzake veiligheidsadviezen[202]

De procedure inzake veiligheidsadviezen werd hervormd en dit zowel op niveau van de reglementaire beslissing van de administratieve overheid als op het niveau van de individuele beslissing. Deze nieuwe regelgeving trad in voege op 1 juni 2018.

Wat de reglementaire beslissing betreft, bepaalt de nieuwe procedure dat het de Koning toekomt te bepalen welke 'activiteitensectoren' onderworpen zijn aan de toepassing van de veiligheidsadviezen alsook de bevoegde (sectoriële) administratieve overheden aan te duiden.[203] Zowel privaatrechtelijke als publiekrechtelijke rechtspersonen die deel uitmaken van een betrokken activiteitensector, voeren vervolgens op vraag van de bevoegde administratieve overheid of op eigen initiatief, een 'risicoanalyse' uit die ze toezenden aan deze laatste. De administratieve overheid vraagt vervolgens een specifieke 'dreigingsanalyse' aan bij 'de bevoegde diensten'. Van zodra ze in het bezit is van deze analyse, stelt de bevoegde administratieve overheid op haar beurt een 'impactanalyse' op. Deze beoogt het in kaart brengen van de mogelijke schade aan fundamentele staatsbelangen. Op basis van bovenvernoemde analyses, zendt de administratieve overheid een aanvraagdossier inzake een veiligheidsverificatie aan de Nationale Veiligheidsoverheid (NVO). De NVO beslist uiteindelijk of er al dan niet veiligheidsverificaties mogen worden uitgevoerd.

Wat de regeling voor de individuele beslissingen betreft, bepaalt de nieuwe regeling dat de rechtspersonen de betrokkene op de hoogte moeten brengen van de verplichting om een veiligheidsverificatie te ondergaan. De veiligheidsofficier van de rechtspersoon vraagt voorafgaand aan de veiligheidsverificatie, de instemming van de betrokkene. De veiligheidsofficier van de bevoegde administratieve overheid waakt onder meer over de conformiteit van de verificatieverzoeken. Hij bezorgt deze op zijn beurt aan de NVO. De NVO doet binnen de opgelegde termijn (maximum één maand) uitspraak over de individuele aanvraag. Indien de NVO nalaat binnen deze termijn een veiligheidsadvies te formuleren, kan ze worden aangemaand om alsnog uitspraak te doen binnen een termijn die minstens even langs is dan de initieel voorgeschreven termijn. Gebeurt dit niet, wordt het advies geacht positief te zijn. De nieuwe regeling bepaalt dat het advies wordt toegekend voor een duur van maximaal vijf jaar[204], en dit onder voorbehoud van een

---

202 Zie artt. 22*quinquies* en 22*quinquies*/1 W.C&VM en het KB van 8 mei 2018 tot wijziging van het Koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS* 1 juni 2018).

203 Het betreft in deze een belangrijk verschil met de initiële regeling inzake veiligheidsadviezen waarbij 'een' (eender welke) administratieve overheid de procedure kon initiëren. Deze bepaling werd ten uitvoer gelegd door het KB van 8 mei 2018 tot vaststelling van de activiteitensectoren en de bevoegde administratieve overheden bedoeld in art. 22*quinquies* § 7, van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS* 1 juni 2018).

204 Ook dit vormt een verschil met de voorgaande regeling die niet voorzag in een 'maximale' geldigheidstermijn. Verder moest bij de voormalige regeling de uitvoering van de veiligheids-

her-evaluatie door de NVO (op basis van nieuwe elementen). De administratieve overheid informeert de veiligheidsofficier van de werkgever over het veiligheidsadvies. Indien er een negatief veiligheidsadvies wordt verleend, wordt de betrokken persoon daarvan per aangetekende zending op de hoogte gebracht, met uitzondering van de motieven waarvan de verspreiding mogelijks schade zou kunnen toebrengen aan één van de fundamentele belangen zoals opgesomd in de wet, aan de bescherming van de bronnen, aan het geheim van een opsporings- of gerechtelijk onderzoek of aan de bescherming van de persoonlijke levenssfeer van derden.[205]

X.2.1.3. De inhoud van de veiligheidsverificatie

De laatste belangrijke pijler van de wetswijzing bestaat in de wijziging van de inhoud van de veiligheidsverificatie (art. 22*sexies* W.C&VM). Daarbij worden drie doelstellingen voor ogen gehouden.

Vooreerst is het de bedoeling om ook veiligheidsverificaties mogelijk te maken ten aanzien van minderjarigen. Verder wordt beoogd om, in het kader van veiligheidsverificaties van meerderjarigen, de tijdens hun minderjarigheid gepleegde feiten mee in rekening te nemen.

Daarnaast laat de nieuwe wet de politie- en inlichtingendiensten toe gegevens op te vragen bij hun buitenlandse homologen wanneer de persoon voor wie de veiligheidsverificatie vereist is in het buitenland woont (of heeft gewoond), er op doorreis is geweest of er verbleven heeft.

Ten slotte breidt de nieuwe wet het aantal te bevragen gegevensbanken uit. Artikel 22*sexies* W.C&VM voorzag reeds in de consultatie en evaluatie van gerechtelijke gegevens[206], van informatie afkomstig van inlichtingendiensten, het centraal strafregister, het strafregister en de bevolkings- en vreemdelingregisters bijgehouden op de gemeenten, het Rijksregister, het wachtregister van de vreemdelingen alsook de politiegegevens ter beschikking van politiefunctionarissen tijdens de uitvoering van identiteitscontroles. De gewijzigde tekst voegt hieraan volgende gegevens toe: de gegevens en informatie uit de internationale politionele databanken voortvloeiend uit verdragen die België binden, de gegevens van administratieve politie, de gegevens uit gemeenschappelijke gegevensbanken en *'andere gegevens en informatie'*. De wet bepaalt dat het toereikend, ter zake en niet overmatig karakter van deze gegevens evenals de lijst ervan moeten worden vastgelegd bij Koninklijk besluit. Dit besluit verscheen eveneens in de loop van 2018.[207]

---

verificatie plaatsvinden 'voorafgaand' aan de toelating om een beroep, functie, opdracht of mandaat uit te oefenen. De wijziging introduceert de mogelijkheid om personen die reeds in functie zijn, aan een veiligheidsverificatie te onderwerpen.

205 Cf. art. 22, lid 5 W.C&VM (ongewijzigd).

206 Overgezonden mits toelating van de bevoegde gerechtelijke overheden.

207 KB van 8 mei 2018 tot bepaling van de lijst van de gegevens en informatie die geraadpleegd kunnen worden in het kader van de uitvoering van een veiligheidsverificatie (*BS* 1 juni 2018).

X.2.1.4. De retributies

Midden 2018 werd tevens een Koninklijk besluit goedgekeurd waarbij de retributies verschuldigd voor de machtigingen, attesten en adviezen werden vastgesteld.[208] De retributie voor een machtiging voor natuurlijke personen bedraagt 150, 175 of 200 euro, en dit naargelang het gevraagde niveau (respectievelijk vertrouwelijk, geheim of zeer geheim). De retributie voor de rechtspersonen bedraagt, afhankelijk van het niveau, 900, 1200 dan wel 1500 euro. De forfaitaire kost voor een veiligheidsattest of -advies is vastgesteld op 50 euro. Deze bedragen worden vervolgens aan de hand van een in het Koninklijk besluit bepaalde verdeelsleutel verdeeld onder de verschillende betrokken overheden.

X.2.2. WIJZIGINGEN AAN DE WERKING VAN HET BEROEPSORGAAN[209]

In 2018 wijzigden drie wetten de samenstelling van het Beroepsorgaan alsook de beroepsprocedure.

Vooreerst werd de W.Beroepsorg. aangepast met het oog op de afstemming op de wijzigingen zoals ingevoerd door de W.C&VM. Het betrof de waarborg voor het behoud van het recht op beroep voor diegene die een negatief veiligheidsadvies ontving. Daarvoor moet deze laatste beroep aantekenen binnen de acht dagen na ontvangst van het advies. Verder werd artikel 12 W. Beroepsorg. aangepast zodat een beroep tegen een (positieve of negatieve) reglementaire beslissing[210] mogelijk wordt

---

208 KB van 8 mei 2018 tot vaststelling van de bedragen van de retributies die verschuldigd zijn voor de veiligheidsmachtigingen, voor de veiligheidsattesten en de veiligheidsadviezen afgegeven door de Nationale Veiligheidsoverheid en voor de veiligheidsattesten afgegeven door het Federaal Agentschap voor de Nucleaire Controle alsook van de verdeelsleutels bedoeld in art. 22*septies*, zesde en achtste lid, van de wet 1998 betreffende classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS* 1 juni 2018).

209 Wet van 13 september 2018 houdende wijziging aan de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS* 5 oktober 2018).

210 De voorbereidende werken preciseren dat '*Dat beroep kan dus niet alleen worden ingediend door een natuurlijke persoon die een dergelijke functie uitoefent of die toegang heeft tot de betrokken plaats, maar ook door een privaatrechtelijke rechtspersoon die tot de sector behoort. […] Dat beroep heeft derhalve wel degelijk betrekking op de goedkeuring of de weigering van het dossier van de administratieve overheid op grond van artikel 12 van de wet betreffende de veiligheidsmachtigingen. In het kader van dat beroep wordt een onderzoek ingesteld naar de relevantie van de veiligheidsaspecten van het dossier. De facto worden de elementen van het dossier van de administratieve overheid inzake de veiligheidsaspecten eveneens onder de loep genomen bij het onderzoek van het beroep. De ervaring en de deskundigheid van de leden van het beroepsorgaan op stuk van veiligheid en bescherming van de vrijheden en de fundamentele rechten rechtvaardigen dat dat orgaan optreedt als beroepsorgaan. Het spreekt vanzelf dat de sector of elkeen die een belang aantoont, eveneens beroep kan instellen tegen het dossier dat de administratieve overheid heeft ingediend (impactanalyse). Dat specifieke beroep kan worden ingesteld bij de Raad van State, aangezien het niet onder bevoegdheid van het beroepsorgaan ressorteert*' (*Parl. St.*, Kamer 2017-18, 54K3107/005, 4).

voor eenieder die een legitiem belang heeft. Maar ook de betrokken administratieve overheid krijgt de mogelijkheid om beroep in te dienen bij het Beroepsorgaan in de hypothese waarbij de NVO zijn verzoek tot verificatie weigerde. Deze beroepen moeten worden ingediend binnen de acht dagen na kennisname van de beslissing van de NVO.

Daarnaast werd de samenstelling van het Beroepsorgaan gewijzigd door de Wet van 13 september 2018, dit om rekening te kunnen houden met de afschaffing van de Commissie voor de bescherming van de persoonlijke levenssfeer. De W.Beroepsorg. bepaalt dat de Voorzitter van de Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA) zetelt in het Beroepsorgaan. Om de continuïteit te garanderen, voorzag de Wet van 13 september 2018 in een overgangsmaatregel opdat de Voorzitter van de GBA zijn functie binnen het Beroepsorgaan zou kunnen blijven uitvoeren tot de benoeming van de Voorzitter van de Geschillenkamer van de GBA. Deze benoeming kwam er op het einde van het eerste trimester van 2019.[211]

En ten slotte, rekening houdende met het gegeven dat de Wet van 3 december 2017[212] niet bepaalt dat de Voorzitter van de Geschillenkamer van de GBA (alsook niemand anders binnen deze geschillenkamer) een magistraat dient te zijn, werd de verplichting tot het hebben van deze hoedanigheid om deel te kunnen uitmaken van het Beroepsorgaan, geschrapt.[213]

X.2.3. DE NIEUWE KADERWET INZAKE DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

Titel 3 van de Wet van 30 juli 2018[214] (GBW) bevat een ondertitel 3 die specifiek gewijd is aan de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens in het kader van de W.C&VM (artikels 106 tot 137 GBW). De regels opgenomen in deze ondertitel zijn mede van toepassing op elke verwerking van dit type van gegevens door het Beroepsorgaan (artikel 107, § 2 GBW). Er dient wel te worden opgemerkt dat het Beroepsorgaan, in zijn hoeda-

---

211 Hielke Hijmans werd benoemd tot Voorzitter van de Geschillenkamer van de Gegevensbeschermingsautoriteit (*Hand.* Kamer 2018-19, 28 mars 2019, CRIV54PLEN278) en legde op 24 april 2019 de eed af.

212 Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (*BS* 10 januari 2018).

213 De voorbereidende werken luiden als volgt: '*Dat betekent derhalve dat de voorwaarden bepaald bij de wetten waarbij de betrokken organen zijn opgericht, in acht worden genomen. Het beroepsorgaan zal nog steeds uit minstens twee magistraten bestaan. De aanwezigheid van twee magistraten (respectievelijk uit het Comité P en het Comité I) in dat orgaan wordt gewaarborgd door de wet waarbij de betrokken organen zijn opgericht*' (*Parl. St.*, Kamer 2017-18, 54K3107/003, 9).

214 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (*BS* 5 september 2018).

nigheid van rechterlijke overheid, niet onderworpen is aan een controle door een toezichthoudende autoriteit voor de bescherming van persoonsgegevens (artikel 128, § 2 GBW).

X.3. GEDETAILLEERDE CIJFERS

In dit onderdeel worden de aard van de bestreden beslissingen, de hoedanigheid van de bevoegde overheden en van de verzoekers[215] en de aard van de beslissingen van het Beroepsorgaan binnen de verschillende beroepsprocedures cijfermatig weergegeven. Om enige vergelijking mogelijk te maken, werden de cijfers van de afgelopen vijf jaar eveneens opgenomen.

Er kunnen drie tendensen worden vastgesteld in 2018. Vooreerst valt er, na twee jaren van aanzienlijke toename, een daling te noteren van het aantal dossiers; het aantal dossiers verminderde van 192 in 2017 naar 158 in 2018. Daarnaast daalde ook het aantal dossiers met betrekking tot militairen, gaande van 20 in 2017 tot 8 in 2018. Een laatste tendens betreft enerzijds het verhoging van het aantal beroepen tegen weigeringen van veiligheidsattesten in de nucleaire sector (7 in 2016 en 2017 en 11 in 2018) en anderzijds een opgemerkte daling van het aantal beroepen tegen negatieve veiligheidsadviezen (101 in 2016, 122 in 2017 en 92 in 2018).[216]

Er vonden in 2018 14 zittingen van het Beroepsorgaan plaats.

Tabel 1. Betrokken veiligheidsoverheid

	2014	2015	2016	2017	2018
Nationale Veiligheidsoverheid	99	68	92	129	113
Veiligheid van de Staat	0	1	0	0	0
Algemene Dienst Inlichting en Veiligheid	60	47	68	53	32

215 Er viel te noteren dat 10 'verzoeken' niet conform waren aan de minimumvereisten van de wet (met als typevoorbeeld het ontbreken van een handtekening) en dus niet konden worden beschouwd als ontvankelijke beroepen.

216 De daling van het aantal beroepen gericht tegen negatieve veiligheidsadviezen valt te verklaren door de jurisprudentie van het Beroepsorgaan uitgesproken in de loop van 2017 volgens dewelke, op basis van de (op dat ogenblik) voorgelegde dossiers inzake veiligheidsverificaties, de veiligheidsadviezen zoals geformuleerd door de NVO voor extern personeel van Europese instellingen, niet konden terugvallen op een afdoende juridische basis. De analyse van de aanpassing van het wetgevend kader (hierboven samengevat) laat toe te veronderstellen dat de materie van de veiligheidsadviezen voor het personeel van Europese instellingen weldra (opnieuw) zal worden onderworpen aan het Beroepsorgaan in de zin dat het KB van 8 mei 2018 (zie *supra*) de leidinggevende ambtenaar van de FOD Buitenlandse Zaken of zijn afgevaardigde aanstelt als administratieve autoriteit bevoegd voor de internationale instanties.

	2014	2015	2016	2017	2018
Federaal Agentschap voor Nucleaire Contrôle	8	10	8	7	10
Federale Politie	3	3	1	3	3
Lokale Politie	1	1	0	0	0
TOTAAL	**171**	**130**	**169**	**192**	**158**

Tabel 2. Aard van de bestreden beslissing

	2014	2015	2016	2017	2018
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)					
Vertrouwelijkl	5	9	5	1	2
Geheim	43	35	38	33	31
Zeer geheim	4	4	7	6	3
Weigering	25	36	28	30	26
Intrekking	9	7	9	7	4
Weigering en intrekking	0	0	0	0	0
Machtiging voor beperkte duur	2	3	4	1	1
Machtiging voor lager niveau	1	0	1	0	0
Geen beslissing binnen termijn	15	2	7	2	5
Geen beslissing binnen verlengde termijn	0	0	1	0	0
Subtotaal veiligheidsmachtigingen	**52**	**48**	**50**	**40**	**36**
Veiligheidsattesten toegang geclassificeerde zones (art. 22*bis*, al.1 W.C&VM)					
Weigering	4	6	1	3	3
Intrekkig	0	0	0	0	0
Geen beslissing binnen termijn	0	0	0	0	0
Veiligheidsattesten plaats of gebeurtenis (art. 22*bis*, al. 2 W.C&VM)					
Weigering	16	12	9	20	15
Intrekking	0	1	0	0	0
Geen beslissing binnen termijn	0	0	0	0	0

	2014	2015	2016	2017	2018
Veiligheidsattesten voor de nucleaire sector (art. 8*bis*, § 2 W.C&VM)					
Weigering	–	–	7	7	11
Intrekking	–	–	1	0	0
Geen beslissing binnen termijn	–	–	0	0	1
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)					
Negatief advies	99	63	101	122	92
Geen advies	0	0	0	0	0
Herroeping van een positief advies	0	0	0	0	0
Normatieve rechtshandelingen (art. 12 W. Beroepsorg.)					
Beslissing van publieke overheid om attesten te eisen	0	0	0	0	0
Weigering NVO om verificaties voor attesten te verrichten	0	0	0	0	0
Beslissing van een administratieve overheid om adviezen te eisen	0	0	0	0	0
Weigering NVO om verificaties voor adviezen te verrichten	0	0	0	0	0
Subtotaal attesten en adviezen	**119**	**82**	**119**	**152**	**122**
TOTAAL BESTREDEN BESLISSINGEN	171	130	169	192	158

Tabel 3. Hoedanigheid van de verzoeker

	2014	2015	2016	2017	2018
Ambtenaar	0	4	2	4	5
Militair	17	29	23	20	8
Particulier	145	93	139	164	140
Rechtspersoon	6	4	5	4	5

Tabel 4. Taal van de verzoeker

	2014	2015	2016	2017	2018
Franstalig	92	75	99	115	83
Nederlandstalig	76	54	70	77	75
Duitstalig	0	0	0	0	0
Anderstalig	0	1	0	0	0

Tabel 5. Aard van de door het Beroepsorgaan genomen voorbereidende beslissingen[217]

	2014	2015	2016	2017	2018
Volledig dossier opvragen (1)	168	130	167	191	154
Aanvullende informatie opvragen (2)	16	7	23	36	12
Horen lid overheid (3)	11	7	10	0	1
Beslissing voorzitter (4)	0	0	0	0	0
Informatie uit dossier halen door Beroepsorgaan (5)	78	50	54	80[218]	72
Informatie uit dossier halen door inlichtingendienst (6)	0	0	0	0	0

(1) Het Beroepsorgaan beschikt over de mogelijkheid het gehele onderzoeksdossier bij de veiligheidsoverheden op te vragen. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan.
(2) Het Beroepsorgaan heeft de mogelijkheid om tijdens de procedure aanvullende informatie die het nuttig acht, op te vragen.
(3) Het Beroepsorgaan kan beslissen om de leden van de inlichtingen- en politiediensten of van de veiligheidsoverheden die aan het veiligheidsonderzoek of de -verificatie hebben meegewerkt, te horen.
(4) De voorzitter van het Beroepsorgaan kan beslissen dat het lid van de inlichtingendienst bepaalde gegevens geheim houdt tijdens zijn verhoor.

217 Het 'aantal genomen voorbereidende beslissingen' (tabel 5), de 'wijze waarop de verzoeker zijn rechten van verdediging gebruikt' (tabel 6) of nog, de 'aard van de beslissingen van het beroepsorgaan' (tabel 7) is niet noodzakelijkerwijs gelijklopend met het aantal ingediende verzoeken uit de tabellen 1 tot en met 4. Immers, sommige dossiers werden bijvoorbeeld al opgestart in 2017, terwijl de beslissing pas viel in 2018.

218 Zie hoger wat betreft art. 5 § 3 W.Beroepsorg. Het dient opgemerkt dat in vele gevallen het verzoek tot niet-inzage slechts gedeeltelijk werd ingewilligd (soms omwille van een gebrekkige motivering door de betrokken dienst).

(5) Indien de betrokken inlichtingen- of politiedienst hierom verzoekt, kan de voorzitter van het Beroepsorgaan beslissen dat bepaalde informatie uit het dossier dat aan de verzoeker ter inzage zal worden voorgelegd, wordt gehaald.[219]
(6) Indien het informatie betreft die afkomstig is van een buitenlandse inlichtingendienst, beslist de Belgische inlichtingendienst zelf of de informatie ter inzage is. Dit is een aspect van de toepassing van de zogenaamde 'derdenregel'.

Tabel 6. Wijze waarop de verzoeker zijn rechten van verdediging gebruikt

	2014	2015	2016	2017	2018
Dossierinzage door klager / advocaat	84	84	87	105	69
Horen van de klager / advocaat[220]	115	107	127	158	111

Tabel 7. Aard van de beslissingen van het Beroepsorgaan

	2014	2015	2016	2017	2018
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)					
Beroep onontvankelijk	0	4	0	3	0
Beroep zonder voorwerp	3	3	7	0	4
Beroep ongegrond	12	19	18	13	12
Beroep gegrond (volledige of gedeeltelijke toekenning)	14	24	24	24	12
Bijkomende onderzoeksdaden door overheid	0	0	2	0	1
Bijkomende termijn voor overheid	12	1	2	1	1
Zonder gevolg	0	1	0	0	3
Veiligheidsattesten toegang geclassificeerde zones (art. 22*bis*, al. 1 W.C&VM)					
Beroep onontvankelijk	0	0	0	1	0
Beroep zonder voorwerp	0	0	0	1	0
Beroep ongegrond	2	4	1	0	1
Beroep gegrond (toekenning)	0	2	1	1	0

219 Zie *supra* in verband met art. 5 § 3 W.Beroepsorg.
220 In bepaalde dossiers wordt de klager (al dan niet bijgestaan door zijn advocaat) meermaals gehoord.

	2014	2015	2016	2017	2018
Veiligheidsattesten plaats of gebeurtenis (art. 22*bis*, al. 2 W.C&VM)					
Beroep onontvankelijk	0	0	0	1	2
Beroep zonder voorwerp	0	0	0	1	0
Beroep ongegrond	6	8	2	12	2
Beroep gegrond (toekenning)	8	10	4	7	3
Verleent akte van afstand van beroep	0	2	0	1	2
Veiligheidsattesten voor de nucleaire sector (art. 8*bis* § 2 W.C&VM)					
Beroep onontvankelijk	–	–	1	1	0
Beroep zonder voorwerp	–	–	1	0	1
Beroep ongegrond	–	–	0	1	1
Beroep gegrond (toekenning)	–	–	7	5	6
Verleent akte van afstand van het beroep	–	–	–	–	2
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)					
Beroepsorgaan onbevoegd	4	0	0	20[221]	12[222]
Beroep onontvankelijk	4	6	15	10	3
Beroep zonder voorwerp	4	0	0	1	3
Bevestiging negatief advies	53	28	42	49	46
Omvorming in positief advies	41	23	46	41	27
Verleent akte van afstand van beroep	0	0	0	1	0
Beroep tegen normatieve rechtshandelingen (art. 12 W.Beroepsorg.)	0	0	0	0	0
TOTAAL	**163**	**137**	**173**	**195**	**144**

221 Het betrof *in casu* de beroepen ingediend tegen (negatieve) veiligheidsadviezen van de Nationale Veiligheidsoverheid met betrekking tot personeel van onderaannemers actief bij in België gevestigde Europese instellingen. Het Beroepsorgaan had beslist dat het ontbrak aan een wettelijke basis van de door de Nationale Veiligheidsoverheid geformuleerde adviezen omdat de overheid die het advies aanvroeg niet dezelfde overheid was als de overheid die het advies wou gebruiken om een beslissing te nemen. Bijgevolg verklaarde het Beroepsorgaan zich zonder rechtsmacht om te oordelen over de al dan niet gegrondheid van het veiligheidsadvies afgeleverd door de Nationale Veiligheidsoverheid.

222 Naar aanleiding van de beslissing van het Beroepsorgaan waarvan sprake in de vorige voetnoot, wijzigde de overheid zijn werkwijze bij het afleveren van adviezen voor personen werkzaam voor de Europese instellingen. Omdat daarbij geen antwoord werd geboden op de kritiek van het Beroepsorgaan, diende het zich in tien gelijkaardige dossiers opnieuw onderbevoegd te verklaren.

HOOFDSTUK XI
DE INTERNE WERKING VAN HET VAST COMITÉ I

XI.1. SAMENSTELLING VAN HET VAST COMITÉ I

In 2018 wijzigde de samenstelling van het Comité grondig: voorzitter Guy Rapaille[223] (F), advocaat-generaal bij het hof van beroep te Luik, gaf de fakkel door aan Serge Lipszyc, eerste substituut arbeidsauditeur bij het arbeidsauditoraat van Luik (F), die op 25 september 2018 als nieuwe voorzitter de eed aflegde.[224] Raadsheer Gérald Vande Walle (F) bereikte op 31 december 2017 de pensioengerechtigde leeftijd en werd begin 2018 vervangen door Laurent Van Doren, voormalig hoofdcommissaris van politie.[225] Raadsheer Pieter-Alexander De Brock (N) bleef in functie.[226]

Bij de Dienst Enquêtes I werden geen wijzigingen opgetekend. De dienst bleef daarmee bestaan uit vijf commissaris-auditoren, waaronder de directeur Frank Franceus (N).

De administratieve staf van het Vast Comité I, onder leiding van griffier Wouter De Ridder (N), bleef met 18 administratieve personeelsleden ongewijzigd. Wel werd een Data Protection Officer (DPO) aangesteld voor alle gegevensverwerkingen van het Comité die buiten de 'nationale veiligheid' vallen (bijvoorbeeld verwerkingen in het kader van het personeelsbeheer en logistiek).

---

223 Overeenkomstig het advies van de Conferentie van Voorzitters van 10 oktober 2018 werd aan Guy Rapaille de titel van ere-voorzitter van het Vast Comité I verleend (CRIV54PLEN251).

224 Op 28 februari 2019 werden respectievelijk Vanessa Samain en Didier Maréchal aangeduid als eerste en tweede plaatsvervangend voorzitter

225 Er dienden in 2018 meerdere oproepen te worden gelanceerd voor de mandaten van eerste en tweede Franstalig lid van het Comité. Op 22 november 2018 werden Thibaut Vandamme en Michel Croquet aangeduid als respectievelijk eerste en tweede plaatsvervanger.

226 Op 26 september 2018 werd door de Kamer beslist (CRIV54PLEN245) een oproep tot kandidaten bekend te maken voor het mandaat van Nederlandstalig lid (*BS* 27 september 2018) en voor de mandaten van eerste en tweede Nederlandstalig plaatsvervangend lid, gelet op het feit dat het mandaat van raadsheer De Brock afliep op 7 mei 2019. Op datum van goedkeuring van onderhavig activiteitenverslag werd in deze nog geen beslissing genomen.

XI.2. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE

In de loop van 2018 vonden vier vergaderingen plaats met de Bijzondere commissie belast met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de veiligheids- en inlichtingendiensten.[227] De dertien stemgerechtigde leden van de commissie waren: Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Peter De Roover (N-VA), Laurette Onkelinx (PS), André Frédéric (PS), David Clarinval (MR), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld), Hans Bonte (sp.a), Stefaan Van Hecke (Ecolo-Groen) en Georges Dallemagne (cdH). De Commissie vergaderde onder het voorzitterschap van Kamervoorzitter Siegfried Bracke (N-VA).

Tijdens de 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). Ook het door het Comité aangeleverde totaaloverzicht van alle nog niet uitgevoerde aanbevelingen van de afgelopen tien jaar, vormde het voorwerp van bespreking.

In november 2018 werd het *Activiteitenverslag 2017* van het Vast Comité I besproken en nam de Commissie kennis van de prospectieve nota 2018-2020 van het Comité. De Commissie nam '*akte van het activiteitenverslag 2017 van het Comité I en verleent haar goedkeuring aan de aanbevelingen van het Comité*'.[228]

XI.3. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITÉ P

De artikelen 52 tot 55 W.Toezicht bepalen de gevallen waarin en de wijze waarop het Vast Comité I en het Vast Comité P gemeenschappelijke vergaderingen dienen te organiseren. Het voorzitterschap van deze gezamenlijke vergaderingen wordt

227 In juli 2018 werd door de Begeleidingscommissie tevens een gedachtewisseling georganiseerd met de minister van Defensie en de Chef ADIV in aanwezigheid van de toenmalige voorzitter van het Comité over het toezichtsonderzoek m.b.t. de werking van de Directie Counterintelligence.

228 *Parl. St.* Kamer 2018-19, nr. 54K3375/001 (Activiteitenverslag 2017 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).

afwisselend waargenomen door de voorzitters van beide Vaste Comités (art. 54 W.Toezicht). Het doel van de vergaderingen is tweeërlei: enerzijds het uitwisselen van informatie en anderzijds het opstarten en bespreken van lopende gemeenschappelijke toezichtonderzoeken.

In 2018 waren twee gemeenschappelijke toezichtonderzoeken aan de orde: het reeds eerder opgestarte onderzoek naar de ondersteunende diensten van het OCAD (cf. I.6.3) en het onderzoek opgestart in mei 2018 naar de '*informatiepositie van het OCAD voorafgaand aan de aanslag in Luik*' (cf. I.4).

Verder werden uiteenlopende punten geagendeerd: de (mogelijke) aanpassing van het administratief statuut, de redactie van een deontologisch charter, de bespreking van de 'Audit dotatiegerechtigde instellingen', de nieuwe wetgeving inzake gegevensbescherming en in datzelfde kader de aanstelling van een gemeenschappelijke Data Protection Officer (DPO) … Ook was de voorbereiding van de organisatie van een viering naar aanleiding van het 25-jarig bestaan van beide Vaste Comités aan de orde.

In 2018 vonden, naast informele contacten op de werkvloer, acht gemeenschappelijke vergaderingen plaats.

XI.4. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Artikel 57, eerste lid, W.Toezicht vermeldt dat de kredieten die noodzakelijk zijn voor de werking dienen te worden uitgetrokken op de begroting van de dotaties. 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.[229] Tot 2017 was deze dotatie onvoldoende om de reële uitgaven van het Comité te dekken, wat een structureel verlies als gevolg met zich meebracht.

Zich bewust van deze precaire situatie en van het belang van de vrijwaring van het evenwicht, heeft de Kamer besloten om de dotatie aan te passen om op die manier de uitvoering van de bijkomende wettelijke opdrachten van het Comité te kunnen waarborgen.

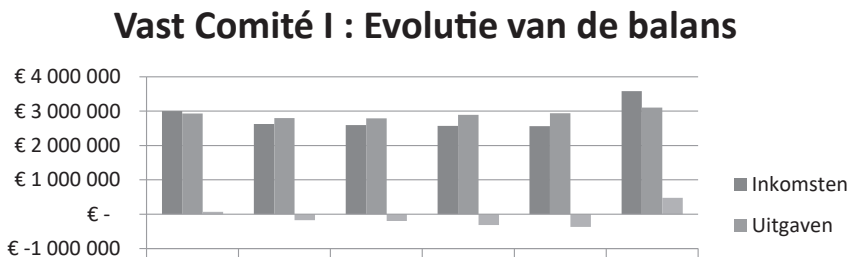
Het 'budget 2018' van het Vast Comité I werd vastgelegd op 3,759 miljoen euro, wat een vermeerdering inhield van 3,4% ten aanzien van het budget 2017. De financieringsbronnen van dit budget werden door de Kamer van Volksvertegenwoordigers[230] als volgt toegewezen: 95,26% dotatiebudget en 4,74% boni van 2016.

---

229 Wet van 7 december 2017 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2018, *BS* 28 december 2017.

230 *Parl. St.* 2017-2018 Kamer, 54K2843/001, 24-29.

De uitvoering van het budget 2018 leverde een budgettaire bonus op van 475.494 euro, te weten het vastgestelde verschil tussen de inkomsten en de samengestelde uitgaven.



	2013	2014	2015	2016	2017	2018
Inkomsten	€ 3 005	€ 2 626	€ 2 597	€ 2 570	€ 2 565	€ 3 582
Uitgaven	€ 2 935	€ 2 799	€ 2 792	€ 2 889	€ 2 937	€ 3 107
Resultaat	€ 70 38	€ -173	€ -194	€ -318	€ -372	€ 475

De zoektocht naar synergieën tussen de verschillende dotatiegerechtigde instellingen blijft ondanks de boni hoog op de agenda. De ontwikkeling van deze synergieën hebben een zeer beperkte financiële invloed ingevolge structurele complicaties, zoals daar zijn het gebrek aan mobiliteit van personeelsleden van diverse instellingen (en dit omwille van de verschillen in de statuten). Ze leiden wel tot betere samenwerkingsverbanden tussen de instellingen die bevorderlijk zijn voor de kwaliteit van het geleverde werk.

XI.5. EEN EXTERNE AUDIT BIJ ALLE DOTATIEGERECHTIGDE INSTELLINGEN

Op verzoek van de Commissie van de Comptabiliteit van de Kamer van Volksvertegenwoordigers startte het Rekenhof in december 2017 samen met Ernst and Young een onderzoek naar de dotatiegerechtigde instellingen, waaronder het Vast Comité I.

Het Rekenhof moest zich vooral richten op de budgettaire aspecten (een analyse van de inkomsten en uitgaven) en op de afbakening van de taken van de diverse instellingen. Ernst and Young kreeg als hoofdopdracht de processen, de systemen en de organisatie die in elk van deze instellingen aanwezig zijn, verder te analyseren.

Om deze werkzaamheden te kunnen uitvoeren, dienden de instellingen tal van documenten en informatie ter beschikking te stellen en een omstandige reeks van punctuele vragen te beantwoorden (december 2017). Aan de hand van de bekomen informatie, werden vervolgens door de onderzoeksteams van het Rekenhof en van Ernst and Young interviews afgenomen van een aantal sleutel-

figuren binnen het Comité (januari-februari 2018). Eind februari werd tijdens een *exit meeting* het ontwerprapport voor commentaar voorgelegd.

Deze audit bracht heel wat werk mee voor het Vast Comité I en dit bovenop de toegenomen werklast (*supra*).

Het auditverslag[231] werd eind maart 2018 opgeleverd en werd op 12 juni 2018 besproken door de Commissie van de Comptabiliteit.

XI.6. VORMING

Omwille van het belang voor de organisatie, moedigt het Vast Comité I zijn leden en medewerkers aan tot het volgen van algemene (informatica, management …) of sectoreigen opleidingen en conferenties.[232] Wat betreft deze laatste categorie werden onderstaande studiedagen door een of meerdere (personeels)leden van het Vast Comité I bijgewoond.

DATUM	TITEL	ORGANISATIE	PLAATS
15 februari 2018	Naar een herbekijking van de Belgische veiligheidsarchitectuur: de vaststellingen en aanbevelingen van de parlementaire onderzoekscommissie 'Terroristische aanslagen'	KU Leuven	Leuven
20-22 februari 2018	Roundtable discussion 'on the outline of the guidelines for intelligence oversight'	Democratic Centre for Armed Forces (DCAF)	Skopje
15 maart 2018	Cybercriminalité & cyberterrorisme	UC Liège	Luik
6 april 2018	Le renseignement et son contrôle	Raad van State, Frankrijk	Parijs
4 mei 2018	High Level Round Table on Public Security	European Corporate Security Association (ECSA) en SAS Institute	Leuven
30 mei 2018	Info session – Implementation of the EU directive 2016/1148	European Corporate Security Association (ECSA) en Center for Cybersecuruty Belgium (CCB)	Brussel

231 *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.

232 Er vonden ook interne opleidingen plaats, waaronder een aantal (door de medewerkers verplicht bij te wonen) veiligheidsbriefings alsook inlichtingengerelateerde opleidingen.

DATUM	TITEL	ORGANISATIE	PLAATS
29 juni 2018	International collaboration regarding intelligence services and intelligence studies	Belgian Intelligence Studies Centre (BISC)	Brussel
24 september 2018	'SIGINT intelligence, surveillance, ethics and control' en 'Round table intelligence, surveillance and technology'	Université de Bordeaux	Parijs
16 oktober 2018	Crypto War	KU Leuven	Brussel
12-19 oktober 2018	Sweepstakes	SHAPE	Lissabon
22 november 2018	10 ans de contrôle parlementaire du renseignement	Parlement, Frankrijk	Parijs
26 november 2018	Le futur de la Défense belge	Egmont Royal Institute for International Relations	Brussel
29-30 november 2018	International Intelligence Oversight Forum (IIOF 2018)	UN-High Commissioner for Human Rights	Malta
29 november 2018	20 jaar Wet houdende regeling van de inlichtingen- en veiligheidsdiensten	ADIV/VSSE	Brussel
6-7 december 2018	European Conference for Intelligence Oversight Bodies	Commission nationale de contrôle des techniques de renseignement (CNCTR) en het Vast Comité I	Parijs

HOOFDSTUK XII
AANBEVELINGEN

Op basis van de in 2018 afgesloten toezichtonderzoeken, controles en inspecties formuleert het Vast Comité I – soms samen met het Vast Comité P of het Controleorgaan voor positionele informatie – onderstaande aanbevelingen. Zij hebben in het bijzonder betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen (XII.1), op de coördinatie en de efficiëntie van de inlichtingendiensten, het OCAD en de ondersteunende diensten (XII.2) en – ten slotte – op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I (XII.3).

XII.1. AANBEVELING IN VERBAND MET DE BESCHERMING VAN DE RECHTEN DIE DE GRONDWET EN DE WET AAN PERSONEN WAARBORGEN

XII.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.*' Er werd evenwel nog geen dergelijk Koninklijk besluit getroffen. Het Vast Comité I dringt er op aan om dit zo spoedig mogelijk te doen.

XII.2. AANBEVELINGEN IN VERBAND MET DE COÖRDINATIE EN DE EFFICIËNTIE VAN DE INLICHTINGENDIENSTEN, HET OCAD EN DE ONDERSTEUNENDE DIENSTEN

XII.2.1. DIVERSE AANBEVELINGEN VOOR DE ADIV NAAR AANLEIDING VAN HET TOEZICHTONDERZOEK NAAR DE WERKING VAN DE DIRECTIE COUNTERINTELLIGENCE

Het onderzoek naar de werking van de Directie Counterintelligence (CI) van de ADIV gaf een inkijk in de ernst, de complexiteit en de pluriformiteit van de tekortkomingen binnen deze dienst.[233] Het Comité was 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. Daartoe werden een aantal aanbevelingen geformuleerd. 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).

XII.2.1.1. Aanbevelingen met een zeer hoge prioriteit

Inzake missie, visie en planningscyclus

- Het formeel vastleggen van de missie en visie voor CI, met inbegrip van hun rol en taak inzake counterterrorisme, onderschreven door alle betrokkenen en in lijn met de algemene beleidslijnen, visie en ambitie van de ADIV;
- Een analyse en een plan maken over de aard van de inlichtingen (operationele *versus* strategische) dewelke CI dient te produceren om tegemoet te komen aan de behoeften van de gebruikers, met aandacht voor proactieve en strategische analyse;
- Zowel intern (binnen de ADIV, binnen de Directie CI en ook ten overstaan van de Directie I(ntelligene)) als extern (in relatie tot de VSSE, het Parket, het OCAD …) dient de ADIV en de Directie CI een ondubbelzinnig gedragen standpunt uit te werken (vastgelegd in SLA's en protocollen) omtrent wat van de dienst kan en mag worden verwacht en dit rekening houdende met de beschikbare middelen. Eens de visie, de ambitie en de strategie is uitgewerkt, moet daaraan daadwerkelijk de hand worden gehouden zodat de dienst zich als een waardevolle partner in het Belgische antiterrorisme-beleid kan manifesteren;

[233] Zie 'Hoofdstuk I.1. De werking van de Directie Counterintelligence (CI) van de ADIV'.

- Het opmaken en formeel goedkeuren van een gesynchroniseerde planning op alle niveaus van CI, tot en met het opstellen van *intelligence requirements* (IR) en *information collection plans* (ICP);
- Het vastleggen in een interne richtlijn van de gebruikte sturing- en planningsmethodologie, -instrumenten en -processen, en van de wijze van opvolging en evaluatie.

Inzake de organisatie en inzet van de middelen, de werklastmeting en -verdeling

- Een concreet behoeftenplan opmaken van de middelen die vereist zijn om de opdrachten en taken uit te voeren, en plannen hoe deze zullen worden ingevuld en aangetrokken;
- Het opmaken van een geconsolideerd organigram met bepaling van functies, bezetting, rollen en communicatielijnen;
- Het beschikken over meetinstrumenten voor het verzamelen van kwantitatieve gegevens op het vlak van werklast en *output*, en het inzamelen van meetresultaten die er uit voortvloeien teneinde de werklast evenwichtig te kunnen verdelen.

Inzake de organisatie van en samenwerking tussen de analyse en de collecte

- Een formeel plan uitwerken waarbij voor elke materie de nodige (evenwichtige) collecte- en analysecapaciteit wordt bepaald, en waarbij wordt gegarandeerd dat de capaciteiten beschikbaar zijn en blijven. Zo nodig een herorganisatie overwegen van de analysefunctie als zelfstandige pijler binnen CI;
- Het opmaken en beschikbaar houden van '*designs*' die de samenwerking tussen de collecte en de analyse moeten aansturen (geïntegreerde *intelligence requirements* en *information collection plans*).

Inzake het informatiebeheer

- Het opstellen van een planning en een systeem om de achterstand bij de *input* van informatie in de database weg te werken en om te garanderen dat inkomende informatie binnen een redelijk termijn wordt ingeput;
- Het uitvoeren van een behoefteanalyse bij CI, inclusief in de provinciale posten, ten einde te bepalen wie nood heeft aan welke systemen (toegang tot interne en externe databanken, *softwares* …) en de implementatie daarvan;
- De organisatie van een opfrissingscyclus om de kennis en het gebruik van de beschikbare *IT-tools* te verbeteren;
- Methoden en interne richtlijnen opstellen die verhinderen dat fenomenen zoals '*broken links*' en het aanleggen van persoonlijke bestanden en opslagruimten, nog kunnen voorkomen;

- Het vastleggen van interne richtlijnen om de samenwerking tussen CI en de stafafdeling J-6 (verantwoordelijk voor communicatie- en informatiesystemen) vorm te geven zodat deze laatste beter kan inspelen op de behoeften van CI;
- Het aanduiden van een ICT-relaisfunctie binnen CI die daarvoor de nodige tijd en kennis heeft.

Inzake de infrastructuur

- Het dringend verbeteren van de materiële omstandigheden in het gebouw dat door de Directie CI wordt betrokken;
- Het wegwerken van de veiligheidsrisico's inzake Operations Security (OpSec) die voortvloeien uit de gebrekkige materiële infrastructuur.

XII.2.1.2. Aanbevelingen met een hoge prioriteit

Inzake het procesbeheer en de Standing Operating Procedures

- Procesbeschrijvingen en formele procedures uitwerken die de verschillende aspecten van de werking van de dienst beschrijven en een upgedate verzameling van *Standard Operating Procedures* (SOP) bijhouden die onder het personeel wordt verspreid en actief toegelicht;
- Het aanduiden binnen CI van een verantwoordelijke die het procesbeheer overziet.

Inzake de interne controle en risicobeheer

- Het ontwikkelen en implementeren binnen CI (maar ook binnen de ADIV) van een intern controlesysteem, waarbij de processen worden gemonitord en afwijkingen op de vooropgestelde normen worden gedetecteerd en gecorrigeerd;
- Het ontwikkelen en implementeren van een systeem van risicobeheer, waarbij de (operationele) risico's in kaart worden gebracht en maatregelen worden voorzien om deze op te vangen.

Inzake de ondersteuning en logistiek, binnen en buiten CI

- Het opmeten van de behoeften aan logistieke ondersteuning binnen CI en het opstellen van een realisatieplan;
- Het documenteren van de manier van samenwerking tussen CI en de stafafdelingen zodat deze beter kunnen inspelen op de behoeften van CI, en het aanduiden van verantwoordelijken binnen CI die als relais dienen (personeel, veiligheid, vorming …). Daarbij moet er in voorzien worden dat de stafdien-

sten, in acht genomen de vereisten inzake discretie, toegang krijgen tot alle gegevens nodig om hun taken adequaat op te nemen;
– Elk plan dat defensiewijde systemen (inzonderheid inzake ICT, maar ook aankoopbeheer …) op de ADIV en CI toepast, moet een studie bevatten over de gevolgen ervan voor de ADIV en CI en over hoe ongewenste gevolgen kunnen vermeden worden.

Inzake communicatie en feedback

– Binnen CI duidelijke en formele communicatierichtlijnen vastleggen (wat, hoe, wie, wanneer …) waarbij afgestapt wordt van de cultuur van mondelinge overdracht van informatie en instructies. Het expliciet toewijzen van de taak en de verantwoordelijkheid voor de interne communicatie aan een leidinggevend personeelslid van CI;
– Het ontwerpen en toepassen van systemen voor interne en externe *feedback* naar de betrokken personeelsleden.

Inzake het personeelsbeheer en loopbanen, vorming en opleiding

– De risico's en te nemen maatregelen in kaart brengen en opvangen die het gevolg zijn van de snelle toename van collectepersoneel, ten einde het evenwicht tussen collecte en analyse niet in gevaar te brengen;
– Het uitwerken van een vakrichting 'inlichtingen' voor militairen die in de inlichtingendienst willen werken, zodat zij beslagen op het terrein komen én in de inlichtingensector een werkelijke militaire loopbaan kunnen uitbouwen;
– Het bepalen van de vormingsbehoeften en maken van een vormingsplan op de domeinen waar het de personeelsleden van CI aan een *up-to-date* kennis (juridisch, operationeel) ontbreekt, en voorzien in een permanente opleiding om daaraan te remediëren. Idem wat betreft de kennis van managementtechnieken voor (aspirant-)leidinggevenden.

Inzake cultuur en tradecraft

– Het ontwikkelen van een aanpak om de verschillen in identiteit te overbruggen en het wij-zij gevoel tegen te gaan, en om te komen tot een reële ADIV-cultuur waarbij er begrip en respect is voor ieders rol en positie;
– Het neerschrijven van een formele procedure om delicate CI-casussen, waarbij personen en/of militairen van buiten en/of van binnen de dienst betrokken kunnen zijn, te behandelen en dit in acht genomen de vereiste vertrouwelijkheid. Duidelijk bepalen welke de verantwoordelijkheden daarbij zijn, wie wanneer moet tussenkomen en aan wie wanneer wordt gerapporteerd;
– De organisatie van overleg tussen de diverse directies van de ADIV ten einde tot een consensus te komen over de principes inzake *tradecraft* (inclusief

OpSec), met respect voor het verschil in rollen en positie van elkeen. Als resultaat daarvan een gemeenschappelijk gedragen *manual* opstellen over de gemeenschappelijk begrepen *tradecraft*;
– Het opfrissen van de regels van de *tradecraft* en OpSec, in het bijzonder wanneer nieuwe personeelsleden die niet uit de inlichtingenwereld komen, zich aandienen.

XII.2.1.3. Aanbevelingen met een gemiddelde prioriteit

Inzake de provinciale detachementen

– Het uitvoeren van een onderzoek naar de behoeften en de domeinen van meerwaarde van de provinciale detachementen. Het bepalen van de taakomschrijving en vereiste middelen waarbij de minimumbezetting en continuïteit (invloed verloven, ziektes, missies, vergaderingen) per post gegarandeerd wordt;
– Het opstellen en de hand houden van regels om de provinciale detachementen efficiënt aan te sturen en om de vereiste doorstroming van informatie en instructies te garanderen;
– Een onderzoek op te starten naar de ICT-behoeften in de provinciale posten (o.a. toegang tot databanken en ICT-tools).

Inzake de statuten en de individuele evaluatie

– Een onderzoek naar en opstellen van een plan voor het wegwerken van ongelijkheden (o.a. pecuniair) tussen personeel met verschillende statuten;
– Het in kaart brengen van de problemen gelieerd aan de verschillende statuten (aanwerving, beoordeling, sanctionering …), zelfs indien deze niet onmiddellijk kunnen worden aangepakt.

XII.2.2. DE AANWIJZING VAN EEN STATION COMMANDER IN OPERATIEZONES

Het Comité beveelt aan dat bij de militaire ontplooiing in een operatiezone een zoneverantwoordelijke '*Station Commander*' wordt aangewezen, verantwoordelijk voor de coördinatie van het geheel van activiteiten van de ADIV voor alle directies, bij toepassing van het principe van eenheid van commando.

XII.2.3. EVALUATIE BIJ DE GEOGRAFISCHE INPLANTING VAN MILITAIRE EENHEDEN

Het Vast Comité I beveelt aan dat er een regelmatige evaluatie zou worden uitgevoerd over de optimale geografische inplanting van de militaire eenheden bij

inzet in een operatie, rekening houdend met de snelle evolutie van de veiligheidssituatie en van de opdrachten opgedragen aan de Belgische eenheden.

XII.2.4. GEEN STRIKTE COMPARTIMENTERING BIJ DE ADIV

Met uitzondering van het specifieke geval waar leden van het personeel van ADIV zelf het voorwerp uitmaken van een veiligheids- of inlichtingenonderzoek, is het Vast Comité I geen voorstander van een strikte compartimentering tussen de directies van de ADIV. Daarbij moet het evident zijn dat iedere persoon die in bezit is van geclassificeerde en gevoelige informatie gehouden is tot geheimhouding op straffe van sancties. Daarentegen moet informatie die geclassificeerd en gevoelig is en die personeel van Defensie betreft, of die betrekking heeft op een bedreiging, gedeeld worden binnen de ADIV.

XII.2.5. DIVERSE AANBEVELINGEN TER VERBETERING VAN DE WERKING VAN EN SAMENWERKING TUSSEN DE DIENSTEN

In het kader van toezichtonderzoek naar de aanslag in Luik werden geen vaststellingen gedaan die wezen op tekortkomingen van de politie-, inlichtingen- en veiligheidsdiensten. Gelet op de aanbevelingen van de Onderzoekscommissie 'Terroristische aanslagen' van de Kamer van Volksvertegenwoordigers[234], formuleerden de Vaste Comités I en P ter verbetering van de werking van en samenwerking tussen de diensten onderstaande aanbevelingen.

XII.2.5.1. Het DG EPI als ondersteunende dienst van het OCAD

De bevoegde ministers zouden het initiatief moeten nemen om het DG EPI als steundienst van het OCAD aan te duiden aangezien deze dienst een belangrijke positie bekleedt in het kader van het detecteren en opvolgen van de radicalisering van gevangenen.[235] Daarbij moeten de nodige voorwaarden tot stand wor-

234 *Parl. St.* Kamer, 2017-18, 54K1752/009, titel 2 (Vierde tussentijds verslag over het onderdeel 'Radicalisme', d.d. 23 oktober 2017, hoofdstuk III, punt 4, zie in het bijzonder de randnummers 151-152 over het uitbouwen van een opleiding van penitentiaire beambten met inbegrip van het vaststellen van aanwijzingen van radicalisme en het creëren van contactpersonen radicalisme in iedere instelling met het oog op verzamelen en analyseren van informatie afkomstig uit observatie van gevangenen, alsmede de randnummers 159-161 inzake de uitwisseling van informatie tussen de gevangenis en andere diensten.

235 Middels het KB van 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 (*BS* 12 september 2018) werd deze aanbeveling gerealiseerd.

den gebracht om het DG EPI in staat te stellen deze rol kwaliteitsvol te vervullen, zoals het voorzien in middelen voor kwaliteitsvolle collecte- en analysecapaciteit binnen het gevangenismilieu, het uitwerken van procedures …

XII.2.5.2. Eenduidige terminologie in het normatieve kader

De bevoegde instanties moeten de verschillende toepasselijke normatieve teksten (wetten, besluiten, circulaires, dienstnota's …) aan een onderzoek onderwerpen teneinde na te gaan of de gebruikte terminologie (tekenen van radicalisering, (niet-)gewelddadig geradicaliseerd, proselitisme …) uitdrukkelijk, duidelijk en op eenzelfde manier worden gedefinieerd, en deze zo nodig doen aanpassen. Een goede uitwisseling van gegevens en samenwerking is ermee gebaat dat alle betrokken diensten dezelfde terminologie hanteren.

XII.2.5.3. Databestanden inzake geradicaliseerde gedetineerden

De diensten, verenigd in de Werkgroep Gevangenissen van het Plan Radicalisme, moesten ten behoeve van de bevoegde ministers tegen eind 2018 een voorstel voorleggen van welke gegevens van gevangenen onder welke voorwaarden in welke databestanden/lijsten zouden moeten worden opgenomen (en desgevallend geschrapt) en met elkaar kunnen worden gedeeld. Daarbij moet:

- bepaald worden welke procedures van gegevensuitwisseling en aanmaak van gegevensbanken verdere formalisering vereisen en hierover dienen voorstellen te worden opgemaakt;
- een taakverdeling worden afgesproken om informatie over deze personen uit te wisselen, te analyseren en voor de verschillende diensten toegankelijk te maken, en te bepalen welke informatie en volgens welke procedures desgevallend in de gemeenschappelijke gegevensbank wordt geplaatst (mits aanpassing van het betreffend reglementair kader);
- een raming worden gemaakt van de noodzakelijke middelen om dit in de praktijk te brengen.

Hierbij mag geen afbreuk worden gedaan aan de verschillende finaliteiten van alle betrokken diensten ter versterking van ieders informatiepositie (inlichtingenfinaliteit, ordehandhaving en criminaliteitsbestrijding, analyse van de dreiging, beheer van de gevangenen en deradicalisering).

XII.2.6. AANBEVELINGEN MET BETREKKING TOT DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN[236]

XII.2.6.1. De aanstelling van een veiligheidsconsulent[237]

Het niet-benoemen van een consulent voor de veiligheid of van een functionaris voor gegevensbescherming (DPO) blijft een belangrijke tekortkoming, vooral omdat het gaat om het aanspreekpunt voor het COC en het Vast Comité I. De ministers van Binnenlandse Zaken en Justitie, die verwerkingsverantwoordelijken zijn rechtvaardigen deze situatie door te stellen dat de WPA zou worden herzien na de aanpassing van het wettelijk kader over de bescherming van de persoonlijke levenssfeer. Het COC en het Vast Comité I voeren evenwel een controle uit op basis van de geldende (en niet de toekomstige) regelgeving. Bovendien merkten zij op dat de afwezigheid van een veiligheidsconsulent praktische problemen oplevert (niet-ontvankelijkheid bij een door een dienst gevraagde loggingscontrole; plotse en onverklaarbare periodes waarin de gegevensbank niet beschikbaar is; gebrek aan een gecoördineerde aanpak van veiligheidsincidenten …). Het COC en het Vast Comité I handhaven dus hun eerdere aanbeveling om over te gaan tot de nodige aanstellingen.[238]

XII.2.6.2. Een informaticatool voor de opvolging van bewaartermijnen

Het COC en het Vast Comité I herhalen hun aanbeveling om een informaticatool te ontwikkelen die het mogelijk maakt de bewaartermijnen van de gegevens die worden bedoeld in artikel 44/11/3*bis* § 5 van de WPA, op te volgen.

XII.2.6.3. Informatieplicht inzake veiligheidsincidenten

Het COC en het Vast Comité I wensen nauw op de hoogte te worden gehouden in geval van een veiligheidsincident dat een weerslag kan hebben op de vertrouwelijkheid van de gemeenschappelijke gegevensbank.

XII.2.6.4. De noodaak om de doorgifte te beveiligen

Het COC en het Vast Comité I hebben naar aanleiding van hun controleopdracht geen formele bevestiging ontvangen dat de in artikel 44/11/3*quater* WPA bedoelde evaluatie systematisch en vooraf wordt uitgevoerd voor de doorgifte van (uittreksels) van de informatiekaart aan derde instanties (d.w.z. diensten die niet worden

---

236 De eerste aanbevelingen vormen een herhaling van reeds eerder geformuleerde aanbevelingen (www.comiteri.be).

237 Zie hierover VAST COMITÉ I, *Activiteitenverslag 2017,* 105-106.

238 Ondertussen werd door beide ministers een DPO aangewezen.

bedoeld in art. 44/11/3*ter* WPA). Bovendien herinneren zij aan hun eerdere aanbeveling met betrekking tot de noodzaak om de doorgifte te beveiligen.

XII.2.6.5. Spontane controle van de loggings

Met uitzondering van één gecontroleerde dienst, werd de aanbeveling om spontaan een controle van de *loggings* uit te voeren, niet opgevolgd. Sommige diensten hebben gemeld dat zij in dat verband initiatieven hebben genomen (of binnenkort zullen nemen). De eerder geformuleerde aanbeveling blijft dus geldig.

XII.2.6.6. Aanbevelingen in verband met de lijsten van namen bestemd voor derden

De aanpassing van het wettelijk kader met betrekking tot de extractie en de doorgifte van lijsten aan derden, noopten het COC en het Vast Comité I tot het formuleren van diverse aanbevelingen:
- Geautomatiseerde vergelijkingen vereisen uitgebreide testen en alle beslissingen moeten worden genomen na menselijke tussenkomst en validatie;
- De basisdienst die een lijst verstrekt, dient de ontvanger van de lijst naar behoren te informeren (over de doelstelling van de lijst in het licht van de wettelijke opdracht van de ontvanger, het gebruik van de lijst uitsluitend voor die doelstelling, de beperkte bewaring van de lijst, de vereiste beveiligings-en vertrouwelijkheidsmaatregelen …), bijvoorbeeld door het sluiten van een protocolakkoord met de ontvangende dienst;
- Er dienen voorzorgsmaatregelen te worden genomen om ervoor te zorgen dat het gebruik van deze lijsten door derden voldoet aan veiligheidsvoorwaarden (vertrouwelijkheid, integriteit …) die gelijkwaardig zijn aan die welke zijn vastgesteld in de regelgeving inzake gemeenschappelijke gegevensbanken;
- De regelgeving over de gemeenschappelijke gegevensbanken kent het COC noch het Vast Comité I de bevoegdheid toe om het gebruik van de lijsten door derden te controleren. Beiden bevelen de verwerkingsverantwoordelijken aan om te beoordelen of het wettelijk kader in dit opzicht toereikend is, met name in het licht van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.

XII.2.6.7. Operationalisering van directe toegangen en rechtstreekse bevragingen

Medio 2018 had een aanzienlijk aantal partnerdiensten en de Justitiehuizen nog steeds geen toegang tot de productieomgeving van de gemeenschappelijke gege-

vensbank en gebruikte die bijgevolg niet. Het COC en het Vast Comité I hebben aanbevolen deze situatie te verhelpen.

Daarnaast moet het recht tot rechtstreekse bevraging van de Algemene Directie van het Crisicentrum worden geconcretiseerd.

Ten slotte stelde het COC in het Vast Comité I dat het reglementaire kader desgewenst moet aangepast worden aan de praktijk waaruit blijkt dat bepaalde centrale diensten van het DG EPI de databank voeden en niet de penitentiaire instellingen zelf, zoals nochtans voorzien in het KB (F)TF.

XII.2.6.8. Beheer van de vereiste veiligheidsmachtigingen

Het COC en het Vast Comité I beveelden aan om de (vrij lange) procedures voor de aanvraag van de veiligheidsmachtigingen snel op te starten. Daarentegen moet systematisch elk verlies van de '*need to know*' van een personeelslid worden gemeld, zodat wordt vermeden dat toegangsmachtigingen die niet noodzakelijk zijn worden behouden of dat veiligheidsonderzoeken die ondertussen nutteloos zijn geworden worden voortgezet.

XII.2.6.9. Actualisering van de validatieprocedures

De validatieprocedures die door bepaalde diensten vóór of naar aanleiding van de in 2018 uitgevoerde controle werden meegedeeld, hadden alleen betrekking op de FTF en moeten worden geactualiseerd voor de HTF en de HP. Bovendien moet het Vlaams Agentschap Jongerenwelzijn een intern validatiesysteem[239] implementeren (artikel 8 van het KB TF).

XII.2.7. BIJKOMENDE VERTAALCAPACITEIT IN HET KADER VAN SIGINT-OPDRACHTEN[240]

Om zijn doelstellingen te bereiken en de wettelijke opdrachten te kunnen uitoefenen, dient de ADIV te kunnen beschikken over voldoende menselijke en technische middelen in het domein van de SIGINT. Het wegwerken van het tekort aan personeel dat kan instaan voor vertalingen, vormt daarbij een prioriteit.

239 Zie 'Hoofdstuk VI. De controle van de gemeenschappelijke gegevensbanken'.
240 Zie 'Hoofdstuk III. Het toezicht op buitenlandse intercepties, beeldopnamen en it-intrusies'.

XII.3. AANBEVELING IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

XII.3.1. DE REGISTRATIE EN TER BESCHIKKING STELLING VAN GEGEVENS OVER GEWONE METHODEN

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 inzet van gewone methoden *ex* artikel 16/2 W.I&V. In zijn vorig activiteitenverslag beveelde het Comité de diensten aan ook deze gegevens te registreren en ter beschikking te stellen.[241] Dit gebeurde vooralsnog niet; het Comité herhaalt dan ook zijn aanbeveling.

241 VAST COMITÉ I, *Activiteitenverslag 2017*, 43.

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 2018 TOT 31 DECEMBER 2018)

Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse – officieuze coördinatie in het Duits, *BS* 4 april 2018

Wet van 21 mars 2018 tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiediensten te regelen, en tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, *BS* 16 april 2018

Wet van 23 februari 2018 houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *BS* 1 juni 2018

Wet van 19 juli 2018 tot wijziging van diverse bepalingen die betrekking hebben op de politiediensten en betreffende de Romeinse instellingen, *BS* 21 augustus 2018

Wet van 19 juli 2018 tot wijzing van de wet van diverse bepalingen betreffende het statuut van de militairen van het reservekader van de Krijgsmacht, *BS* 31 augustus 2018

Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, *BS* 5 september 2018

Wet van 15 juli 2018 houdende diverse bepalingen Binnenlandse Zaken, *BS* 25 september 2018

Wet van 13 september 2018 houdende wijziging van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *BS* 5 oktober 2018

K.B. 19 december 2017 houdende gedeeltelijke verdeling, betreffende de strijd tegen het terrorisme en het radicalisme van het provisioneel krediet ingeschreven in het programma 03-41-1 van de algemene uitgavenbegroting voor het begrotingsjaar 2017 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* 10 januari 2018

K.B. 13 december 2017 houdende gedeeltelijke verdeling, betreffende de strijd tegen het terrorisme en het radicalisme van het provisioneel krediet ingeschreven in het pro-

gramma 03-41-1 van de algemene uitgavenbegroting voor het begrotingsjaar 2017 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* 15 januari 2018

K.B. 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten – Duitse vertaling, *BS* 9 mei 2018

K.B. 23 april 2018 betreffende de gemeenschappelijke gegevensbank haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1*bis* "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt, *BS* 30 mei 2018

K.B. 23 april 2018 tot wijziging van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Foreign Terrorist Fighters en tot uitvoering van sommige bepalingen van de afdeling 1*bis* "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank Foreign Terrorist Fighters naar de gemeenschappelijke gegevensbank Terrorist Fighters, *BS* 30 mei 2018

K.B. 28 mei 2018 tot wijziging van het koninklijk besluit van 10 februari 2008 tot vaststelling van de wijze waarop wordt aangegeven dat er camerabewaking plaatsvindt, *BS* 1 juni 2018

K.B. 8 mei 2018 tot wijziging van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *BS* 1 juni 2018

K.B. 8 mei 2018 tot bepaling van de lijst van de gegevens en informatie die geraadpleegd kunnen worden in het kader van de uitvoering van een veiligheidsverificatie, *BS* 1 juni 2018

K.B. 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

K.B. 29 mei 2018 tot wijziging van het koninklijk besluit van 23 januari 2007 betreffende het personeel van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 11 juni 2018

K.B. 18 juni 2018 houdende aanwijzing van de voorzitter van de raad van beroep van de buitendiensten van de Veiligheid van de Staat, *BS* 27 juli 2018

K.B. 22 juli 2018 betreffende de basisopleiding van de personeelsleden van het kader van beveiligingsagenten van politie en van het kader van beveiligingsassistenten van politie en tot vaststelling van de inwerkingtreding van de artikelen 1, 9 tot 13, 15 tot 24, 33 tot 38 en 41 tot 49 van de wet van 12 november 2017 betreffende de beveiligingsassistenten en -agenten van politie en tot wijziging van sommige bepalingen met betrekking tot de politie, *BS* 16 augustus 2018

K.B. 30 juli 2018 houdende gedeeltelijke verdeling, betreffende schadevergoedingen en gerechtskosten van het provisioneel krediet ingeschreven in het programma 06-90-1 van de algemene uitgavenbegroting voor het begrotingsjaar 2018 bestemd tot het dekken van gerechtskosten en schadevergoedingen, achterstallige premies voor compe-

tentieontwikkeling, cybersecurity, investeringen in Defensie en andere diverse uitgaven, *BS* 21 augustus 2018

K.B. 2 september 2018 tot vastlegging van de nadere bepalingen voor kennisgeving alsook van de informatie te bezorgen aan het Instituut, conform artikel 33, § 2, vierde lid, en § 3, vijfde lid, van de wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 7 september 2018

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, *BS* 12 september 2018

M.B. 10 juli 2018 tot wijziging, wat betreft de Veiligheid van de Staat, van het ministerieel besluit van 11 juni 2018 besluit betreffende de overdracht van bevoegdheid van de minister van Justitie aan bepaalde autoriteiten inzake de gunning en de uitvoering van de overheidsopdrachten voor aanneming van werken, leveringen en diensten en inzake toelagen en diverse uitgaven, *BS* 19 juli 2018

M.B. 3 juli 2018 tot bepaling van de wapens en munitie die behoren tot de voorgeschreven uitrusting van de personeelsleden van de Krijgsmacht en tot vaststelling van de bijzondere bepalingen betreffende het verwerven, het voorhanden hebben, het bewaren, het dragen, het gebruiken en het vervreemden van deze wapens en munitie, *BS* 5 september 2018

M.B. 16 oktober 2018 houdende interne organisatie, overdracht van bevoegdheid en machtigingen tot handtekening in de Veiligheid van de Staat inzake de plaatsing en de uitvoering van overheidsopdrachten en inzake diverse uitgaven, *BS* 24 oktober 2018

Vergelijkende selectie van Franstalige Attachés internationale relaties (m/v/x) (niveau A1) voor de Veiligheid van de Staat, *BS* 10 januari 2018

Vergelijkende selectie van Nederlandstalige Attachés internationale relaties (m/v/x) (niveau A1) voor de Veiligheid van de Staat, *BS* 10 januari 2018

Vergelijkende selectie van Franstalige Deskundigen internationale relaties (m/v/x) (niveau B) voor de Veiligheid van de Staat, *BS* 10 januari 2018

Vergelijkende selectie van Nederlandstalige Deskundigen internationale relaties (m/v/x) (niveau B) voor de Veiligheid van de Staat, *BS* 10 januari 2018

Oproep tot kandidaten voor de mandaten van voorzitter en van eerste en tweede plaatsvervangende voorzitter van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *BS* 25 januari 2018

Vergelijkende Franstalige selecties voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat (FOD Justitie): assistent analisten (m/v/x)- opleidingsdeskundigen (m/v/x) – veiligheidsdeskundigen (m/v/x) – preventieadviseurs (m/v/x), *BS* 31 januari 2018

Vergelijkende Nederlandstalige selecties voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat (FOD Justitie): assistent analisten (m/v/x)- opleidingsdeskundigen (m/v/x) – veiligheidsdeskundigen (m/v/x) – preventieadviseurs (m/v/x), *BS* 31 januari 2018

Oproep tot kandidaten voor de mandaten van voorzitter en van eerste en tweede plaatsvervangende voorzitter van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I) – Erratum, *BS* 1 februari 2018

Vergelijkende selectie van Nederlandstalige netwerk/firewall beheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat (FOD Justitie), *BS* 2 februari 2018

Resultaat van de vergelijkende selectie van Franstalige Diensthoofd Budget en Boekhouding (m/v/x) (niveau A3) voor de Veiligheid van de Staat, *BS* 5 februari 2018

Vergelijkende selectie van Nederlandstalige ICT-consultants voor het OCAD (m/v/x) (niveau B) voor de FOD Binnenlandse Zaken, *BS* 5 februari 2018

Oproep tot kandidaten voor de mandaten van eerste en tweede plaatsvervangend lid (F) van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *BS* 6 februari 2018

Tweede oproep tot kandidaten voor de mandaten van eerste en tweede plaatsvervangend lid (F) van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I)), *BS* 26 mars 2018

Ministeriële omzendbrief van 29 maart 2018 betreffende veiligheidscontroles naar aanleiding van evenementen, *BS* 5 april 2018

Resultaat van de vergelijkende selectie van Nederlandstalige netwerk en firewallbeheerders (m/v/x) (niveau B) voor Veiligheid van de Staat, *BS* 16 april 2018

Vergelijkende selectie van Franstalige systeembeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat, *BS* 27 april 2018

Resultaat van de vergelijkende selectie van Franstalige Deskundige internationale relaties (m/v/x) (niveau B) voor de Veiligheid van de Staat, *BS* 30 april 2018

Omzendbrief van 22 mei 2018 van de minister van Veiligheid en Binnenlandse zaken en de minister van Justitie betreffende de informatie-uitwisseling rond en de opvolging van terrorist fighters en haatpropagandisten (Beperkte verspreiding art. 20 KB 24 maart 2000)

Resultaat van de vergelijkende selectie van Franstalige Attachés internationale relaties (m/v/x) (niveau A1) voor de Veiligheid van de Staat, *BS* 22 mei 2018

Aanwerving bij wijze van detachering en samenstelling van een wervingsreserve van Franstalige Commissarissen-auditors met een bijzondere kennis van ICT/Data (m/v) voor de Dienst Enquêtes van het Vast Comité I, *BS* 30 mei 2018

Resultaat van de vergelijkende selectie van Nederlandstalige Attachés internationale relaties (m/v/x) (niveau A1) voor de Veiligheid van de Staat, *BS* 4 juni 2018

Resultaten van de vergelijkende Nederlandstalige selectie voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat: Preventieadviseurs (m/v/x), *BS* 20 juni 2018

Resultaten van de vergelijkende Franstalige selectie voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat: Preventieadviseurs (m/v/x), *BS* 20 juni 2018

Resultaten van de vergelijkende Nederlandstalige selectie voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat: Assistent-analisten (m/v/x), *BS* 21 juni 2018

Resultaten van de vergelijkende Franstalige selectie voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat: Assistent-analisten (m/v/x), *BS* 21 juni 2018

Resultaten van de vergelijkende Franstalige selectie voor bevordering naar niveau B (specifiek gedeelte), voor de Veiligheid van de Staat: Veiligheidsdeskundigen, *BS* 27 juni 2018

Resultaten van de vergelijkende Nederlandstalige selectie voor bevordering naar niveau B (specifiek gedeelte), voor de Veiligheid van de Staat: Veiligheidsdeskundigen (m/v/x), *BS* 27 juni 2018

Resultaat van de vergelijkende selectie van Franstalige Systeembeheerders (m/v/x) (niveau B), voor de Veiligheid van de Staat, *BS* 18 juli 2018

Nieuwe oproep tot kandidaten voor het mandaat van tweede plaatsvervangend lid (F) van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *BS* 19 juli 2018

Vergelijkende selectie van Nederlandstalige Loopbaanbeheerders (m/v/x) (niveau A1) voor de Veiligheid van de Staat, *BS* 7 september 2018

Vergelijkende selectie van Nederlandstalige Budgetdeskundigen (m/v/x) (niveau B) voor de Veiligheid van de Staat, *BS* 7 september 2018

Vergelijkende selectie van Nederlandstalige Diensthoofden logistiek (m/v/x) (niveau A3) voor de Veiligheid van de Staat, *BS* 14 september 2018

Vergelijkende selectie van Franstalige Diensthoofden logistiek (m/v/x) (niveau A3) voor de Veiligheid van de Staat, *BS* 14 september 2018

Oproep tot kandidaten voor het mandaat van Nederlandstalig lid en van eerste en tweede plaatsvervangend lid (N) van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *BS* 27 september 2018

Protocolakkoord van 13 november 2018 betreffende de samenwerking tussen de Passagiersinformatie-eenheid en de ADIV in het kader van de Wet betreffende de verwerking van passagiersgegevens (Beperkte verspreiding, art. 20 KB 24 maart 2000)

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 2018 TOT 31 DECEMBER 2018)

Senaat

Conferentie van voorzitters van de Parlementen van de Europese Unie, Tallinn, 23-24 april 2018, *Parl. St.* Senaat 2017-18, nr. 6-432/1

Kamer van Volksvertegenwoordigers

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – benoeming van de voorzitter en van de eerste en tweede plaatsvervangende voorzitters – oproep tot kandidaten, *Hand.* Kamer 2017-18, 11 januari 2018, CRIV54PLEN210, 52

Wetsontwerp houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *Parl. St.* Kamer 2017-18, nrs. 54K2767/003 tot 54K2767/006 en *Hand.* Kamer 2017-18, 18 januari 2018, CRIV54PLEN211, 51

Wetsontwerp wijziging van de wet op het politieambt het gebruik van camera's door de politiediensten te regelen, en tot wijziging de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik bewakingscamera's, van de wet van november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid, *Parl. St.* Kamer 2017-18,

nrs. 54K2855/001 tot 54K2855/007 en *Hand.* Kamer 2017-18, 8 maart 2018, CRIV54PLEN217, 62

Wetsontwerp tot wijziging van het Consulaire Wetboek, *Parl. St.* Kamer 2017-18, nrs. 54K2989/001 tot 54K2989/005

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – Benoeming van de voorzitter – ingediende kandidatuur, *Hand.* Kamer 2017-18, 15 maart 2018, CRIV54PLEN219, 64

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – Benoeming van de voorzitter, *Hand.* Kamer 2017-18, 19 april 2018, CRIV54PLEN223, 58

Aanpassing van de begrotingen van ontvangsten en uitgaven voor het begrotingsjaar 2018, *Parl. St.* Kamer 2017-18, nr. 54K3035/001

Wetsontwerp tot wijziging van diverse bepalingen die betrekking hebben op de politiediensten en betreffende de Romeinse instellingen, *Parl. St.* Kamer 2017-18, nr. 54K3089/001

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – Benoeming van een eerste en tweede plaatsvervangend lid (F) – Derde oproep tot kandidaten, *Hand.* Kamer 2017-18, 3 mei 2018, CRIV54PLEN227, 40

Wetsontwerp houdende wijziging van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *Parl. St.* Kamer 2017-18, nrs. 54K3107/001 tot 54K3107/008, *Hand.* Kamer 2017-18, 18 juli 2018, CRIV54PLEN242, 1 en *Hand.* Kamer 2017-18, 19 juli 2018, CRIV54PLEN243, 47

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – Benoeming van een eerste en tweede plaatsvervangend lid (F) – Ingediende kandidaturen, *Hand.* Kamer 2017-18, 28 juni 2018, CRIV54PLEN236, 77

Wetsontwerp houdende organisatie van een centraal aanspreekpunt van rekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest, *Parl. St.* Kamer 2017-18, nr. 54K3114/001

Wetsontwerp tot wijziging van de wet van 16 mei 2001 houdende statuut van de militairen van het reservekader van de Krijgsmacht, *Parl. St.* Kamer 2017-18, nr. 54K3125/001

Wetsontwerp houdende diverse bepalingen Binnenlandse Zaken, *Parl. St.* Kamer 2017-18, nrs. 54K3127/001 tot 54K3127/003

Wetsvoorstel tot wijziging van de wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *Parl. St.* Kamer 2017-18, nr. 54K3166/001

Voorstel van resolutie betreffende de bestrijding van antisemitisme, *Parl. St.* Kamer 2017-18, nr. 54K3194/001

Het gebruik van drones in de veiligheids- en defensiesector, *Parl. St.* Kamer 2017-18, nr. 54K3224/001

Gedachtewisseling met de heer Marc De Mesmaeker, commissaris-generaal van de federale politie, *Hand.* Kamer 2017-18, 16 juli 2018, CRIV54COM950, 1

Wetsontwerp houdende diverse bepalingen met betrekking tot het Rijksregister en de bevolkingsregisters, *Parl. St.* Kamer 2017-18, nr. 54K3256/001

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – Benoeming van het tweede Franstalig plaatsvervangend lid – Ingediende kandidatuur, *Hand.* Kamer 2017-18, 20 september 2018, CRIV54PLEN244, 45

Comité P – Benoeming van de voorzitter en van de eerste en de tweede plaatsvervangende voorzitter – Ingediende kandidaturen, *Hand.* Kamer 2017-18, 26 september 2018, CRIV54PLEN245, 28

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – Benoeming van het Nederlandstalig lid en van het eerste en het tweede Nederlandstalig plaatsvervangend lid – Oproep tot kandidaten, *Hand.* Kamer 2017-18, 26 september 2018, CRIV54PLEN245, 28

Wetsontwerp houdende de Middelenbegroting voor het begrotingsjaar 2019, *Parl. St.* Kamer 2018-19, nr. 54K3293/001

Voorstel van resolutie over de evolutie en de modernisering van het reservekader van de Krijgsmacht, *Parl. St.* Kamer 2018-19, nr. 54K2683/005

Vast Comité van toezicht op de politiediensten – Benoeming van de voorzitter, *Hand.* Kamer 2018-19, 14 november 2018, CRIV54PLEN254, 52

Wetsontwerp houdende de Algemene uitgavenbegroting voor het begrotingsjaar 2019, *Parl. St.* Kamer 2018-19, nrs. 54K3294/001, 54K3294/018, 54K3294/028, 54K3294/029, 54K3294/033 en 54K3294/039

Verantwoording van de algemene uitgavenbegroting voor het begrotingsjaar 2019 en FOD Economie, KMO, Middenstand en Energie, *Parl. St.* Kamer 2018-19, nrs. 54K3295/002, 54K3295/003, 54K3295/006, 54K3295/007, 54K3295/008, 54K3295/009, 54K3295/010, 54K3295/016 en 54K3295/017

Algemene beleidsnota: Bestrijding van de sociale fraude, Privacy en Noordzee, Buitenlandse Zaken, Justitie en Defensie, FOD Werkgelegenheid, arbeid en sociaal overleg, *Parl. St.* Kamer 2018-19, nrs. 54K3296/003, 54K3296/005, 54K3296/006, 54K3296/015 en 54K3296/028

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, nr. 54K3340/001

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, Controleorgaan op de politionele informatie, BIM-Commissie, Federale Deontologische Commissie, *Parl. St.* Kamer 2018-19, nrs. 54K3418/001 tot 54K3418/005 en *Hand.* Kamer 2018-19, 20 december 2018, CRIV54PLEN264, 67

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 2018 TOT 31 DECEMBER 2018)

Senaat

Schriftelijke vraag van M. Taelman aan de minister van Justitie over de 'cybercrime – bedrijfsleven – maatregelen' (Senaat 2014-15, 4 december 2014, Vr. nr. 6-277)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over 'ondersteuningsnetwerk van veroordeelde terroristen – oproepen tot het bevrijden van gedetineerden – handhaving – Veiligheid van de Staat' (Senaat 2017-18, 14 april 2017, Vr. nr. 6-1379)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over 'ondersteuningsnetwerk van veroordeelde terroristen – oproepen tot het bevrijden van gedetineerden – handhaving – Veiligheid van de Staat' (Senaat 2017-18, 14 april 2017, Vr. nr. 6-1383

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over de 'Veiligheid van de Staat (VSSE) – buitenlandse partnerdiensten – vraag tot telefoonidentificatie – responstijd – terrorisme' (Senaat 2017-18, 29 november 2017, Vr. nr. 6-1671)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Defensie over het 'Vast Comité I – voorspellend karakter van de inlichtingendienst – behoefte aan feedback' (Senaat 2017-18, 29 november 2017, Vr. nr. 6-1673)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Defensie over de 'Algemene Dienst Inlichtingen en Veiligheid (ADIV) – Vast Comité I – Informatiepositie – Databeheer' (Senaat 2017-18, 29 november 2017, Vr. nr. 6-1674)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie 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 2017-18, 8 december 2017, Vr. nr. 6-1681)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie 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 2017-18, 8 december 2017, Vr. nr. 6-1687)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie 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 2017-18, 8 december 2017, Vr. nr. 6-1690)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over 'wetenschappelijk en economisch potentieel (WEP) – bescherming relaties tussen de Veiligheid van de Staat, de onderzoekscentra en de privésector' (Senaat 2017-18, 8 december 2017, Vr. nr. 6-1693)

Schriftelijke vraag van J.-J. De Gucht aan de minister van Justitie over de 'Veiligheid van de Staat (VSSE) – Algemene Dienst Inlichting en Veiligheid (ADIV) – Social Media Intelligence (SOCMINT) – personeelsleden – aanwerving – personeel met (Arabi-

sche) talenkennis en kennis van allochtone milieus' (Senaat 2017-18, 29 december 2017, Vr. nr. 6-1737)

Schriftelijke vraag van P. Van Rompuy aan de minister van Sociale Zaken over de 'Staatsveiligheid – cyberveiligheid – Chinese netwerkinfrastructuur – veiligheid van het Belgische telefoonnetwerk' (Senaat 2017-18, 28 juni 2018, Vr. nr. 6- 1922)

Kamer van Volksvertegenwoordigers

Vraag van V. Yüksel aan de minister van Binnenlandse Zaken over 'de Internet Referral Unit van de federale politie' (*Hand*. Kamer 2017-18, 10 januari 2018, CRIV54COM795, 14, Vr. nr. 22854)

Vraag van K. Gabriëls aan de minister van Binnenlandse Zaken over het 'dreigingsniveau 3' (*Vr. en Ant*. Kamer 2017-18, 10 januari 2018, QRVA 141, 308, Vr. nr. 2351)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over de 'terrorismebestrijding – organisatie van een missie naar Saudi-Arabië' (*Vr. en Ant*. Kamer 2017-18, 10 januari 2018, QRVA 141, 397, Vr. nr. 1203)

Vraag van F. Dewinter aan de minister van Justitie over 'Ibrahim El Bakraoui' (*Vr. en Ant*. Kamer 2017-18, 10 januari 2018, QRVA 141, 427, Vr. nr. 1196)

Vraag van F. Dewinter aan de minister van Justitie over 'van terrorisme of terroristische medeplichtigheid verdachte asielzoekers' (*Vr. en Ant*. Kamer 2017-18, 10 januari 2018, QRVA 141, 454, Vr. nr. 2079)

Vraag van Ph. Pivin aan de minister van Justitie over de 'signalen van radicalisering in scholen' (*Vr. en Ant*. Kamer 2017-18, 10 januari 2018, QRVA 141, 461, Vr. nr. 2158)

Vraag van Ph. Pivin aan de minister Binnenlandse Zaken over 'de intrekking van de verblijfsvergunning van de imam van de Grote Moskee' (*Hand*. Kamer 2017-18, 17 januari 2018, CRIV54COM797, 2, Vr. nr. 22314)

Samengevoegde vragen van K. Jadin en V. Yüksel aan de minister van Defensie over 'de gevolgen van operatie Vigilant Guardian' (*Hand*. Kamer 2017-18, 17 januari 2018, CRIV54COM798, 10, Vr. nrs. 22747 en 23031)

Vraag van K. Metsu aan de minister van Justitie over 'de inlichtingendiensten in de gevangenissen' (*Hand*. Kamer 2017-18, 17 januari 2018, CRIV54COM799, 25, Vr. nr. 22976)

Vraag van K. Metsu aan de minister van Justitie over 'de meertaligheid van cipiers' (*Hand*. Kamer 2017-18, 17 januari 2018, CRIV54COM799, 26, Vr. nr. 22977)

Vraag van K. Metsu aan de minister van Justitie over 'de risicoprofielen in onze gevangenissen' (*Hand*. Kamer 2017-18, 17 januari 2018, CRIV54COM799, 24, Vr. nr. 22978)

Vraag van C. Van Cauter aan de minister van Justitie over 'de opvolging van veroordeelden voor terroristische misdrijven' (*Hand*. Kamer 2017-18, 17 januari 2018, CRIV54COM799, 21, Vr. nr. 23015)

Vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'van terrorisme of terroristische medeplichtigheid verdachte asielzoekers' (*Vr. en Ant*. Kamer 2017-18, 17 januari 2018, QRVA 142, 175, Vr. nr. 2456)

Vraag van K. Gabriëls aan de minister van Binnenlandse Zaken over 'de arrestatie van haatprediker Chadlioui' (*Vr. en Ant*. Kamer 2017-18, 17 januari 2018, QRVA 142, 192, Vr. nr. 2611)

Vraag van K. Gabriëls aan de minister van Binnenlandse Zaken over de 'terreuraanslag in Brussel-Centraal op 20 juni 2017' (*Vr. en Ant*. Kamer 2017-18, 17 januari 2018, QRVA 142, 196, Vr. nr. 2625)

Vraag van B. Vermeulen aan de minister van Binnenlandse Zaken over de 'ANPR-camera's – lokale, gewestelijke en federale netwerken' (*Vr. en Ant*. Kamer 2017-18, 17 januari 2018, QRVA 142, 230, Vr. nr. 2712)

Samengevoegde vragen van Ph. Pivin en G. Dallemagne aan de minister van Binnenlandse Zaken over 'de onderhandelingen over de Grote Moskee van Brussel' (*Hand.* Kamer 2017-18, 18 januari 2018, CRIV54PLEN211, 10, Vr. nrs. 2545 en 2546)

Vraag van T. Vandenput aan de minister van Buitenlandse Zaken over 'de ontmoeting met de minister van Buitenlandse Zaken van Saudi-Arabië' (*Hand.* Kamer 2017-18, 18 januari 2018, CRIV54PLEN211, 16, Vr. nr. 2551)

Vraag van V. Wouters aan de Eerste Minister over 'de parlementaire controle: het beantwoorden van vragen door de ministers van de regering-Michel' (*Hand.* Kamer 2017-18, 18 januari 2018, CRIV54PLEN211, 23, Vr. nr. 2555)

Vraag van Ph. Pivin aan de minister van Justitie over de 'inlichtingendiensten – uniformisering van de registratietechnieken' (*Vr. en Ant*. Kamer 2017-18, 29 januari 2018, QRVA 143, 281, Vr. nr. 891)

Vraag van W. Janssen aan de minister van Justitie over de 'FOD Justitie – de vergroening van het wagenpark' (*Vr. en Ant*. Kamer 2017-18, 29 januari 2018, QRVA 143, 321, Vr. nr. 2202)

Vraag van S. Crusnière aan de minister van Justitie over 'Waals-Brabant – personeelsbezetting bij de parketten' (*Vr. en Ant*. Kamer 2017-18, 29 januari 2018, QRVA 143, 333, Vr. nr. 2233)

Vraag van B. Hellings aan de minister van Justitie over de 'dood van Dag Hammarskjöld – onderzoek van de VN' (*Vr. en Ant*. Kamer 2017-18, 29 januari 2018, QRVA 143, 338, Vr. nr. 2262)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over 'de situatie van de Belgen die in Irak en Syrië aangehouden werden' (*Hand.* Kamer 2017-18, 1 februari 2018, CRIV54PLEN213, 34, Vr. nr. 2601)

Vraag van G. Calomne aan de minister van Justitie over 'de brochure van de Veiligheid van de Staat over het salafisme' (*Hand.* Kamer 2017-18, 1 februari 2018, CRIV54PLEN213, 40, Vr. nr. 2602)

Vraag van V. Yüksel aan de minister van Defensie over 'de situatie van de Belgen die in Irak en Syrië aangehouden werden' (*Hand.* Kamer 2017-18, 1 februari 2018, CRIV54PLEN213, 45, Vr. nr. 2605)

Vraag van A. Top aan de minister van Defensie over 'de samenwerking met de Koerdische militie YPG in Syrië' (*Hand.* Kamer 2017-18, 7 februari 2018, CRIV54COM815, 6, Vr. nr. 23489)

Vraag van É. Thiébaut de minister van Binnenlandse Zaken over 'de racistische schietpartij in Italië en het surveilleren van extreemrechts' (*Hand.* Kamer 2017-18, 7 februari 2018, CRIV54COM817, 17, Vr. nr. 23553)

Vraag van G. Calomne aan de minister van Binnenlandse Zaken over 'het dark web' (*Vr. en Ant*. Kamer 2017-18, 9 februari 2018, QRVA 144, 113, Vr. nr. 2435)

Vraag van K. Degroote aan de minister van Binnenlandse Zaken over de 'evolutie overtal officieren' (*Vr. en Ant*. Kamer 2017-18, 16 februari 2018, QRVA 145, 162, Vr. nr. 2808)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'spionnen in onze gevangenissen' (*Vr. en Ant*. Kamer 2017-18, 16 februari 2018, QRVA 145, 188, Vr. nr. 2870)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'reorganisatie van de inlichtingendiensten' (*Vr. en Ant*. Kamer 2017-18, 16 februari 2018, QRVA 145, 191, Vr. nr. 2893)

Vraag van G. Calomne aan de minister van Binnenlandse Zaken over de 'screening van vluchtelingen op radicalisme' (*Vr. en Ant*. Kamer 2017-18, 16 februari 2018, QRVA 145, 293, Vr. nr. 1296)

Vraag van B. Hellings aan de minister van Defensie over 'de opvolging van de Belgische foreign terrorist fighters die nog in Irak en in Syrië verblijven' (*Hand*. Kamer 2017-18, 28 februari 2018, CRIV54COM828, 15, Vr. nr. 23834)

Vraag van A. Frédéric aan de minister van Justitie over 'de Veiligheid van de Staat en de sekten' (*Hand*. Kamer 2017-18, 28 februari 2018, CRIV54COM829, 4, Vr. nr. 23753)

Vraag van S. Van Hecke aan de minister van Justitie over 'de hervorming van het veiligheidsadvies over gebedshuizen in het kader van een aanvraag tot erkenning' (*Hand*. Kamer 2017-18, 28 februari 2018, CRIV54COM829, 18, Vr. nr. 23807)

Vraag van G. Dallemagne aan de minister van Justitie over 'de informatie betreffende Oussama Atar' (*Hand*. Kamer 2017-18, 28 februari 2018, CRIV54COM829, 22, Vr. nr. 23941)

Samengevoegde vragen van H. Bonte en P. Dewael aan de minister van Justitie over de 'terrorismedatabank' (*Hand*. Kamer 2017-18, 1 maart 2018, CRIV54PLEN216, 11, Vr. nrs. 2660 en 2661)

Samengevoegde vragen van M. Van Hees, B. Hellings, R. Hedebouw, O. Maingain, M. De Coninck, W. De Vriendt en J. Fernandez Fernandez aan de minister van Binnenlandse Zaken over 'de verificatie van artikel 3 van het Europees Verdrag voor de Rechten van de Mens' (*Hand*. Kamer 2017-18, 6 maart 2018, CRIV54COM832, 8, Vr. nrs. 23134, 23135, 23438, 23475, 23482, 23740, 23814, 24062, 24063, 24070 en 24082)

Samengevoegde vragen van B. Vermeulen en S. Lahaye-Battheu aan de minister van Binnenlandse Zaken over de 'transmigratie' (*Hand*. Kamer 2017-18, 7 maart 2018, CRIV54COM835, 6, Vr. nrs. 24051 en 24163)

Vraag van B. Hellings aan de minister van Buitenlandse Zaken over 'de opvolging van de Belgische Foreign Terrorist Fighters die nog in Irak en in Syrië verblijven' (*Hand*. Kamer 2017-18, 7 maart 2018, CRIV54COM838, 31, Vr. nr. 23836)

Vraag van V. Yüksel aan de minister van Defensie over 'de deelname en de bijdrage van het Belgische leger aan de operatie tegen IS' (*Hand*. Kamer 2017-18, 8 maart 2018, CRIV54PLEN217, 23, Vr. nr. 2689)

Vraag van F. Dewinter aan de minister van Justitie over 'de screening van kandidaat-asielzoekers op linken met terroristische groeperingen of met radicale potentieel gewelddadige groeperingen' (*Vr. en Ant*. Kamer 2017-18, 29 maart 2018, QRVA 150, 210, Vr. nr. 2409)

Vraag van K. Jadin aan de minister van Justitie over de 'Kazachse geheime diensten in België' (*Vr. en Ant*. Kamer 2017-18, 29 maart 2018, QRVA 150, 223, Vr. nr. 2475)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over 'de financiële transacties in verband met terrorisme' (*Vr. en Ant*. Kamer 2017-18, 4 april 2018, QRVA 151, 152, Vr. nr. 1883)

Vraag van Ph. Pivin aan de minister van Justitie over de 'informatiedoorgifte tussen Europese inlichtingendiensten' (*Vr. en Ant*. Kamer 2017-18, 4 april 2018, QRVA 151, 213, Vr. nr. 2286)

Vraag van P. Buysrogge aan de minister van Justitie over de 'VSSE – infrastructuurinvesteringen' (*Vr. en Ant.* Kamer 2017-18, 4 april 2018, QRVA 151, 230, Vr. nr. 2470)

Vraag van B. Vermeulen aan de minister van Defensie over de 'valse profielen op sociale media, cyberspionage bij overheidsmedewerkers' (*Vr. en Ant.* Kamer 2017-18, 4 april 2018, QRVA 151, 317, Vr. nr. 1445)

Vraag van K. Jadin aan de minister van Defensie over de 'reorganisatie van de inlichtingendiensten' (*Vr. en Ant.* Kamer 2017-18, 4 april 2018, QRVA 151, 320, Vr. nr. 1442)

Vraag van P. Luykx aan de minister van Buitenlandse Zaken over 'de beveiliging van de Belgische risico-vertegenwoordigingen' (*Vr. en Ant.* Kamer 2017-18, 20 april 2018, QRVA 153, 238, Vr. nr. 1339)

Vraag van S. Vermeulen aan de minister van Binnenlandse Zaken over 'het vermelden van een andere nationaliteit in het Rijksregister' (*Hand.* Kamer 2017-18, 25 april 2018, CRIV54COM880, 22, Vr. nr. 24867)

Vraag van K. Metsu aan de minister van Justitie over de 'terugkerende vrouwen van Syriëstrijders' (*Vr. en Ant.* Kamer 2017-18, 9 mei 2018, QRVA 155, 330, Vr. nr. 2303)

Vraag van B. Vermeulen aan de minister van Justitie over het 'valse profielen op sociale media – cyberspionage bij overheidsmedewerkers' (*Vr. en Ant.* Kamer 2017-18, 9 mei 2018, QRVA 155, 335, Vr. nr. 2354)

Vraag van Ph. Pivin aan de minister van Defensie over de 'beveiliging van de openbare ruimte – Coördinatie Vigilant Guardian' (*Vr. en Ant.* Kamer 2017-18, 9 mei 2018, QRVA 155, 452, Vr. nr. 1461)

Vraag van S. Van Hecke aan de minister van Justitie over 'de beveiliging van de Belgische risico-vertegenwoordigingen' (*Vr. en Ant.* Kamer 2017-18, 17 mei 2018, QRVA 156, 237, Vr. nr2304)

Samengevoegde vragen van B. Helling, P. Vanvelthoven en G. Dallemagne aan de minister van Financiën over de 'levering – tot 24 maal toe door 3 Belgische bedrijven – van chemische producten die gebruikt kunnen worden voor de productie van chemische wapens in Syrië' (*Hand.* Kamer 2017-18, 22 mai 2018, CRIV54COM901, 14, Vr. nrs. 25283, 25335 en 25344)

Samengevoegde vragen van D. Van der Maelen en B. Hellings aan de minister van Buitenlandse Zaken over 'de aanduiding van een hoge, onafhankelijke ambtenaar in het kader van het onderzoek naar de dood van Dag Hammarskjöld' (*Hand.* Kamer 2017-18, 23 mai 2018, CRIV54COM904, 18, Vr. nrs. 24839 en 25006)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over 'de Interpol-signalering van O. Atar' (*Hand.* Kamer 2017-18, 30 mei 2018, CRIV54COM909, 1, Vr. nr. 25257)

Samengevoegde vragen van O. Maingain, B. Pas, C. Van Cauter, L. Onkelinx, S. Van Hecke, R. Hedebouw, H. Bonte, S. De Wit, Ph. Pivin, M. de Lamotte, R. Terwingen, V. Wouters, M. Gerkens en A. Carcaci aan de minister van Binnenlandse Zaken over 'de terreuraanslag in Luik' (*Hand.* Kamer 2017-18, 31 mei 2018, CRIV54PLEN231, 2, Vr. nrs. 2884 tot 2896 en 2904)

Samengevoegde vragen van W. De Vriendt, T. Vandenput, A. Top, S. Crusnière en P. Buysrogge aan de minister van Defensie over 'de activiteiten van de ADIV in Syrië' (*Hand.* Kamer 2017-18, 31 mei 2018, CRIV54COM919, 23, Vr. nrs. 25692, 25696, 25716, 25725 en 26050)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'Centrale terroristendatabank' (*Vr. en Ant.* Kamer 2017-18, 6 juni 2018, QRVA 158, 230, Vr. nr. 3088)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'beveiliging van de openbare ruimte – coördinatie Vigilant Guardian' (*Vr. en Ant.* Kamer 2017-18, 6 juni 2018, QRVA 158, 232, Vr. nr. 3114)

Vraag van G. Calomne aan de minister van Justitie over de 'nieuwe bijzondere opsporings- en onderzoeksmethoden van de Veiligheid van de Staat' (*Vr. en Ant.* Kamer 2017-18, 6 juni 2018, QRVA 158, 338, Vr. nr. 2648)

Vraag van B. Vermeulen aan de minister van Defensie over de 'militairen en burgerpersoneel bij Defensie met een meervoudige nationaliteit' (*Vr. en Ant.* Kamer 2017-18, 6 juni 2018, QRVA 158, 399, Vr. nr. 1483)

Vraag van S. Lahaye-Battheu aan de minister van Binnenlandse Zaken over het 'personeelskader lokale en federale politie' (*Vr. en Ant.* Kamer 2017-18, 12 juni 2018, QRVA 159, 267, Vr. nr. 1144)

Vraag van B. Vermeulen aan de minister van Binnenlandse Zaken over de 'valse profielen op sociale media – cyberspionage bij overheidsmedewerkers' (*Vr. en Ant.* Kamer 2017-18, 12 juni 2018, QRVA 159, 284, Vr. nr. 2844)

Vraag van K. Degroote aan de minister van Binnenlandse Zaken over de 'oorzaken politietekorten' (*Vr. en Ant.* Kamer 2017-18, 12 juni 2018, QRVA 159, 287, Vr. nr. 2863)

Vraag van P. De Roover aan de minister van Justitie over 'het OCAD-rapport inzake de Grote Moskee' (*Hand.* Kamer 2017-18, 13 juni 2018, CRIV54COM923, 1, Vr. nr. 25751)

Vraag van B. Vermeulen aan de minister van Justitie over 'de financiering van moskeeën met geld uit de drugshandel' (*Hand.* Kamer 2017-18, 13 juni 2018, CRIV54COM923, 2, Vr. nr. 25728)

Vraag van J.-J. Flahaux aan de minister van Buitenlandse Zaken over de 'internationale conferentie over de financiering van het terrorisme' (*Vr. en Ant.* Kamer 2017-18, 18 juni 2018, QRVA 160, 140, Vr. nr. 1358)

Vraag van A. Frédéric aan de minister van Justitie over 'de situatie bij de top van OCAD' (*Hand.* Kamer 2017-18, 20 juni 2018, CRIV54COM930, 1, Vr. nr. 25752)

Samengevoegde vragen van C. Van Cauter en S. De Wit aan de minister van Justitie over 'de beperkte detentie van een geradicaliseerde gevangene' (*Hand.* Kamer 2017-18, 20 juni 2018, CRIV54COM930, 3, Vr. nrs. 26127 en 26228)

Samengevoegde vragen van C. Van Cauter en A. Lambrecht aan de minister van Justitie over 'de arrestatie van een contact van Benjamin Herman' (*Hand.* Kamer 2017-18, 20 juni 2018, CRIV54COM930, 7, Vr. nrs. 25944 en 26017)

Vraag van S. De Wit aan de minister van Justitie over 'de informatiedoorstroming naar politie en burgemeesters wanneer bepaalde gedetineerden tijdelijk of voorwaardelijk worden vrijgelaten' (*Hand.* Kamer 2017-18, 20 juni 2018, CRIV54COM930, 18, Vr. nr. 26231)

Vraag van Ph. Goffin aan de minister van Justitie over 'de termijnen voor het verkrijgen van een veiligheidsmachtiging voor de gevangenisdirecteurs' (*Hand.* Kamer 2017-18, 20 juni 2018, CRIV54COM930, 21, Vr. nr. 26164)

Vraag van B. Friart aan de minister van Binnenlandse Zaken over het 'personeelsbestand van de politie' (*Vr. en Ant.* Kamer 2017-18, 22 juin 2018, QRVA 161, 100, Vr. nr. 2219)

Vraag van A. Top aan de minister van Binnenlandse Zaken over de 'politiekorpsen van groot Brussel' (*Vr. en Ant.* Kamer 2017-18, 22 juin 2018, QRVA 161, 107, Vr. nr. 2720)

Vraag van B. Pas aan de minister van Binnenlandse Zaken over de 'federale en lokale politie – evolutie' (*Vr. en Ant.* Kamer 2017-18, 22 juin 2018, QRVA 161, 115, Vr. nr. 2987)

Vraag van P. Luykx aan de minister van Buitenlandse Zaken over de 'accreditatie van diplomaten in België' (*Vr. en Ant.* Kamer 2017-18, 22 juin 2018, QRVA 161, 191, Vr. nr. 1364)

Vraag van V. Yüksel aan de minister van Defensie over 'de outsourcing bij het ministerie van Landsverdediging' (*Hand.* Kamer 2017-18, 27 juni 2018, CRIV54COM936, 12, Vr. nr. 26051)

Vraag van G. Dallemagne aan de Eerste Minister over de 'financiering van terrorisme' (*Vr. en Ant.* Kamer 2017-18, 29 juin 2018, QRVA 162, 97, Vr. nr. 320)

Vraag van K. Jadin aan de eerste minister over de 'financiering van terrorisme' (*Vr. en Ant.* Kamer 2017-18, 29 juin 2018, QRVA 162, 102, Vr. nr. 321)

Vraag van F. Schepmans aan de minister van Defensie over de 'cybersecuritydeskundigen' (*Vr. en Ant.* Kamer 2017-18, 29 juin 2018, QRVA 162, 229, Vr. nr. 1509)

Samengevoegde vragen van B. Vermeulen en V. Yüksel aan de minister van Binnenlandse Zaken over de 'inmenging van buitenlandse mogendheden tijdens de verkiezingen in België' (*Hand.* Kamer 2017-18, 18 juli 2018, CRIV54COM954, 12, Vr. nrs. 26354 en 26631)

Vraag van B. Lutgen aan de minister van Defensie over de 'defensieattachés in het buitenland' (*Vr. en Ant.* Kamer 2017-18, 20 juli 2018, QRVA 164, 336, Vr. nr. 1547)

Vraag van B. Hellings aan de minister van Binnenlandse Zaken over de 'CGVS – regels inzake de screening van sociale media' (*Vr. en Ant.* Kamer 2017-18, 20 juli 2018, QRVA 164, 463, Vr. nr. 1418)

Vraag van E. Burton aan de minister van Justitie over de 'gedetineerden die geradicaliseerd zijn of dreigen te radicaliseren' (*Vr. en Ant.* Kamer 2017-18, 3 augustus 2018, QRVA 165, 351, Vr. nr. 2561)

Vraag van G. Calomne aan de minister van Justitie over de 'voertuigen van overheidsdiensten met een dieselmotor' (*Vr. en Ant.* Kamer 2017-18, 3 augustus 2018, QRVA 165, 386, Vr. nr. 2777)

Vraag van J.-J. Flahaux aan de minister van Justitie over de 'terrorismebestrijding – Frans-Belgische samenwerking' (*Vr. en Ant.* Kamer 2017-18, 3 augustus 2018, QRVA 165, 392, Vr. nr. 2789)

Vraag van G. Dallemagne aan de minister van Justitie over 'met de interdepartementale provisie inzake de strijd tegen het terrorisme gefinancierde projecten' (*Vr. en Ant.* Kamer 2017-18, 3 augustus 2018, QRVA 165, 396, Vr. nr. 2793)

Vraag van P. Luykx aan de minister van Buitenlandse Zaken over 'de inzet van Belgische ambassades bij het opsporen van Syriëstrijders' (*Vr. en Ant.* Kamer 2017-18, 4 september 2018, QRVA 167, 211, Vr. nr. 231)

Vraag van N. Lijnen aan de minister van Buitenlandse Zaken over de 'betrokkenheid Iran bij verijdelde aanslag' (*Vr. en Ant.* Kamer 2017-18, 4 september 2018, QRVA 167, 272, Vr. nr. 1495)

Samengevoegde vragen van J Chabot en G. Dallemagne aan de minister van Defensie over 'de Algemene Dienst Inlichting en Veiligheid (ADIV)' (*Hand.* Kamer 2017-18, 19 september 2018, CRIV54COM960, 16, Vr. nrs. 26671 en 26915)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over 'het standpunt van Saudi-Arabië over de Grote Moskee van Brussel' (*Hand.* Kamer 2017-18, 20 september 2018, CRIV54PLEN244, 21, Vr. nr. 3070)

Vraag van W. De Vriendt aan de minister van Buitenlandse Zaken over de 'boots on the ground in Syrië' (*Vr. en Ant.* Kamer 2017-18, 28 september 2018, QRVA 170, 107, Vr. nr. 1487)

Vraag van G. Calomne aan de minister van Justitie over de 'Staatsveiligheid – recruitment' (*Vr. en Ant.* Kamer 2017-18, 28 september 2018, QRVA 170, 143, Vr. nr. 2613)

Vraag van L. Onkelinx aan de minister van Binnenlandse Zaken over 'de bij de federale politie genomen maatregelen om zich te beveiligen tegen hacking en cyberaanvallen' (*Hand.* Kamer 2017-18, 3 oktober 2018, CRIV54COM974, 1, Vr. nr. 26648)

Vraag van E. Burton aan de minister van Justitie over de 'talenkennis van de penitentiair beambten in de Deradexafdelingen' (*Vr. en Ant.* Kamer 2018-19, 8 oktober 2018, QRVA 171, 372, Vr. nr. 2560)

Vraag van G. Calomne aan de minister van Justitie over de 'rekrutering van beïnvloedbare personen door de terreurnetwerken' (*Vr. en Ant.* Kamer 2018-19, 8 oktober 2018, QRVA 171, 379, Vr. nr. 2752)

Vraag van B. Vermeulen aan de minister van Justitie over de 'buitenlandse financiering van politieke partijen' (*Vr. en Ant.* Kamer 2018-19, 8 oktober 2018, QRVA 171, 387, Vr. nr. 2799)

Vraag van B. Hellings aan de minister van Justitie over de 'overeenstemming van de handelwijze van het parket van Brussel met de geest van het Wetboek van de Belgische nationaliteit' (*Vr. en Ant.* Kamer 2018-19, 16 oktober 2018, QRVA 172, 189, Vr. nr. 789)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over 'het uitblijven van een reactie van België naar aanleiding van de in Villepinte verijdelde aanslag' (*Hand.* Kamer 2018-19, 17 oktober 2018, CRIV54COM982, 19, Vr. nr. 27126)

Vraag van J. Chabot aan de minister van Defensie over 'de ADIV en de dreiging van cyberaanvallen' (*Hand.* Kamer 2018-19, 7 november 2018, CRIV54COM992, 4, Vr. nr. 27147)

Vraag van Ph. Pivin aan de minister van Justitie over 'de voorwaarden voor de vrijlating van geradicaliseerde gevangenen n' (*Hand.* Kamer 2018-19, 7 november 2018, CRIV54COM994, 8, Vr. nr. 27326)

Vraag van B. Bonte aan de minister van Binnenlandse Zaken over de 'eenmaking Brusselse politiezones – nood aan een regeringsinitiatie' (*Vr. en Ant.* Kamer 2018-19, 9 november 2018, QRVA 174, 153, Vr. nr. 2290)

Vraag van P. Dewael aan de minister van Binnenlandse Zaken over de 'financiering van moskeeën vanuit de Golfstaten' (*Vr. en Ant.* Kamer 2018-19, 9 november 2018, QRVA 174, 163, Vr. nr. 3212)

Vraag van J.-J. Flahaux aan de minister van Binnenlandse Zaken over de 'personen in België die bekend zijn bij de veiligheidsdiensten' (*Vr. en Ant.* Kamer 2018-19, 9 november 2018, QRVA 174, 177, Vr. nr. 3314)

Vraag van V. Yüksel aan de minister van Justitie over de 'teruggekeerde Syriëstrijders' (*Vr. en Ant.* Kamer 2018-19, 9 november 2018, QRVA 174, 350, Vr. nr. 2009)

Vraag van K. Degroote aan de minister van Binnenlandse Zaken over de 'personeelsbestand geïntegreerde politie' (*Vr. en Ant.* Kamer 2018-19, 22 november 2018, QRVA 175, 150, Vr. nr. 3490)

Vraag van D. Van der Maelen aan de minister van Buitenlandse Zaken over 'het gebruik van Sputnik News op een officieel sociaal mediakanaal van de Belgische minister van Buitenlandse Zaken' (*Vr. en Ant.* Kamer 2018-19, 22 november 2018, QRVA 175, 261, Vr. nr. 1536)

Vraag van G. Dallemagne aan de minister van Buitenlandse Zaken over de 'Russische inmenging in de Italiaanse verkiezingscampagne om extreemrechts te bevoordelen' (*Vr. en Ant.* Kamer 2018-19, 22 november 2018, QRVA 175, 273, Vr. nr. 1543)

Vraag van B. Vermeulen aan de Eerste Minister over 'het CCB' (*Vr. en Ant.* Kamer 2018-19, 6 december 2018, QRVA 176, 133, Vr. nr. 345)

Vraag van B. Vermeulen aan de eerste minister over de 'inmenging van buitenlandse mogendheden tijdens Belgische verkiezingen' (*Vr. en Ant.* Kamer 2018-19, 6 december 2018, QRVA 176, 140, Vr. nr. 348)

Vraag van K. Degroote aan de minister van Binnenlandse Zaken over de 'mobiliteit geïntegreerde politie' (*Vr. en Ant.* Kamer 2018-19, 6 december 2018, QRVA 176, 191, Vr. nr. 3487)

Vraag van H. Bonte aan de minister van Justitie over de 'Foreign terrorist fighters en de goksector' (*Vr. en Ant.* Kamer 2018-19, 6 december 2018, QRVA 176, 243, Vr. nr. 2373)

Vraag van B. Pas aan de minister van Justitie over de 'databank inzake terrorisme en extremisme' (*Vr. en Ant.* Kamer 2018-19, 6 december 2018, QRVA 176, 245, Vr. nr. 2539)

Samengevoegde vragen van V. Matz, Ph. Pivin en S. De Crom aan de minister van Binnenlandse Zaken over 'de politiestakingen' (*Hand.* Kamer 2018-19, 13 december 2018, CRIV54PLEN262, 12, Vr. nrs. 3301 tot 3303)

Vraag van H. Bonte aan de minister van Justitie over 'de vrijlating van een haatprediker en de nood aan terbeschikkingstelling' (*Hand.* Kamer 2018-19, 13 december 2018, CRIV54PLEN262, 17, Vr. nr. 3306)

Vraag van A. Lambrecht aan de minister van Justitie over de 'geradicaliseerde gedetineerden' (*Hand.* Kamer 2018-19, 21 december 2018, CRIV54PLEN177, 67, Vr. nr. 2474)

Vraag van P. De Roover aan de minister van Justitie over de 'religieuze instellingen – buitenlandse financieringsstromen' (*Hand.* Kamer 2018-19, 21 december 2018, CRIV54PLEN177, 77, Vr. nr. 2723)

BIJALGE D.
VERSTERKING VAN HET TOEZICHT OP DE INTERNATIONALE GEGEVENSUITWISSELING TUSSEN DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Een samenwerking tussen:

Belgian Standing Intelligence Agencies Review Committee
(Comité permanent de contrôle des services de renseignement et de sécurité / Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten)
www.comiteri.be

Danish Intelligence Oversight Board
(Tilsynet med Efterretningstjenesterne)
www.tet.dk

Review Committee on the Intelligence and Security Services - The Netherlands
(Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten)
www.ctivd.nl

EOS Committee - The Norwegian Parliamentary Intelligence Oversight Committee
(EOS-utvalget)
www.eos-utvalget.no

Independent Oversight Authority for Intelligence Activities (OA-IA)
(Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND/ Autorité de surveillance indépendante des activités de renseignement AS-Rens)
www.ab-nd.admin.ch

1. INHOUD

Vijf Europese toezichthouders op de inlichtingendiensten hebben een nieuw samenwerkingsinitiatief opgestart.
In deze verklaring zullen we:

- Ons project beschrijven, wat inhield dat eenieder een onderzoek voerde naar het gebruik door de inlichtingendiensten van de respectievelijke landen van informatie inzake foreign terrorist fighters en waarbij de methodologie, best practices en ervaringen werden gedeeld.
- De uitdagingen aanpakken waarmee we werden geconfronteerd bij het toezicht op internationale gegevensuitwisseling, met inbegrip van het risico op een toezichthiaat wanneer inlichtingen- en veiligheidsdiensten internationaal samenwerken.
- Mogelijkheden aanreiken om vooruitgang te boeken inzake de versterking van de samenwerking op vlak van toezicht, bijvoorbeeld door het verminderen van de geheimhouding tussen toezichtsinstanties zodat bepaalde informatie kan worden gedeeld en dit met het oog op een verbetering van het toezicht op internationale gegevensuitwisseling.

2. INLEIDING

Recente terreuraanslagen, zoals deze in Parijs, Brussel en Londen, werden uitgevoerd door personen die werden aangestuurd, aangemoedigd of geïnspireerd door ISIS, Al Qaida of vergelijkbare terroristische groeperingen. De dreiging van *homegrown* en terugkerende *foreign fighters* identificeren en onderzoeken is een belangrijke taak voor de inlichtingen- en veiligheidsdiensten in heel Europa.

De dreiging van jihadistisch terrorisme werd de voorbije jaren steeds complexer en wijdverbreider. Het onderzoeken van die dreiging vereist internationale samenwerking tussen inlichtingen- en veiligheidsdiensten, zowel op bilateraal als op multilateraal vlak. Een dergelijke samenwerking bestaat in Europa en met andere landen. Omwille van die verhoogde samenwerking, is ook de uitwisseling van persoonsgegevens tussen de diensten toegenomen. Gegevensuitwisseling met partnerdiensten is een van de dagelijkse activiteiten van inlichtingen- en veiligheidsdiensten. Gegevens kunnen daarbij op verschillende manieren worden uitgewisseld, zowel mondeling als schriftelijk.

De toezichtsorganen hebben uiteraard de ontwikkeling van de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten op de voet gevolgd. Aangezien ons respectieve toezichtsmandaat strikt nationaal is, maakten we ons zorgen over een mogelijks 'toezichtshiaat'. In het ideale geval, zijn de nationale toezichtsstelsels complementair: wanneer de ene toezichtsinstantie de grenzen van haar nationale mandaat bereikt, is een andere bevoegd om effectief toezicht te houden. Echter, de nationale wetgeving met betrekking tot de uitwisseling van gegevens en het toezicht op dergelijke uitwisselingen voldoet niet steeds aan die voorwaarden. Bovendien zou de internationale samenwerking tussen inlichtingendiensten zich op zodanige wijze kunnen ontwikkelen dat nationaal toezicht de samenwerking niet langer kan bijhouden. Dan zou een 'democratisch deficit' of een 'toezichtshiaat' kunnen ontstaan.

In het licht hiervan, hebben de vijf toezichtsorganen van België, Denemarken, Nederland, Noorwegen en Zwitserland besloten om een gezamenlijk project op te starten om

ervaringen en methoden uit te wisselen. Elke toezichthoudende instantie heeft een nationaal onderzoek gevoerd naar de internationale uitwisseling van gegevens over *foreign terrorist fighters* door de inlichtingen- en veiligheidsdiensten waarop ze respectievelijk toezicht houdt.

Deze nationale toezichtonderzoeken werden min of meer gelijktijdig uitgevoerd, elk vanuit de eigen nationale context en binnen het kader van het nationaal mandaat. Er werd regelmatig bijeengekomen om onderzoeksmethoden te vergelijken, juridische kaders te interpreteren, juridische en praktische problemen te bespreken en de bevindingen en conclusies te verzamelen. Er werd geen geclassificeerde informatie uitgewisseld.

3. BESTAANDE TOEZICHTSPRAKTIJKEN INZAKE GEGEVENSUITWISSELING

De deelnemende toezichtorganen houden op diverse manieren toezicht op de gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten. We kunnen
- de samenwerkingsrelaties of afspraken tussen inlichtingen- en veiligheidsdiensten beoordelen;
- de legitimiteit en kwaliteit van specifieke gegevensuitwisseling met buitenlandse diensten beoordelen;
- het systeem van gegevensuitwisseling als geheel beoordelen, met inbegrip van de waarborgen;
- betrokken zijn bij procedures betreffende individuele rechtsmiddelen en klachten.

Hoewel de mandaten van de toezichthouders verschillend zijn, hebben we allemaal een breed scala van instrumenten voor het toezicht op internationale gegevensuitwisseling.

Beoordeling van de samenwerkingsverbanden

Toezichthouders kunnen beoordelen of de samenwerkingsverbanden tussen de eigen dienst en de diensten van partnerlanden al dan niet aan bepaalde criteria voldoen. De wetgeving met betrekking tot inlichtingen- en veiligheidsdiensten kan specifieke criteria inzake samenwerking vooropstellen. Gewoonlijk omvatten deze criteria de noodzaak tot samenwerking, de eerbiediging van de mensenrechten en het bestaan van wetgeving met betrekking tot gegevensbescherming en/of betrouwbaarheid. Er moet een hoge drempel zijn voor de samenwerking met diensten die niet aan de criteria voldoen. De toezichtinstanties van België, Nederland, Noorwegen en Zwitserland beoordelen de overwegingen die worden gemaakt door hun nationale diensten.

Samenwerkingsverbanden tussen de diensten kunnen gebaseerd zijn op overeenkomsten, bijvoorbeeld intentieverklaringen of *memoranda of understanding*. Dergelijke overeenkomsten zijn gewoonlijk niet juridisch afdwingbaar, maar bieden een praktisch kader voor de uitwisseling van gegevens door de diensten. Zelfs het bestaan van sommige van die overeenkomsten is geclassificeerd. Andere overeenkomsten worden dan weer door overheden of door de diensten zelf openbaar gemaakt. Ze kunnen de contouren schetsen van de samenwerkingsrelatie door thema's aan te reiken zoals het doel van de samenwerking, hoe de samenwerking naar verwachting zal functioneren, de beperkingen betref-

fende de openbaarmaking aan derden of procedurele aspecten van de samenwerking. De toezichthouders van de vijf landen kunnen die overeenkomsten beoordelen of rapporteren of ze in overeenstemming zijn met de nationale wet- en regelgeving.

Beoordeling van de legitimiteit van specifieke gegevensuitwisselingen

Toezichtsinstanties kunnen beoordelen of individuele gegevensuitwisselingen aan de wettelijke vereisten opgelegd door nationale wetten en regelgeving voldoen.

De nationale wetgevingen van onze landen delen een aantal gemeenschappelijke kenmerken, met name de beginselen van noodzakelijkheid en evenredigheid. Die gemeenschappelijke beginselen vinden hun oorsprong in internationale wetgevende kaders zoals het Europees Verdrag voor de Rechten van de Mens. Het noodzakelijkheidsbeginsel omvat de vereiste van een duidelijk en wettelijk doel voor de gegevensuitwisseling en de redelijke verwachting dat de uitwisseling van de gegevens aan dit doel zal beantwoorden. Het evenredigheidsbeginsel vereist dat de dienst het doel van de uitwisseling afzet tegen de ernst van de inbreuk op de grondrechten. De meeste nationale wetgevingen bevatten nog andere vereisten, zoals de redelijkheid, correctheid, effectiviteit en betrouwbaarheid van de gegevensuitwisseling.

Het interne beleid van de diensten kan bovendien extra regels voor gegevensuitwisseling vaststellen. Een dergelijk beleid kan bijvoorbeeld nader specificeren welke type gegevensuitwisseling is toegestaan onder welke omstandigheden, welk toelatingsniveau is vereist en welk gebruik mag worden gemaakt van de ontvangen gegevens. Wanneer nationale wetgeving of bilaterale en multilaterale overeenkomsten ontbreken of niets zeggen over een specifieke aangelegenheid, kan intern beleid extra waarborgen bieden.

Beoordeling van de kwaliteit van specifieke gegevensuitwisselingen

Kwaliteit kan betrekking hebben op de inhoud of op de *format* van gegevens. Wat inhoud betreft, betekent kwaliteit dat de gegevens correct, voldoende duidelijk en nauwkeurig geformuleerd zijn, bevestigd door onderliggende gegevens, *up-to-date* en met een indicatie van de waarschijnlijkheid of betrouwbaarheid ervan. Wat *format* betreft, hebben kwaliteitsaspecten betrekking op de opname van een rubriceringsniveau, de datum van de uitwisseling, de aangewezen ontvangende partnerdienst(en) en voorbehouden met betrekking tot het verdere gebruik van de gegevens. De vijf toezichtsinstanties kunnen de kwaliteit van de gegevensuitwisseling in dit opzicht beoordelen.

Kwaliteit kan ook een andere betekenis hebben. Het kan betrekking hebben op efficiëntie en effectiviteit, d.w.z. of de gegevensuitwisseling relevant is, of de uitwisseling tijdig is gebeurd en of ze haar doel heeft bereikt. Dit soort kwaliteitsbeoordeling is minder gebruikelijk voor toezichthouders. De Belgische en Zwitserse toezichtsorganen zijn uitdrukkelijk bevoegd om te beoordelen of de gegevensuitwisseling effectief en efficiënt is verlopen.

Beoordeling van het systeem van gegevensuitwisseling als geheel
Toezichtinstanties kunnen een bredere aanpak hanteren bij het beoordelen van de legitimiteit van de gegevensuitwisseling. Bij het beoordelen van bepaalde multilaterale samenwerkingsverbanden kijkt de Nederlandse toezichthouder uitdrukkelijk naar het systeem van gegevensuitwisseling als geheel en naar de bescherming van individuele rechten in dat systeem. Hoewel bepaalde specifieke gegevensuitwisselingen legitiem kunnen zijn, kan het systeem nog steeds onvoldoende waarborgen bevatten om de legitimiteit van de gegevensuitwisseling op langere termijn te waarborgen. Dit soort beoordeling kan helpen om onrechtmatige gegevensuitwisseling tussen de inlichtingen- en veiligheidsdiensten te voorkomen.

Men zou een vergelijkbare aanpak kunnen voorstaan bij het beoordelen van de kwaliteit van de gegevensuitwisseling. Wanneer de uitwisseling van gegevens is bedoeld om jihadisme aan te pakken, kan de algemene kwaliteit van de gegevensuitwisseling worden gemeten door de hoeveelheid gedeelde informatie te onderzoeken die heeft geleid tot vervolging en veroordeling, of zelfs tot een directe voorkoming van een terreuraanslag. Maar de bruikbaarheid van de uitgewisselde gegevens op die manier meten, kan een hele uitdaging zijn. Dergelijke beoordelingen worden vaak gestart nadat een terreuraanslag heeft plaatsgevonden. De toezichtinstantie beoordeelt dan of de relevante gegevens voldoende en adequaat met nationale en internationale partners werden uitgewisseld. De Belgische toezichtinstantie was bij dit soort beoordelingen betrokken.

Betrokkenheid bij individuele rechtsmiddelen en klachten

In het algemeen kunnen de toezichtinstanties in de vijf landen klachten van individuen ontvangen met betrekking tot de activiteiten van de nationale inlichtingen- en veiligheidsdiensten. Meestal kunnen toezichthouders niet-juridisch bindende adviezen of aanbevelingen doen aan de inlichtingen- en veiligheidsdiensten en/of de ministers die politieke verantwoordelijkheid dragen. Gewoonlijk houden de diensten rekening met dergelijke adviezen of aanbevelingen. In 2017 werd in Nederland een nieuwe wet aangenomen die de toezichthouder de bevoegdheid geeft om bindende besluiten over klachten te nemen. Dit kan ook een bevel zijn om de uitoefening van een bevoegdheid te beëindigen of de verwerkte gegevens te vernietigen of te verwijderen.

De geheimhouding die nodig is voor de inlichtingen- en veiligheidsdiensten om hun activiteiten uit te oefenen, beperkt gewoonlijk het recht van een persoon op toegang tot persoonsgegevens. Sommige landen geven individuen expliciet het recht om de nationale toezichthouder te vragen om de persoonsgegevens te bekijken die hun diensten over hem of haar hebben verwerkt. In Denemarken mag elkeen het Deense toezichtorgaan vragen om te onderzoeken of de veiligheidsdienst onrechtmatig persoonsgegevens over hem of haar verwerkt. Voor de militaire inlichtingendienst, is dit beperkt tot inwoners van Denemarken. In beide gevallen kan de Deense toezichthouder de opdracht geven om de persoonsgegevens van de aanvrager te verwijderen.

In België is het toezichtorgaan verplicht alle klachten te onderzoeken die niet kennelijk ongegrond zijn. De klager ontvangt de algemene bevindingen van het onderzoek en heeft

dan de mogelijkheid om die bevindingen te gebruiken voor de rechtbank of een administratieve autoriteit. In sommige specifieke gevallen moet de toezichtinstantie na een klacht een officieel advies aan een rechtbank geven en met betrekking tot twee andere klachten (het gebruik van bijzondere inlichtingenmethoden en gegevensbescherming) kan het bindende besluiten nemen.

In Noorwegen hebben inwoners hetzelfde recht om een klacht in te dienen bij de toezichtinstantie als een burger vermoedt dat hij of zij aan onrechtmatig toezicht is onderworpen. De Noorse toezichtinstantie heeft echter niet de bevoegdheid om de verwijdering van gegevens te bevelen. In Zwitserland behandelt dan weer de Federal Data Protection & Information Commissioner (FDPIC) individuele verzoeken over gegevensverwerking.

4. UITDAGINGEN VOOR HET TOEZICHT OP INTERNATIONALE GEGEVENS-UITWISSELING

In de loop van ons project hebben we vastgesteld dat de nauwere samenwerking tussen inlichtingen- en veiligheidsdiensten en de uitwisseling van gegevens tussen deze diensten, vooral op multilateraal niveau, juridische en praktische uitdagingen kan inhouden voor de toezichtinstanties.

Toezicht overschrijdt de landsgrenzen niet

De nationale wetgeving bevordert vaak de samenwerking en uitwisseling van informatie tussen inlichtingen- en veiligheidsdiensten, zowel bilateraal als multilateraal. Maar ze biedt meestal geen specifieke rechtsgrond voor toezichtinstanties om samen te werken of informatie over personen uit te wisselen. Geen van de vijf toezichthouders die samenwerken in het kader van deze gemeenschappelijke verklaring heeft een expliciete rechtsgrond om gegevens met een andere toezichtinstantie uit te wisselen, en al zeker niet wanneer het geclassificeerde informatie betreft.

Inlichtingen- en veiligheidsdiensten kunnen landsgrenzen overschrijden, maar toezichtinstanties kunnen dat niet. Het toezicht is beperkt tot een nationaal mandaat. Dit weerspiegelt slechts één kant van gegevensuitwisseling: ofwel richt het toezicht zich op het verstrekken van gegevens en de voorafgaande verzameling ervan, ofwel op de ontvangst van gegevens en het gebruik ervan. Nationale toezichtinstanties zijn afzonderlijk niet in staat om zich geen volledig beeld van de uitwisseling van persoonsgegevens vormen, laat staan dat ze de rechtmatigheid van het hele uitwisselingsproces kunnen beoordelen.

Een dergelijke beperking voor nationaal toezicht vormt niet noodzakelijk een 'toezichthiaat'. Wanneer het toezicht aan weerszijden van de grens allesomvattend en effectief is, is er geen hiaat tussen de mandaten van de toezichtinstanties. Maar wanneer het gaat om samenwerking tussen inlichtingen- en veiligheidsdiensten – voornamelijk multilaterale samenwerking – is de samenwerking van toezichthouders slechts zo sterk als haar zwakste schakel.

De uitdaging van samenwerking tegenover geheimhouding

Toezichtinstanties zijn beperkt tot nationale regels inzake geheimhouding en kunnen de inhoud van hun onderzoeken niet delen en bespreken met uitzondering van wat als openbare informatie werd aangeduid. In de praktijk betekent dit dat de toezichtinstanties slechts heel beperkt inzicht hebben in de vraag of het toezicht op 'de andere kant' van gegevensuitwisseling effectief is of dat er een toezichthiaat is. Toezichtorganen kunnen niet alleen geen grenzen overschrijden, ze kunnen ook niet met andere toezichtinstanties delen wat er binnen hun grenzen gebeurt.

Naarmate het gezamenlijk project tussen de vijf toezichthouders vorderde, werden we ons bij talloze gelegenheden bewust van het feit dat we zelfs niet in staat waren om zaken die ons allen bekend waren te bespreken, zoals bijvoorbeeld de inhoud van overeenkomsten tussen de diensten waarop we toezicht houden. Daarnaast werden we ons ook bewust dat wat in het ene land als openbare informatie wordt beschouwd, in een ander land als vertrouwelijk kan worden beschouwd. Dit leverde problemen op voor dit project en beperkte de mogelijkheid om de thematiek in kwestie uitgebreid te bespreken.

Beoordeling van noodzakelijkheid en evenredigheid

Zoals hierboven vermeld, beoordelen de toezichthouders voortdurend of de uitwisseling van gegevens noodzakelijk is voor een specifiek doel en in verhouding staat tot het nagestreefde doel. Dit vereist dat toezichtorganen rekening houden met het beschermingsniveau van de individuele rechten dat wordt geboden door de ontvangende dienst. Naarmate het volume van gegevensuitwisseling en het aantal buitenlandse diensten waarmee de gegevens worden gedeeld toeneemt, zal dit een steeds groter probleem vormen voor de toezichtinstanties. Deze test van noodzakelijkheid en evenredigheid kan abstracter worden en kan aan waarde verliezen wanneer de uitgewisselde gegevens minder specifiek zijn of wanneer ze worden uitgewisseld binnen een grotere groep van inlichtingen- en veiligheidsdiensten.

Verschillende nationale wettelijke regelingen kunnen verschillende legitimiteits- en kwaliteitsnormen omvatten voor het verzamelen, verwerken, bewaren en uitwisselen van gegevens. Het beschermingsniveau van individuele rechten dat wordt geboden door de dienst die de gegevens ontvangt, is een belangrijk element bij het beoordelen van de evenredigheid van een bepaalde gegevensuitwisseling. Dit is niet altijd eenvoudig vast te stellen, omdat inlichtingen- en veiligheidsdiensten niet altijd open zijn over alle aspecten van het bestaande juridisch kader en de normen die ze toepassen.

In het kader van de multilaterale gegevensuitwisseling, kunnen gemeenschappelijke normen en definities helpen bepalen onder welke omstandigheden de gegevensuitwisseling als noodzakelijk en evenredig wordt beschouwd en welk minimumniveau van gegevensbescherming nodig is om de individuele rechten voldoende te waarborgen. Alle partijen – inlichtingen- en veiligheidsdiensten en toezichthouders – hebben belang bij dergelijke gemeenschappelijke normen en een gemeenschappelijke interpretatie van de bestaande

juridische waarborgen. Dit kan ook bijdragen aan de legitimiteit van de multilaterale uitwisseling in kwestie.

Sommige landen maken een onderscheid tussen burgers en buitenlanders

Sommige nationale wetgevende kaders bieden voor onderdanen of inwoners een hogere mate van bescherming en meer geprivilegieerde toegang tot individuele rechtsmiddelen dan voor buitenlanders of niet-ingezetenen. Het onderscheid tussen die groepen kan leiden tot beperkte toegang of helemaal geen toegang tot individuele rechtsmiddelen voor buitenlanders of niet-ingezetenen van wie de gegevens door de respectieve inlichtingen- of veiligheidsdienst werden uitgewisseld.

Een vergelijkbaar onderscheid kan het mandaat van de toezichtinstantie bepalen. Sommige toezichtinstanties hebben alleen het mandaat om de gegevensuitwisseling met betrekking tot onderdanen of ingezetenen te beoordelen. Het verstrekken van gegevens met betrekking tot andere personen, kan buiten hun bereik liggen. Als geen andere toezichtinstantie dit deel van de gegevensuitwisseling op effectieve wijze kan beoordelen, is er een toezichtshiaat.

Middelen en methoden voor gegevensuitwisseling

Inlichtingen- en veiligheidsdiensten wisselen op verschillende manieren gegevens uit. Sommige middelen en methoden voor gegevensuitwisseling vormen een extra uitdaging voor de toezichtinstanties. Een voorbeeld van een dergelijke uitdaging is de informele uitwisseling van gegevens en de vraag hoe men efficiënt toezicht kan bieden op gegevens die worden uitgewisseld op congressen en vergaderingen, telefonisch, enz. Door de toename van internationale gegevensuitwisseling kan het nodig voor toezichtinstanties om meer geavanceerde methoden voor toezicht te bedenken, aangezien het niet langer mogelijk is om elke uitwisseling van gegevens te beoordelen. Met betrekking tot gegevensbescherming kunnen ontwikkelingen in multilaterale gegevensuitwisseling de verantwoordelijkheid inroepen van alle deelnemende diensten en de toezichtinstanties. Om de individuele rechten voldoende te beschermen, kan het nodig zijn dat inlichtingen- en veiligheidsdiensten de normen die zij toepassen bespreken en streven naar een gelijk minimumniveau van bescherming door alle deelnemende diensten.

5. TOEZICHT OP INTERNATIONALE GEGEVENSUITWISSELING – DE TOEKOMST

Ons project heeft aangetoond dat de inspanningen van de inlichtingen- en veiligheidsdiensten om nieuwe manieren te vinden om op effectieve wijze gegevens uit te wisselen, vooral op multilateraal niveau, en de grote toename van de hoeveelheid uitgewisselde gegevens, op hun beurt tot nieuwe uitdagingen voor de toezichtinstanties hebben geleid. Dit geldt zowel voor de limieten van de nationale mandaten van de toezichthouders en hun onvermogen om internationale gegevensuitwisseling adequaat te bespreken met andere toezichtorganen, als voor hun eigen inspanningen om hun procedures en methoden te vernieuwen om effectief toezicht te waarborgen.

Nationale soevereiniteit en belangen bepalen de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten. Verwacht wordt dat, in tegenstelling tot andere gebieden van internationale samenwerking, het toezicht op de inlichtingen- en veiligheidsdiensten zal blijven gebeuren door nationale toezichtinstanties. Maar inlichtingen- en veiligheidsdiensten kunnen landsgrenzen overschrijden, toezichtinstanties kunnen dat niet. Bijgevolg beoordeelt het toezicht steeds slecht één kant van de gegevensuitwisseling. Bovendien is het voor toezichtinstanties grotendeels onmogelijk om hun beoordeling van een bepaalde gegevensuitwisseling met andere toezichtorganen te delen. Als gevolg van deze beperkingen voor nationaal toezicht bestaat het risico op een toezichthiaat met betrekking tot de internationale gegevensuitwisseling door inlichtingen- en veiligheidsdiensten. De vraag blijft hoe een dergelijk risico moet worden aangepakt.

Door kennis, ervaring en onderzoeksmethoden uit te wisselen en door hun bevindingen, conclusies en aanbevelingen te vergelijken, kunnen toezichtinstanties dichter bij elkaar komen. Onze ervaring is dat dit precies is wat dit gemeenschappelijke project heeft bereikt. We hebben van elkaars *best practices* geleerd, meer begrip ontwikkeld van elkaars juridische systemen en we hebben vertrouwen opgebouwd. Om ervoor te zorgen dat toezichtinstanties de ontwikkelingen in de internationale samenwerking tussen inlichtingen- en veiligheidsdiensten kunnen bijhouden, is het precies dat wat we moeten doen: intensiever samenwerken.

Een waardevolle en noodzakelijke stap naar een nauwere samenwerking is het verminderen van de geheimhouding bij het delen van informatie tussen toezichtinstanties. Op zijn minst zouden toezichthouders concrete bilaterale en multilaterale samenwerkingsverbanden moeten kunnen bespreken tussen de inlichtingen- en veiligheidsdiensten waarop ze toezicht uitoefenen. Een logische aanvullende stap zou kunnen zijn om met andere toezichtinstanties informatie te delen die door de inlichtingen- en veiligheidsdiensten zelf al is gedeeld. Zodra de gegevens zijn uitgewisseld, hoeft het toezicht niet achter te blijven. We suggereren niet dat alle nationale geheimhoudingsbeperkingen moeten worden afgeschaft, integendeel. Samenwerking tussen toezichtinstanties moet plaatsvinden binnen de grenzen en volgens de normen vastgesteld door de nationale wetgevers.

Het kunnen bespreken van internationale samenwerkingsverbanden en gegevensuitwisseling met andere toezichthouders brengt ook bepaalde verantwoordelijkheden mee. Voldoende bescherming van individuele rechten bij internationale samenwerking vereist niet alleen dat inlichtingen- en veiligheidsdiensten de normen die zij toepassen bespreken en streven naar een gelijk minimumniveau van bescherming door alle deelnemende diensten. Het vereist ook dat toezichtinstanties een dergelijk minimumniveau van gegevensbescherming handhaven en een gemeenschappelijke basis proberen te vinden bij het interpreteren van bestaande juridische waarborgen.

Wegens de technologische ontwikkeling en toegenomen samenwerking intensiveert de gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten, wat resulteert in een toename van het aantal afzonderlijke gegevensuitwisselingen. De enorme hoeveelheid uitgewisselde gegevens kan een uitdaging op zich worden. Het beoordelen van de legitimiteit en kwaliteit van elke individuele uitwisseling kan een overweldigende taak worden voor

de toezichtinstanties. Naast het uitvoeren van steekproefsgewijze controles, wordt het steeds belangrijker om het systeem en kader voor gegevensuitwisseling en het bestaan en functioneren van waarborgen voor de bescherming van grondrechten te beoordelen.

Om dit op effectieve wijze te kunnen doen, zullen toezichtinstanties nieuwe methoden moeten ontwikkelen. Eén van de mogelijke manieren is om in toenemende mate gebruik te maken van gecomputeriseerde automatisering en hulpmiddelen die zijn ontwikkeld voor het toezicht op grote hoeveelheden gegevens. Om dit te bereiken, moeten toezichthouders hun IT-expertise en kennis van de systemen van de diensten uitbreiden. Een andere manier om een effectiever toezicht mogelijk te maken, is rekening houden met de behoeften van de toezichtinstanties wanneer de diensten nieuwe systemen implementeren en de mechanismen voor interne en externe controle versterken.

De toezichthouders van België, Denemarken, Nederland, Noorwegen en Zwitserland zullen methoden en *best practices* blijven uitwisselen, internationale uitdagingen voor toezicht blijven bespreken en voortdurend zoeken naar de beste manieren om die uitdagingen aan te pakken. We nodigen toezichtinstanties van andere landen uit om ons te vervoegen bij onze inspanningen om het risico van een toezichthiaat te verkleinen en het toezicht op internationale gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten te verbeteren.

Ondertekend in Bern op 22 oktober 2018

Mr. Serge Lipszyc, Voorzitter van het Belgian Standing Intelligence Agencies Review Committee

Mr. Michael Kistrup, Voorzitter van de Danish Intelligence Oversight Board

Mr. Harm Brouwer, Voorzitter van het Dutch Review Committee on the Intelligence and Security Services

Mrs. Eldbjørg Løwer, Voorzitter van het EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee

Mr. Thomas Fritschi, Directeur van de Independent Oversight Authority for Intelligence Activities

RAPPORT D'ACTIVITÉS 2018
ACTIVITEITENVERSLAG 2018

Quis custodiet ipsos custodes ?

Quis custodiet ipsos custodes ? est une série de publications qui a pour objectif de stimuler une discussion approfondie sur le fonctionnement, les compétences et le contrôle des services de renseignements et de sécurité et sur le travail de renseignement. 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 renseignements et de sécurité, rue de Louvain 48, boîte 4 à 1000 Bruxelles (02 286 29 88).

Déjà parus dans cette série

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

RAPPORT D'ACTIVITÉS 2018

Comité permanent de Contrôle des services de renseignements et de sécurité

Comité permanent de Contrôle des services
de renseignements et de sécurité

intersentia
Antwerpen – Cambridge

Le présent *Rapport d'activités 2018* a été approuvé par le Comité permanent de Contrôle des services de renseignements et de sécurité lors de la réunion du 28 août 2019.

(*soussignés*)
Serge Lipszyc, président
Pieter-Alexander De Brock, conseiller
Laurent Van Doren, conseiller
Wouter De Ridder, greffier

Rapport d'activités 2018
Comité permanent de Contrôle des services de renseignements et de sécurité

ISBN 978-94-000-1107-6
D/2019/7849/144
NUR 823

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

ACC	Autorité de contrôle compétente
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
CEDH	Convention européenne des droits de l'homme
CHOD	*Chief of Defence*
CHODOPORDER	Ordre opérationnel du Chef de la Défense
CI	*Counterintelligence*
CIC	Code d'instruction criminelle
CNCTR	Commission nationale de contrôle des techniques de renseignement
CNS	Conseil national de sécurité
C.O.C.	Organe de contrôle de l'information policière
Comité permanent P	Comité permanent de contrôle des services de police
Comité permanent R	Comité permanent de contrôle des services de renseignement et de sécurité
Commission BIM	Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité
CP	Code pénal
CRABV	Compte Rendu Analytique – *Beknopt Verslag*
CRIV	Compte Rendu Intégral – *Integraal Verslag*
CSIL-R	Cellule de sécurité intégrale locale en matière de radicalisme, d'extrémisme et de terrorisme
CT	*Counterterrorism*
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten*
C-Ops	Centre des opérations
DCAF	*Geneva Centre for the Democratic Control of Armed Forces*
DG/DO	Direction des opérations de police administrative
DG EPI	Direction générale des Établissements pénitentiaires
DGJ/DJO	Direction des opérations de police judiciaire
Doc. parl.	Documents parlementaires de la Chambre et du Sénat
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
EI	État islamique
EION	*European Intelligence Oversight Network*
FragO	Ordres fragmentaires
FTF	*Foreign terrorist fighters*
HTF	*Homegrown terrorist fighters*
HUMINT	*Human intelligence*
ICP	*Intelligence collection plan*
ICT	*Information and communications technology*

IMINT	*Image intelligence*
IPCO	*Investigatory Powers Commissioner's Office*
IR	*Intelligence requirements*
ISTAR	*Intelligence, surveillance, target acquisition and reconnaissance*
JIB	*Joint Information Box*
KPI	*Key performance indicator*
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 sur la protection des données)
L.R&S	Loi du 30 novembre 1998 organique des services de renseignement et de sécurité
LTF	*Local task force*
M.B.	Moniteur belge
MoU	*Memorandum of Understanding*
MRD	Méthodes de recueil des données
NA	Note aux autorités
NTF	*National Task Force*
OCAM	Organe de coordination pour l'analyse de la menace
OE	Office des étrangers
ONU	Organisation des Nations Unies
OPSEC	*Operations security*
OSINT	*Open sources intelligence*
OTAN	Organisation du Traité de l'Atlantique Nord

PDR	Plan Directeur du Renseignement
PH	Propagandistes de haine
POC	*Point of contact*
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
RGPD	Règlement Général sur la Protection des Données
RIR	Rapport d'information
SGRS	Service Général du Renseignement et de la Sécurité
SIGINT	*Signals intelligence*
SLA	*Service Level Agreement*
SOP	*Standard Operating Procedures*
SPF	Service public fédéral
TESSOC	*Terrorisme, Espionage, Sabotage, Subversion and Organised Crime*
TF	*Terrorist fighters*
VSSE	Sûreté de l'État

PRÉFACE

Un secret a toujours la forme d'une oreille'
Jean Cocteau (Le Rappel à l'ordre)

De la lutte contre le terrorisme à la défense de nos intérêts stratégiques en matière de télécommunications, d'Edward Snowden à la présence d'espions en Belgique, de la reconnaissance de lieux de cultes à l'octroi d'habilitations de sécurité, la nécessité de services de renseignement performants est une préoccupation sociétale majeure.

À cet effet, l'État se doit d'assurer la sécurité tout en garantissant l'exercice des droits fondamentaux et des libertés individuelles. Cet exercice d'équilibre doit être réalisé grâce à l'intervention mesurée des services de renseignement, lesquels constituent un des rouages essentiels de l'arsenal de la sécurité.

Dans ce cadre, le rôle du Comité permanent R consiste non seulement à exercer ses propres missions mais également à veiller au développement contrôlé de la Sûreté de l'État et du Service général du Renseignement et de la Sécurité, ainsi que de l'Organe de coordination pour l'analyse de la menace, en collaboration avec le Comité permanent P.

Le Comité permanent R entend articuler son intervention sur plusieurs plans. Il se doit tout d'abord, comme il le fait depuis 25 ans, de formuler des recommandations qu'il adresse tant aux responsables qu'aux ministres compétents et au Parlement. Celles-ci participent de la volonté d'efficience du fonctionnement de l'État démocratique.

Le Comité permanent R suscite également les évolutions législatives. Il doit, par le biais de son expertise et son indépendance vis-à-vis des institutions, constituer une source de réflexion sur les enjeux de demain et l'architecture future du monde du renseignement.

Il se doit, en outre, d'être à la disposition des citoyens, tant à l'égard de ceux déposant plainte, estimant notamment que l'État a illégalement recueilli ou traité du renseignement à leur sujet, qu'à l'égard des justiciables s'adressant à l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité.

Le Comité permanent R entend rappeler que des centaines de femmes et d'hommes travaillent quotidiennement à la sécurité de l'État et que les enquêtes réalisées dans leurs services respectifs durant l'année 2018 attestent de leur engagement et de leur volonté d'être compétents, loyaux et intègres.

Le Comité développe son action de contrôle tant au niveau national qu'international, avec ses différents homologues afin de rencontrer la réalité du monde et de ses enjeux, notamment au regard du respect des données à caractère personnel. Dans ce contexte, force est de constater que tant les services étatiques que les sociétés privées recueillent du renseignement et sont soumis à des dispositions contraignantes en matière de sécurité de l'information. Par conséquent, le rôle du Comité permanent R ne devrait-il pas être redéfini ?

Il y a un an, je prêtais serment entre les mains du Président de la Chambre des représentants, en présence de mon prédécesseur, Guy Rapaille. Le Comité tient à souligner le travail de son président honoraire qui forme la base de notre travail actuel.

Avec les Conseillers du Comité, le Greffier et l'ensemble des collaborateurs, je souhaite ouvrir à mon tour le chemin et tracer la voie de l'organe de contrôle du renseignement belge. Aujourd'hui, avec cette équipe, j'entends sans relâche œuvrer à la définition de nouveaux objectifs, assurer l'accomplissement de nos missions et veiller au respect de nos valeurs démocratiques.

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

28 août 2019

CHAPITRE I
LES ENQUÊTES DE CONTRÔLE

En 2018, le Comité permanent R a finalisé cinq enquêtes de contrôle (I.1 à I.5), dont deux avaient été ouvertes à son initiative. Il a par ailleurs initié trois nouvelles enquêtes. Dans une enquête, le Comité a été saisi par le ministre de la Défense (art. 32 L. Contrôle)[1], tandis que deux enquêtes – dont une avec le Comité permanent P – ont été menées à la demande de la Commission parlementaire de suivi. Une description succincte des enquêtes en cours et/ou des enquêtes qui ont été lancées en 2018 figure au chapitre I.6. Les recommandations émises à l'issue des enquêtes de contrôle ont été regroupées au Chapitre XII.

Au total, le Comité permanent R a reçu 72 plaintes ou dénonciations en 2018. Depuis 2016, le processus de travail 'plaintes et dénonciations' fait l'objet d'un assouplissement, d'une 'déformalisation' et d'une standardisation.[2] Le cas échéant, après une brève pré-enquête et la vérification de plusieurs données objectives, le Comité a rejeté 68 plaintes ou dénonciations, soit parce qu'elles étaient manifestement non fondées (art. 34 L.Contrôle), soit parce que le Comité n'était pas compétent pour en traiter les griefs. Dans ces derniers cas, les plaignants ont été renvoyés, si possible, vers les instances compétentes (le Comité permanent P, la Police fédérale, le procureur du Roi ou d'autres instances). Une des plaintes a donné lieu à l'ouverture d'une enquête de contrôle (I.5), deux plaintes ont été ajoutées à une enquête en cours (I.1) et, compte tenu de la compétence conjointe, la plainte relative au fonctionnement de l'OCAM a été notifiée, fin 2018, au Comité permanent P en vue d'un traitement commun.

Outre les enquêtes de contrôle, le Comité permanent R a ouvert ce que l'on appelle des 'dossiers d'information'. Ceux-ci doivent permettre de répondre à des questions relatives au fonctionnement des services de renseignement et de

---

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

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).

l'OCAM.[3] Si ces dossiers font apparaître des indices de dysfonctionnement ou des aspects du fonctionnement des services de renseignement qui requièrent un examen approfondi, le Comité peut procéder, dans un second temps, à l'ouverture d'une enquête de contrôle formelle. Si toutefois il s'avère que ce genre d'enquête n'apporterait aucune plus-value au regard des finalités du Comité, aucune suite n'est donnée au dossier d'information. En 2017, un dossier d'information avait été ouvert, entre autres, sur le déploiement d'une capacité de renseignement du SGRS dans une zone de conflit, ce qui a donné lieu à l'ouverture d'une enquête de contrôle en 2018 (I.3).

Enfin, des briefings sont très régulièrement organisés. Des membres des services de renseignement y informent le Comité sur des thématiques actuelles et importantes pour la communauté du renseignement (p. ex. la *Belgian Passenger Information Unit* (BELPIU) ou encore la mise en œuvre des méthodes particulières de renseignement). Ces briefings doivent promouvoir une discussion approfondie sur le fonctionnement, les compétences et le contrôle des services de renseignement et de sécurité et de l'OCAM, ainsi que sur le travail de renseignement. Ils peuvent également donner lieu à l'ouverture d'une enquête.

I.1. LE FONCTIONNEMENT DE LA DIRECTION COUNTERINTELLIGENCE (CI) DU SGRS

I.1.1. CONTEXTUALISATION ET OBJET DE L'ENQUÊTE

En application de l'article 32 L.Contrôle, le ministre de la Défense a demandé au Comité permanent R, fin décembre 2016, d'effectuer une enquête sur le fonctionnement de la Direction Counterintelligence (CI), qui est une des quatre anciennes directions du SGRS. C'est un courrier envoyé mi-décembre 2016 par une part importante du personnel de CI qui est à l'origine de cette demande. Des préoccupations quant au fonctionnement du service et quant aux conditions dans lesquelles le personnel devait remplir ses missions légales, étaient exprimées dans ce courrier.

Le Comité permanent R a débuté son enquête de contrôle en janvier 2017[4] et l'a finalisée en février 2018. L'enquête a donné un aperçu de la gravité, de la

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

[4] 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').

complexité et de la diversité des manquements observés au sein de la Direction CI. Le Comité avait posé comme postulat que la sécurité nationale requérait 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.

I.1.2. LA MISSION (LÉGALE) DE LA DIRECTION CI

I.1.2.1. Ambitions, mission et vision en matière de 'counterintelligence'

Dans un document interne de 2012, l'ambition de ce qui était encore la 'Division' CI était décrite comme suit : '*Teneinde elke bedreiging te voorkomen moet de Div CI instaan voor de identificatie, de preventie en neutralisatie van al de activiteiten die kunnen ontplooid worden door buitenlandse inlichtingendiensten, door andere organisaties of door individuele personen in het kader van terrorisme, spionage, sabotage of subversie (TESS) en die de belangen van Defensie in de ruimste zin van het woord, hetzij haar personeel, haar infrastructuur, haar plannen en operaties worldwide ; of deze van haar militaire partners in België zou kunnen bedreigen*'.[5]

Dans le même document, figurait également la vision : '*Be able to prevent all threats to all Defence related matters*'. '*De Divisie CI moet in staat zijn elke realistische bedreiging waaraan de vitale belangen van Defensie kan aan blootgesteld worden, te voorkomen. De werking van de Div CI moet in alle DISCRETIE kunnen gebeuren. Dit betreft de kennis van de structuur, de modus operandi, het personeel en de middelen. Het uitvoeren van de operaties en van de opdrachten moet AFGESCHERMD gebeuren*'.[6]

Cette ambition et cette vision ont été traduites en objectifs stratégiques dans le 'Plan Directeur du renseignement de Sécurité et d'Actions Sécuritaires 2015-2018'[7] : '*Le Dept CI doit être en mesure de prévenir de manière réaliste chaque menace pouvant exposer des intérêts vitaux de la Défense, et ce, dans le cadre des*

---

5 *'Afin de prévenir toute menace, la Div CI doit se porter garante de l'identification, de la prévention et de la neutralisation de toutes les activités susceptibles d'être déployées par des services de renseignement étrangers, par d'autres organisations et par des individus dans le cadre du terrorisme, de l'espionnage, du sabotage ou de la subversion (TESS), et susceptibles de menacer les intérêts de la Défense dans le sens le plus large du terme, que ce soit son personnel, son infrastructure, ses plans et ses opérations aux quatre coins du monde ; ou ceux de ses partenaires militaires'.* (traduction libre).

6 *'Être en mesure de prévenir toutes les menaces pouvant exposer tous les domaines liés à la Défense. La Division CI doit être en mesure de prévenir de manière réaliste toute menace pouvant exposer les intérêts vitaux de la Défense. La Division CI doit pouvoir fonctionner en toute DISCRÉTION, qu'il s'agisse de la connaissance, de la structure, des modes opératoires, du personnel et des moyens. L'exécution des opérations et des missions doit être PROTEGÉE.'* (traduction libre).

7 SGRS, Plan Directeur du renseignement de Sécurité et d'Actions Sécuritaires 2015-2018. Révision 2016 – Veiligheidsinlichtingen Stuur- en Veiligheid Actieplan 2015-2018. Herziening

missions et des moyens prévus par les textes légaux. En outre, le Dept CI doit être en mesure de pouvoir honorer les engagements et les accords en vigueur conclus avec des services homologues, et plus particulièrement dans le cadre d'une coopération avec les services de renseignement, avec les services de police et avec la Justice. Le Dept CI doit également être en mesure de porter assistance à ses partenaires militaires étrangers localisés sur le territoire belge dans le domaine de la contre-ingérence'. Cinq priorités ont par ailleurs été définies dans ce même Plan Directeur du renseignement de Sécurité et d'Actions Sécuritaires 2015-2018.

Cette ambition, cette mission et cette vision découlent de la réglementation de l'OTAN et de la législation belge.

I.1.2.2. La réglementation de l'OTAN

En 2014, l'OTAN a défini de manière univoque les notions utilisées dans le cadre de son fonctionnement dans un *standardization agreement* (STANAG).[8] Le contre-espionnage (*counterintelligence*) est défini comme suit :

- *'Counter Intelligence (CI organizations, military or civilian, of the member nations including Law Enforcement Organizations) of the Alliance are responsible for counteracting the threat to security posed by hostile intelligence services and subversive, criminal or terrorist groups or individuals'.*
- *Counter-intelligence includes those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organisations or by individuals engaged in espionage, sabotage, subversion or terrorism. […] (2) The main thrust of the CI effort is to protect personnel, information, plans and resources, both at home and when deployed. It aims to provide knowledge and understanding of the prevailing situation to keep privileged information secret, equipment secure and personnel safe. CI should be proactive and preventative in its approach. (3) CI is an intelligence function that provides commanders at all levels with a detailed understanding of threats, vulnerabilities and risks to enable them to make well-educated decisions on security measures. In reality, there are likely to be compromises between what is needed and what is feasible.*[9]

2016, SECRET (Loi 11 décembre 1998), March 1, 2016, 11. Il s'agit d'une 'révision' du plan établi en 2016. Le service a déclassifié ce passage.

8 NATO Standardization Office (NSO), STANAG 2190. Allied Joint Doctrine for intelligence, counter-intelligence and security, Edition 2, September 2014 (NSO(JOINT)1165(2014) JINT/2190, 7-2.

9 *Le contre-espionnage (organisations CI militaires ou civiles des États membres, en ce compris les organismes chargés de l'application de la législation) de l'Alliance a pour mission de contrer la menace qui pèse sur la sécurité et qui émane de services de renseignement ennemis et de groupes ou d'individus subversifs, criminels ou terroristes'.*
Les activités qui relèvent du contre-espionnage consistent à identifier et à lutter contre la menace qui pèse sur la sécurité et qui émane de services de renseignement ennemis ou d'organisations ou de personnes impliquées dans des activités d'espionnage, de sabotage, de

Ce même document de l'OTAN revient sur le rôle spécifique du contre-espionnage : '*to ensure successful military operations the commandor should deny the adversary the opportunity to conduct terrorism, espionage, subversion, sabotage, organized crime or computer network attacks against friendly force. To achieve this requires identification of friendly force's vulnerability to an adversary's intelligence gathering operations. This information is used to inform OPSEC, counter surveillance and deception planning including Protective Security Policy*'.[10]

Deux autres documents, datant respectivement de 2001 et 2016[11] décrivent la mission des Divisions CI au sein des services de renseignement militaires nationaux. Leur mission est de détecter et de contrer l'espionnage, le sabotage ainsi que les menaces de terrorisme et de subversion à l'encontre de l'OTAN et des forces de la coalition. Pour certaines nations, s'y ajoutent la protection contre les menaces provenant du crime organisé, du fondamentalisme, de l'extrémisme et des opérations de renseignement (de pays étrangers).

I.1.2.3. La législation belge

Si la Loi du 30 novembre 1998 ne mentionne pas explicitement le contre-espionnage, plusieurs missions visées à l'article 11 L.R&S peuvent néanmoins être comprises comme des missions qui s'apparentent à du contre-espionnage. L'A.R. du 21 décembre 2001[12], qui détermine la structure générale du Ministère de la Défense et fixe les compétences de certaines autorités, ne définit pas non plus la notion de contre-espionnage et ne fait pas mention d'une Direction

---

subversion ou de terrorisme. […] (2) Les efforts déployés par CI visent essentiellement la protection du personnel, des informations, des plans et des ressources, tant au niveau national que lors d'un déploiement à l'étranger. L'objectif est de connaître et de comprendre la situation existante afin de garder secrètes des informations privilégiées, de sécuriser l'équipement et de garantir la sécurité du personnel. CI devrait adopter une approche proactive et préventive. (3) CI assure une fonction de renseignement qui fournit à tous les niveaux de commandement une vision détaillée des menaces, des vulnérabilités, et des risques, et ce pour leur permettre de prendre des décisions éclairées sur les mesures de sécurité. En réalité, des compromis doivent probablement être trouvés entre ce qui est nécessaire et ce qui est faisable. (traduction libre).

10 *'En vue de garantir la réussite d'une opération militaire, le commandant doit refuser à l'adversaire la possibilité de commettre des attaques terroristes, de mener des activités d'espionnage, de subversion, de sabotage, de crime organisé ou de mener des attaques informatiques contre des alliés. Pour ce faire, il convient d'identifier les vulnérabilités des forces armées amies face aux opérations de recueil de renseignements d'un adversaire. Ces informations sont utilisées pour informer l'OPSEC, pour la contre-surveillance, pour planifier l'imposture, y compris la Protective security Policy.* (traduction libre).

11 Il s'agit de l''Allied Joint doctrine for Intelligence, Counterintelligence and Security (AJP 2(A) (février 2016)' et de l''AJP 2.2 '(Restricted) Counter-intelligence and Security Procedures' (novembre 2001) de l'OTAN.

12 A.R. du 21 décembre 2001 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités, *M.B.* 12 janvier 2002. Cet A.R. a été remplacé par l'A.R. du 2 décembre 2018, qui ne définit pas la notion de contre-espionnage, pas plus qu'il ne fait mention d'une Direction Counterintelligence.

Counterintelligence. Il en va de même pour l'A.R. du 4 juillet 2014 qui fixe le statut de certains agents civils du SGRS.[13]

I.1.3. LES MISSIONS DE CI DANS LA PRATIQUE

I.1.3.1. CI en Belgique et à l'étranger

La Direction CI se concentrait à l'origine sur la détection d'activités d'espionnage militaire – tant des membres de l'armée belge elle-même que des services étrangers – et sur la contre-subversion en Belgique. La définition du contre-espionnage dans les milieux militaires a été progressivement élargie et comprend, outre la subversion, ce que l'on appelle le 'TESSOC' : 'Terrorisme, Espionage, Sabotage, Subversion, Organised Crime'. La Direction CI a aussi pour mission de détecter les phénomènes TESSOC au sein de son propre service (SGRS). Ce n'est pas illogique puisque le service de renseignement militaire peut constituer une cible de choix (en termes d'infiltration) pour les services de renseignement étrangers.

Compte tenu du déploiement plus fréquent des troupes belges à l'étranger et dans le cadre de la coopération OTAN, la Direction s'est également vu confier, à partir de 2012, ce que l'on appelle la mission 'CI en OpsZone'. Il s'agit de l'envoi de personnel CI à l'étranger en appui aux troupes belges qui y sont déployées afin de contrer l'espionnage militaire local ou des formes de crime organisé (prostitution, drogues, etc.) pouvant donner lieu à une infiltration ou à la subversion d'un militaire. Cette mission, communément dénommée *force protection*, trouve, elle aussi, sa base légale dans l'article 11 L.R&S.

I.1.3.2. Le contre-terrorisme et la compétence du SGRS

Le Comité permanent R avait déjà souligné dans des enquêtes de contrôle précédentes la profonde influence de la montée du terrorisme (islamiste) sur le fonctionnement des services de renseignement belges, en l'espèce le SGRS et la Direction CI. Les caractéristiques changeantes du terrorisme (davantage de filières et d'activités transfrontalières, etc.) ont donné lieu à un mélange de tâches et de responsabilités au sein du SGRS, que ce soit en ce qui concerne la territorialité (Belgique *versus* étranger) ou en ce qui concerne les aspects devant faire l'objet d'un suivi (civil *versus* militaire). Dans ce cadre, le Comité permanent R préconisait une évaluation approfondie de la manière dont le service de renseignement en général, et la Direction CI en particulier, ont été dirigés dans une certaine direction.[14]

---

13 A.R. du 4 juillet 2014 fixant le statut de certains agents civils du département d'état-major renseignement et sécurité des forces armées, *M.B.* 18 juillet 2014.

14 Le SGRS doit conserver sa spécificité et donc se concentrer sur l'aspect militaire. Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2016*, 4 et suiv. ('II.1. La problématique des *foreign terrorist fighters*').

Le fait que des terroristes, guidés par une logique militaire (des cellules en Europe étaient dirigées par le commandement militaire de l'EI depuis la Syrie/l'Irak), allaient entrer en action avec des moyens militaires lourds[15], et surtout les attentats de mars 2016 à Bruxelles et Zaventem, ont d'autant plus renforcé cette évolution (le mélange des tâches). Cette période a constitué un moment clé pour le SGRS (et la Direction CI). La compétence propre au service, qui était jusque-là 'militaire', a progressivement fait l'objet d'une interprétation plus large (lisez : civile).

Pour autant, dans une période nécessitant une collaboration maximale de chaque service, la direction n'a pas pu vérifier concrètement si le SGRS – et en particulier la Direction CI – s'était véritablement senti concerné et, le cas échéant, s'il avait pu offrir une valeur ajoutée claire avec les moyens à sa disposition.

Cette situation a été à l'origine de toute une série de problèmes ces dernières années, notamment la réduction des moyens, le morcellement des compétences et au sein du service, ou le fait de ne pas endosser certaines tâches ou compétences, l'assistance technique dans des dossiers judiciaires avec une plus-value limitée.

En outre, la Direction CI définissait son rôle en s'appuyant toujours sur les règles de l'OTAN. Selon ces règles, la lutte contre le terrorisme se concentre sur le terrorisme qui vise des cibles militaires, principalement dans un contexte international (p. ex. des théâtres d'opérations à l'étranger). Le terrorisme qui ne vise que des cibles principalement civiles et qui sévissait surtout, historiquement, sur le territoire national (p. ex. CCC, RAF), ne relevait pas, en principe, du domaine des instances militaires, mais bien de celui du service de renseignement civil (VSSE).

Le Comité a dès lors estimé que la mission en matière de contre-terrorisme devait impérativement être clarifiée. Le SGRS (et en particulier la Direction CI) devait déterminer explicitement, dans le cadre des orientations politiques existantes, 'jusqu'où va le militaire', où commence le purement 'civil' et comment les deux sont liés.

Le Comité a recommandé que tant en interne (au sein du SGRS, de la Direction CI, mais aussi à l'égard de la Direction I) que vis-à-vis de l'extérieur (en collaboration avec la VSSE, le Parquet, l'OCAM, etc.), le SGRS et la Direction CI élaborent une position claire sur ce que l'on peut et doit attendre du service ainsi que sur son ambition, en prenant en considération les moyens disponibles. Une fois que cette vision, cette ambition et cette stratégie auront été élaborées, il conviendra de s'y tenir pour que le service soit perçu comme un partenaire qui compte dans l'anti-terrorisme belge.

---

15 Le fait que les terroristes qui se trouvaient en Europe disposaient d'armes 'militaires' constituait une indication supplémentaire expliquant la compétence du SGRS. En effet, l'article 11 § 2, 1° L.R&S limite la compétence du SGRS aux activités qui menacent le territoire national ou la population *'par des moyens de nature militaire'*.

I.1.4. LA DIRECTION COUNTER-INTELLIGENCE AU SEIN DU SGRS

La direction du SGRS est exercée par le Commandement (SGRS/C), qui peut disposer d'un staff et d'un secrétariat. Avant 2013, le SGRS – où se côtoient des militaires *et* des civils – était composé de quatre divisions : A(ppui), C(ounter) I(ntelligence), S(ecurity) et I(ntelligence). En 2013, CI et S ont fusionné. Peu après, la Direction A a été supprimée. En 2017, une nouvelle réorganisation a été mise en place. 'Les 'Divisions' sont devenues des 'Directions'. La Direction S(ecurity) et la Direction C(ounter)I(ntelligence), qui ciblent le territoire national, ont de nouveau été dédoublées. À côté de la Direction I(ntelligence), qui est plutôt axée sur l'étranger, une nouvelle Direction Cyber a été créée.

Le Comité a cependant constaté qu'il n'existait pas d'organigramme uniforme/unique de la Direction CI. En effet, plusieurs versions utilisant différentes terminologies (directions, bureaux, sections, piliers, etc.) étaient en circulation. Il était donc impossible pour les membres du personnel d'avoir une vision claire de leur organisation ou de qui précisément est responsable de quoi.

I.1.5. LES CONSTATATIONS DE L'ENQUÊTE

I.1.5.1. L'opposition (supposée) entre 'SGRS' et 'ACOS IS'

Le Comité a dû une nouvelle fois constater que le plus grand flou régnait autour du contenu et de l'utilisation des dénominations 'SGRS' et 'ACOS-IS'.[16] La plupart des membres du personnel de la Direction CI – en ce compris des dirigeants –estimaient que leur direction constituait en fait 'le SGRS', tandis que les autres directions (surtout la Direction CI) constituaient 'ACOS/IS'. Ils considéraient en outre que la Direction CI devait être un service indépendant de la structure de la Défense, et ce en l'absence de toute base légale ou réglementaire.

De nombreuses incertitudes et discussions sur la mission de la Direction CI résultent du fait que dans la réglementation, il est question à la fois du Service Général du Renseignement et de la Sécurité (SGRS) et du Département d'état-major Renseignement et Sécurité (ACOS-IS). Les missions du SGRS sont définies dans la L.R&S (à savoir l'art. 10) et le service relève directement du ministre de la Défense (art. 2 L.R&S). ACOS-IS était mentionné dans l'A.R. 21 décembre 2001 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités.[17] En vertu de cet arrêté, ce service doit

16 ACOS-IS est l'acronyme d' 'Assistant Chief of Staff Intelligence and Security'.

17 Cet arrêté royal a été remplacé par l'A.R. du 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attritions de certaines autorités, *M.B.* 18 janvier 2019. Cet arrêté n'a pas eu d'impact dans le cadre de la présente enquête.

appuyer les opérations de la Défense (art. 22-24 AR) et est placé sous la direction du sous-chef d'état-major renseignement et sécurité, qui est lui-même placé sous la tutelle du CHOD (Chief of Defense). Toujours selon l'arrêté, le sous-chef d'état-major et le chef du SGRS sont une seule et même personne. Certes, le chef du SGRS relève directement du ministre et les missions du SGRS sont plus larges que celles qui étaient définies dans la L.R&S. Le Comité attendait de la direction du SGRS et de la Direction CI qu'elles dissipent cette confusion une fois pour toutes.

I.1.5.2. Polarisation entre les civils et les militaires

Le Comité permanent R a pu constater que les collaborateurs de CI estiment que la Direction CI occupe une 'place particulière' au sein du SGRS (ACOS/IS) (*infra*) et qu'elle a développé sa propre culture. Compte tenu de la nature de ses missions, CI doit souvent mener des enquêtes impliquant également des collaborateurs de la Défense (essentiellement des militaires), et la direction en tant que telle est perçue comme un organe de contrôle. C'est la raison pour laquelle le personnel de CI avait l'impression de susciter la méfiance des autres directions du SGRS et d'autres composantes de la Défense. Il avait aussi le sentiment que d'autres entités ne comprenaient pas le rôle de CI.

Cette méfiance, l'absence de compréhension mutuelle ainsi que le flux d'informations défaillant entre les Direction CI et I ont notamment généré des conflits et diminué les possibilités de coopération.[18] De plus, l'esprit de corps très présent parmi les militaires donnait souvent l'impression de faire courir le risque de voir les enquêtes CI 'tuées dans l'œuf'. Le Comité permanent R estimait que ce risque n'était pas irréel. Il se basait à cet égard sur une série d'incidents survenus dans des dossiers très délicats, dans lesquels des services n'avaient pas toujours communiqué certaines données ou signalé des comportements de membres du SGRS à CI. Mais l'inverse était vrai également : la Direction CI ne communiquait pas certaines informations à la chaîne de commandement, en ce sens que même le chef du SGRS n'était parfois pas au courant.

Le Comité considérait que CI s'isolait trop du reste du SGRS. Cette direction aurait une propension excessive à ne pas partager certaines informations pourtant nécessaires au bon fonctionnement du SGRS. Signe révélateur : une partie du personnel de la Direction CI préférerait la voir fonctionner en dehors du SGRS. Aux yeux du Comité, cette position risquait de voir la Direction CI appliquer des normes et des règles différentes de celles appliquées par d'autres unités du SGRS, ce qui hypothèquerait la coordination des différentes activités de renseignement.

---

18 Le Comité permanent R l'avait signalé il y a longtemps déjà, voir COMITÉ PERMANENT R, *Rapport d'activités 2010*, 41 ('II.10. Gestion de l'information au sein du service de renseignement militaire').

I.1.5.3. Direction, orientation et planification

Comme en 2013[19], le Comité a constaté que les collaborateurs de CI n'avaient pas toujours connaissance de leurs objectifs précis en matière de renseignements. En l'absence de plusieurs documents d'orientation pourtant essentiels, l'incertitude régnait au sein de la Direction CI et sur le terrain quant aux attributions de cette direction. Les relations entre CI et d'autres directions était plutôt problématiques, faute de consensus sur les missions exactes à remplir.

I.1.5.4. Organisation et structure

La Direction CI ne disposait pas d'un organigramme uniforme/unique officiellement reconnu, le tableau organique ne correspondait pas à l'affectation réelle, et plusieurs membres du personnel accomplissaient des tâches qui ne correspondaient pas à leur fonction. Certains postes n'étaient même pas pourvus, et l'appui logistique faisait défaut.

I.1.5.5. La nature des produits

Le fonctionnement des différentes sections et des différents bureaux de CI était orienté vers le travail de renseignement opérationnel.[20] On y opérait de manière réactive et *ad hoc* autour de dossiers concrets. De plus, peu de produits de renseignement (voire aucun) étaient fournis au niveau stratégique. Selon le Comité, une redéfinition de la relation entre la collecte et l'analyse (éventuellement couplée à une restructuration au sein de la Direction CI et/ou plus à plus grande échelle) s'imposait.

I.1.5.6. Les détachements provinciaux

Les détachements provinciaux – les antennes locales de la Direction CI – sont chargés de collecter des informations (notamment via le HUMINT), de représenter le SGRS au niveau local ainsi que d'entretenir des relations avec, d'une part, les autorités et les institutions locales et, d'autre part, les unités locales de la Défense. Le Comité permanent R a notamment observé un manque de communication et de feedback de la part des services basés au quartier

---

19 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 20 ('II.1.3.3.5. Un manque de clarté sur la nature des renseignements à recueillir'). Le Comité recommandait que *'le SGRS définisse les liens qui doivent être établis entre les renseignements opérationnels, tactiques et stratégiques et les missions légales décrites dans la L.R&S'*, (*Ibid.*, 113).

20 L'analyse opérationnelle génère des renseignements qui sont utilisables, c'est-à-dire qui sont immédiatement applicables dans des dossiers concrets. Les renseignements opérationnels sont généralement à usage interne et ont une valeur tactique. Ils contribuent à la réalisation des objectifs à court terme.

général, des problèmes d'accès direct à la banque de données de CI, un sous-effectif et un manque d'appui. En outre, une confusion régnait quant au rapport et à l'interaction (coordination et répartition des tâches) entre les détachements provinciaux et le Détachement national. En effet, les deux fonctionnaient indépendamment l'un de l'autre. Enfin, il n'y avait pas non plus de concertation entre les détachements provinciaux ni entre ceux-ci et le Département national.

I.1.5.7. CI en Ops-zone

La section CI en Ops-zone est une section particulière de la Direction CI.[21]

À l'origine, le SGRS déployait des équipes mixtes (I/CI) en appui des opérations : du personnel de la Division I collaborait avec du personnel de la Division CI. Des problèmes d'effectifs n'ont plus permis à la Direction CI d'honorer les déploiements. La section I/Ops a alors repris le flambeau et a couvert les aspects de *force protection* en appui des troupes déployées. En 2012/2013, la Direction CI a émis de nouveau le souhait de déployer des éléments en zones d'opération. Ces membres du personnel n'étaient pas intégrés dans la structure de l'I/Ops en zone, de sorte qu'ils ne pouvaient être assimilés à ce détachement. Cependant, le cadre de la Direction CI ne permettait pas, à ce moment-là, la mise à disposition permanente de personnel dédié à cette mission particulière. Avec le temps, deux officiers ont pu être libérés en vue d'intégrer cette cellule de manière permanente.

Le Comité a constaté que la structure bicéphale en opération était une source de tensions entre les deux directions.

I.1.5.8. Processus et méthodes : SOP, mesure de la charge de travail, KPI et feedback interne

Le Comité a dû constater que les *Standing Operating Procedures* (SOP)[22] qui s'appliquaient à CI ne formaient pas un ensemble cohérent et n'étaient pas actualisées ; elles ne tenaient pas compte des modifications de la structure de CI ni des modifications en termes de missions légales. Selon CI, cette situation était due à un manque de personnel.

De plus, le Comité permanent R a observé que la charge de travail au sein de la Direction CI n'était mesurée, analysée, gérée ou évaluée nulle part. La charge de travail n'était pas non plus objectivable faute de définition de priorités,

---

21 L'OTAN a élaboré des directives au déploiement de ces cellules nationales de renseignement (BENIC). Ces directives préconisent que ces cellules intègrent, si possible, des éléments CI nationaux.

22 Une *'standing (standard) operating procedure' (SOP)* est définie comme suit : *'a set of instructions covering those features of operations which lend themselves to a definite or standardized procedure without the loss of effectiveness. The procedure is applicable unless ordered otherwise'* (NATO Glossary Terms and Definitions, AAP-6(V)).

d'objectifs clairement établis, de structure de la Direction CI, de descriptions de fonctions, (de connaissance) de(s) procédures, d'indicateurs de gestion et d'un *benchmark,* qui est un point de référence servant à effectuer une mesure, c'est-à-dire un étalonnage permettant de mesurer diverses performances. Le Comité a constaté un manque d'investissement de la part du Commandement du SGRS et de la Direction CI en la matière.

En outre, CI n'avait pas élaboré de *key performance indicators* (KPI).[23] En revanche, des critères d'analyse étaient définis. Il ne s'agissait quasi exclusivement que de critères qualitatifs et non quantitatifs.

Par ailleurs, le Comité a pu constater que des problèmes se posaient en matière de gestion de la communication interne.

I.1.5.9. Processus et méthodes : la maîtrise du tradecraft

Le travail de renseignement requiert une maîtrise du *tradecraft*.[24] Cette notion comprend 'les méthodes, techniques, technologies, procédures et principes de base mis au point et utilisés par les services de renseignement afin de mener à bien leurs missions et leurs opérations'.[25]

Le Comité a eu connaissance d'exemples traduisant un manque de partage des connaissances, de compréhension et de mise en pratique commune du *tradecraft*. Le Comité a constaté à cet égard l'existence d'un conflit entre la manière dont le *tradecraft* était considéré du point de vue de CI et l'approche de ce concept, par exemple, dans le cadre du contre-terrorisme (CT) : la culture du *need to know* se heurtait à celle du *need to share*.

I.1.5.10. Gestion du personnel

Statuts différents et diminution du nombre d'effectifs

Plus de la moitié du personnel de CI est constituée de civils. On distingue quatre groupes distincts dans cette catégorie : les 'Commissaires et Inspecteurs'

---

23 Un indicateur de performance est un indicateur d'efficience ou de résultat (efficacité) qui est un instrument de mesure en appui à la décision. Un KPI oriente une démarche de progrès. Il peut être collectif ou personnel et est nécessairement en phase avec la stratégie choisie. Il est utilisé dans la présentation de tableaux de bord de gestion.

24 Ces règles sont rarement formalisées, mais n'en sont pas moins très importantes pour maintenir les liens de confiance entre les services de renseignement qui collaborent.

25 Par exemple, le besoin d'en connaître ou *need to know*, la règle du tiers service, le respect de la classification, la surveillance et la contre-surveillance, les légendes ou *cover stories*, la sécurité opérationnelle, la gestion et la protection des sources humaines, les MRD, l'utilisation de la cryptographie. Par *tradecraft*, on entend également l'acceptation de plusieurs principes/concepts tels que le cycle du renseignement. Il convient toutefois de veiller à ce que ces 'normes techniques' demeurent conformes aux normes légales, réglementaires, et que ce *tradecraft* soit suffisamment documenté et, si nécessaire, différencié.

statutaires et ceux qui ont une carrière particulière, qui diffère de celle des agents de l'État classiques (statut A.R. du 4 juillet 2014[26]), les 'Commissaires analystes' statutaires, ayant également une carrière particulière (cf. le même A.R. du 4 juillet 2014), les agents de l'État statutaires relevant du statut Camu (A.R. du 2 octobre 1937) et les agents contractuels, ayant la plupart un contrat de travail à durée indéterminée (loi relative aux contrats de travail de 1978). La carrière des membres du personnel relevant du Statut du 4 juillet 2014 est étroitement liée au SGRS, qui est leur seul lieu d'affectation possible, alors que les agents de l'État du statut Camu et les contractuels peuvent, en principe, être également affectés dans d'autres unités de la Défense.

La Direction CI dispose de moins de personnel que dans les années 80. Or, d'autres services tels que la VSSE, la police et l'OCAM ont entre-temps été renforcés.[27] Même la vague de recrutements prévue (*infra*) ne permettrait de retrouver que le niveau des effectifs de départ. Compte tenu de la désillusion et du découragement qui gagnait le personnel, les dirigeants de CI estimaient que la continuité du service pouvait être mise en péril. Le Commandement a reconnu l'existence de ces problèmes, qu'il expliquait par le gel des recrutements dans la fonction publique fédérale entre 1988 et 2009.

En ce qui concerne les différents aspects de la problématique du personnel, le SGRS dépend de la DGHR, à l'instar de toutes les autres entités de la Défense. La marge de manœuvre du service de renseignement militaire s'en trouve très limitée.

Les fonctions et les tâches des civils endossées par des militaires : un problème ?

Si la Direction CI était au départ composée majoritairement de civils, ce n'est plus le cas depuis longtemps déjà. Historiquement, la création d'une composante 'civile' au sein du service de renseignement militaire avait pour objectif de pouvoir recourir à un 'corps' civil et indépendant de l'appareil militaire pour contrer les menaces potentielles au sein même de cet appareil militaire (surtout l'espionnage, mais aussi la subversion et l'extrémisme). Le personnel civil estime être le seul à même de garantir l'indépendance nécessaire à l'égard de la hiérarchie militaire. Le Comité ne partageait pas cet avis, l'indépendance n'étant pas nécessairement liée au statut du personnel (civils ou militaires) mais bien à l'état d'esprit des personnes, aux structures et aux procédures. Le gel des recrutement instauré en 1988 explique également l'intégration progressive de

26 Arrêté royal du 4 juillet 2014 fixant le statut de certains agents civils du département d'état-major renseignement et sécurité des forces armées, *M.B.* du 18 juillet 2014. L'A.R. éponyme datant du 7 juillet 2003 a été abrogé.

27 Le plan stratégique du ministre de la Défense du 29 juin 2016 prévoyait que le SGRS dans son ensemble verrait ses effectifs croître d'environ un tiers à l'horizon 2030. Le SGRS a émis des doutes quant à la réalisation de cet objectif, vu que la diminution des effectifs à la Défense (25.000 unités en 2020) est plus rapide que prévu.

militaires au sein de la Direction CI. D'un point de vue légal, rien ne s'y oppose. Ce 'mix' était considéré comme une plus-value au sein de CI.

Il est vrai que l'affectation du personnel militaire n'est pas exempte de difficultés : le Comité avait déjà constaté, lors de l'Audit 2011, que la rotation rapide des militaires posait des défis majeurs en termes d'accueil, de formation et de gestion des connaissances. Mais l'affectation de militaires comporte aussi des avantages (transfert des meilleures pratiques, idées novatrices, etc.). Le Comité était néanmoins conscient que l'intervention de militaires dans une mission de CI n'allait pas de soi.

Un autre aspect important portait sur la reconnaissance et la valorisation du personnel civil. Nombreux étaient les civils à se sentir sous-estimés. L'Audit 2011 avait déjà montré que de toutes les catégories de personnel, c'était chez les commissaires (niveau A de CI) que ce ressenti était le plus fort. Dans cet audit, le Comité affirmait qu'il était donc préférable '*de ne pas penser en termes de 'groupes du personnel' (militaires et civils, contractuels et statutaires, niveau X et niveau Y, etc.), mais plutôt en termes de 'fonctions*".[28] En l'absence de résultats, le Comité a estimé que des mesures structurelles plus fortes s'imposaient. Une restructuration complète du SGRS devait pouvoir être envisagée, mais sans perdre de vue la spécificité des différentes missions.

La problématique du personnel contractuel

La Direction CI compte dans ses rangs un nombre limité d'analystes contractuels qui sont entrés en service il y a très longtemps. Leurs perspectives de carrière et leur rémunération sont les moins attrayantes. Le Commandement a reconnu l'existence de la problématique et a indiqué s'être efforcé, en 2016 et 2017, d'améliorer leur statut. Le Commandement a également fait référence aux initiatives prises en la matière par le ministre de la Fonction publique.

Les descriptions de fonction et le contenu du travail

Les problèmes identifiés par le Comité ont souvent à voir avec un manque de procédure, un manque de précision sur qui fait quoi et qui porte quelle responsabilité. Malgré les recommandations du Comité dans l'Audit 2011, force a été de constater que de nombreuses descriptions de fonction faisaient encore défaut ou n'étaient pas suffisamment transparentes.

D'autre part, de nombreux membres du personnel se disaient très satisfaits du contenu de leur travail, qualifié de 'varié, aventureux et palpitant'. Ils disposaient d'une large autonomie et évoluaient dans une ambiance collégiale.

28 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 11.

Le recrutement, la sélection, la mobilité et les départs

Le SGRS, et donc aussi la Direction CI, fait intégralement partie des Forces armées. Il ne jouit d'aucune autonomie en matière de gestion du personnel, que ce soit en matière de recrutement, de formation ou autre. En matière de recrutement, la Direction CI dépend donc dans une large mesure de la DGHR (pour le recrutement du personnel militaire) et du SELOR (pour le recrutement des civils). Selon le Comité, le SGRS porte une part de responsabilité dans le processus : il doit en effet soumettre des descriptions bien définies pour permettre de mieux cibler les recrutements.

Un autre problème réside dans la rotation des militaires. Dans le cadre du plan de carrière des officiers au sein de la Défense, la règle veut qu'ils soient affectés à différentes unités au cours de leur carrière ; les officiers doivent rester dans une même unité pendant trois ans, et les sous-officiers, pendant cinq ans.[29] Cette situation était parfois considérée comme problématique, étant donné que les militaires issus d'une autre unité ne pouvaient pas toujours être affectés de manière efficace et efficiente au SGRS compte tenu de la spécificité d'un service de renseignement et du travail de renseignement. Il n'en reste pas moins que ce système permet d'insuffler des idées novatrices.

Le personnel civil peut changer de direction, mais il ne le fait pas souvent. Un départ de contractuels a bien été constaté vers la Police fédérale, la Justice et la VSSE, qui leur offraient une stabilité professionnelle.

Formation, entraînement et gestion des connaissances

Les civils entrent comme inspecteur ou comme commissaire et, dès leur recrutement, sont destinés à développer une carrière dans le renseignement. Ils sont d'ailleurs sélectionnés et formés à cette fin. En revanche, les militaires qui sont mutés au SGRS y arrivent souvent sans connaissances spécifiques, ce qui constitue un problème de taille.

Au sein du SGRS, une cellule est chargée de la formation. Sa tâche consiste principalement à organiser et à suivre le parcours professionnel des membres du personnel.

Un *Basic Inspector Counter Intelligence Course 2018-2019* a été élaboré pour la formation des nouveaux membres du personnel. Les candidats doivent suivre des modules avant d'effectuer un stage d'un an.

[29] Il existe toutefois des exceptions.

Malgré de précédentes recommandations[30], le Comité a une nouvelle fois constaté l'absence de gestion formelle des connaissances au sein de CI.[31] En outre, beaucoup de connaissances étaient concentrées entre les mains des membres du personnel à titre individuel et n'étaient pas partagées. Enfin, le Comité a constaté que le risque de perte de connaissances et d'expertise au sein de l'organisation était accru en raison de la rotation du personnel (surtout des analystes) et qu'il n'y avait aucune procédure spécifique permettant d'endiguer cette perte de connaissances et d'expertise.

L'évaluation individuelle

Le Comité a pu remarquer la co-existence de trois systèmes d'évaluation au sein du SGRS : deux pour les civils (statut Camu/contractuels *versus* Statut 2014) et un troisième pour les militaires, ce qui donne lieu à des inégalités de traitement. Ce qui est certain, c'est que les militaires n'ont pas leur mot à dire dans les évaluations des civils et vice versa. Cela interfère avec les lignes hiérarchiques et peut s'avérer problématique.

I.1.5.11. Conditions de travail et infrastrutures

Le Comité permanent R a pu (une nouvelle fois) constater que les conditions de travail étaient pénibles et inacceptables à maints égards.

Les conditions de travail au niveau matériel constituaient LA priorité pour le personnel. Le Comité a pu observer divers manquements, notamment au niveau de la sécurité, de l'hygiène et des commodités, qui mettaient gravement en péril l'intégrité des bâtiments et du personnel.[32] Pour l'amélioration des conditions matérielles, le SGRS dépend de la Direction générale *'Material Resources' (DGMR) ;* son autonomie est des plus restreintes.

Il convient d'inscrire la problématique de l'hébergement du SGRS, et partant, de la Direction CI, dans le contexte plus global de la construction d'une nouvelle

30 Le Comité permanent R recommandait, dans l'Audit 2011, de s'atteler d'urgence à circonscrire les risques en termes de discontinuité de l'exercice de la fonction et de la perte des connaissances. Il convenait plus particulièrement d'instaurer une gestion prévisionnelle du personnel : *'il est indiqué qu'une attention particulière soit accordée au sein du SGRS à la gestion des connaissances. Des instructions claires doivent être élaborées afin d'identifier les connaissances actuelles, d'évaluer leur pertinence et de prendre des mesures afin de les stocker, les conserver et ensuite les communiquer. Il est recommandé de nommer un gestionnaire des connaissances dans chaque division qui soutiendra la gestion des connaissances'*, dans COMITÉ PERMANENT R, *Rapport d'activités 2011*, 107.

31 Il s'agit du processus visant à créer, inventorier (qui sait quoi), partager, utiliser et gérer les connaissances et de l'expertise au sein d'une organisation.

32 Le ministre de la Défense a signalé que dans l'attente d'une solution structurelle, des travaux de maintenance étaient effectués.

infrastructure pour l'état-major. Par conséquent, il faut, selon le Comité, s'atteler d'urgence à améliorer les conditions de travail.

I.1.5.12. Appui et logistique

Il est apparu que le personnel des services d'appui du SGRS (gestion du personnel et du budget, ICT, Logistique, etc.) n'était pas au fait de la culture du renseignement et de la spécificité du service. Il ne connaissait pas le travail de renseignement et il lui était donc difficile de traduire les besoins du service vis-à-vis des autres Directions générales et départements. Il a été constaté que la communication entre la Direction CI et les services d'appui n'était pas efficace, voire peu développée.

Le Comité permanent R a dû également constater que la Direction CI communiquait peu avec les sections d'état-major, tout en soulignant que ces sections représentent l'interface permettant de communiquer avec les autres acteurs extérieurs au SGRS. Des collaborateurs de CI ont fait savoir que l'appui logistique et technique s'était en grande partie vidé de sa substance. Les plaintes portaient sur le manque d'autonomie et la lourdeur bureaucratique.

I.1.5.13. Gestion des informations[33]

De précédentes enquêtes du Comité permanent R avaient déjà montré que la gestion des informations au SGRS était particulièrement problématique.[34]

La présente enquête a une nouvelle fois confirmé ces constats en ce qui concerne la Direction CI. C'est ce que le Comité a pu notamment déduire du questionnaire soumis au personnel. Les réponses à ces questions ont laissé apparaître qu'un problème se posait en matière d'accès à des banques de données externes. La Direction CI a aussi recueilli un faible score, notamment en termes de rapidité, de structure, d'exhaustivité, de convivialité et d'accès aux informations et à la documentation. En ce qui concerne la banque de données de la Direction CI, trois problèmes majeurs se posaient : un retard dans le traitement des données, des liens manquants avec les documents sources et la création de structures de fichiers individuelles.

---

33 La problématique de la gestion des informations est en réalité beaucoup plus vaste. Depuis que le Comité a constaté les problèmes relatifs au stockage et à la gestion des informations en 2005, un programme de travail et d'investissements a été établi en 2007. Compte tenu des restrictions budgétaires, les investissements n'ont pu débuter qu'en 2013. En outre, une cellule d''Information Management' a été créée en 2013 afin d'améliorer la gestion des informations. Cette cellule a développé un modèle de gestion des métadonnées, mais les moyens manquaient pour le faire fonctionner. À ce propos : Sénat 2017-18, 29 novembre 2017, Q. n° 6-1674.

34 Voir à ce propos, par exemple, COMITÉ PERMANENT R, *Rapport d'activités 2016*, 35 ('II.3. Enquête de contrôle sur la position d'information des deux services de renseignement avant les attentats de Paris').

I.1.5.14. Partenariats

La Direction CI a de nombreux partenaires nationaux et internationaux (administrations belges, partenaires étrangers, partenaires privés, etc.). Pourtant, peu de synergies ont été observées. Le Comité s'est référé à cet égard aux constatations et aux recommandations de la Commission d'enquête parlementaire 'Attentats terroristes'.[35] Dans le cadre de l'élaboration de synergies, il convient naturellement de veiller à ne pas mettre en péril la spécificité des missions de la Direction CI.

I.1.5.15. Feedback

Dès 2010[36], le Comité recommandait au SGRS d'élaborer un mécanisme de feedback pour tous les produits fournis. D'une part, les services devaient spécifier à quelles conditions, comment et à qui ils voulaient ou pouvaient diffuser des renseignements et quelle 'ambition' on était en droit d'attendre du service à cet égard (renseignements descriptifs, explicatifs ou prédictifs). Le Comité a aussi insisté sur le rôle des clients. Ils doivent préciser leurs attentes et leurs besoins (en matière de renseignements). Dans la présente enquête également, le Comité a dû constater qu'il n'était peu ou pas question de feedback.

I.2. LES ACTIVITÉS DU SGRS DANS UNE ZONE D'OPÉRATION À L'ÉTRANGER

Une part très importante du travail du SGRS est orientée vers la production de renseignements sur la situation politico-militaire à l'étranger. C'est la raison pour laquelle le Comité s'était intéressé au rôle de ce service en zone de conflit, par exemple en Afghanistan et au Liban.[37] En 2018, le Comité a une nouvelle fois examiné le déploiement du SGRS – et, par extension, du Bataillon ISTAR (voir *infra*) – dans une zone d'opération déterminée.[38, 39] Le SGRS a fourni un appui

35 Enquête parlementaire chargée d'examiner les circonstances qui ont conduit aux attentats terroristes du 22 mars 2016 dans l'aéroport de Bruxelles-National et dans la station de métro Maelbeek à Bruxelles, y compris l'évolution et la gestion de la lutte contre le radicalisme et la menace terroriste, troisième rapport intermédiaire, *Doc. parl.*, Chambre 2016-17, 54-1752/7.

36 Notamment dans : COMITÉ PERMANENT R, *Rapport d'activités 2011*, 104-105 ('IX.2.2.1. Recommandations relatives aux conditions organisationnelles requises pour une affectation adéquate des moyens').

37 COMITÉ PERMANENT R, *Rapport d'activités 2013* ('II.1. Le rôle du Service Général du Renseignement et de la Sécurité dans le suivi de la situation en Afghanistan'), 7-25 et *Rapport d'activités 2007* ('II.2. Le suivi de l'islamisme radical par le SGRS'), 21.

38 Pour des raisons de sécurité, le Comité permanent R a décidé de ne pas mentionner la localisation.

39 L'enquête a été ouverte en mars 2018 et a été clôturée début juillet 2018.

aux commandants militaires belges sur place afin de garantir la *force protection* des militaires belges déployés, et ce conformément aux recommandations de la Commission d'enquête parlementaire Rwanda.[40] Le SGRS a également mené des missions en appui à l'ambassade belge et a contribué à la sécurité des expatriés. Enfin, via ses bureaux d'analyse en Belgique, le service a contribué à l'élaboration de la vision stratégique belge dans cette zone de conflit.

Pour son enquête, le Comité s'est basé, entre autres, sur l'étude de nombreux documents[41], sur les briefings du SGRS et sur les contacts avec des membres du personnel du service de renseignement militaire. Il s'est en outre penché sur la collaboration entre les différentes sections du SGRS et sur la collaboration avec des partenaires étrangers actifs sur le terrain. En raison de la classification des informations apparues lors de l'enquête, le Comité ne peut entrer dans les détails dans le présent rapport. Seuls trois éléments seront succinctement expliqués : le contexte juridique du déploiement du SGRS, le fonctionnement du Bataillon ISTAR et le contrôle exercé sur celui-ci, et, enfin, quelques conclusions générales.

I.2.1. CONTEXTE JURIDIQUE DU DÉPLOIEMENT ET DES ACTIVITÉS DANS LA ZONE

Le déploiement d'unités militaires dans la zone s'inscrit dans le cadre d'un conflit armé non international. En d'autres termes, c'est le Droit des Conflits Armés qui est d'application. Le déploiement des troupes belges a été réalisé conformément à une résolution du Conseil de Sécurité des Nations Unies et a été approuvé par le Conseil des Ministres.

La compétence d'appui du SGRS aux opérations est définie à l'article 11 § 1er, 1°, d) L.R&S : '*§ 1er. Le Service Général du Renseignement et de la Sécurité a pour mission : 1° de rechercher, d'analyser et de traiter le 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, ainsi que le renseignement relatif à toute activité qui menace ou pourrait menacer : d) l'accomplissement des missions des Forces armées ; […] et d'en informer sans délai les ministres compétents ainsi que de donner des avis au Gouvernement, à la demande de celui-ci, concernant la définition de sa politique extérieure de défense*'.

Étant donné que le service ne peut pas effectuer toutes les missions possibles dans ce cadre, des priorités sont fixées dans ce que l'on appelle le 'Plan Directeur

40 *Doc. parl.*, Sénat 1997-1998, 6 décembre 1996, n°1-611/7.

41 L'Ordre d'Opération du Chef de la Défense (CHODOPORDER), les briefings des différentes sections, les rapports produits par les unités déployées, etc.

du Renseignement' (PDR). Le pays dans lequel se trouvait la zone de conflit figurait parmi les plus hautes priorités dans le PRD 2015-2018.

Les activités concrètes que doit mener le SGRS lors d'opérations à l'étranger sont précisées par ce que l'on appelle les Ordres d'Opération du CHOD (CHODOPORDER). Enfin, il y a également les *Fragmentary Orders* (FragO). Ceux-ci définissent le déploiement d'unités spécifiques du SGRS, telles que les *Contact Teams,* qui sont envoyées sur place pour une durée déterminée. Tous ces documents définissent le cadre et les limites dans lesquels les différents détachements (y compris ceux du SGRS) peuvent effectuer leurs missions. Afin d'être complet, il est nécessaire de mentionner que le Conseil national de sécurité pourrait également émettre des directives particulières dans le cadre du déploiement d'éléments du SGRS à l'étranger. À ce jour, ce cas de figure ne s'est jamais présenté.

I.2.2. LE BATAILLON ISTAR

En 2013 déjà, le Comité permanent R s'était prononcé dans le cadre d'activités de renseignement menées par le Bataillon ISTAR (*Intelligence Surveillance Target Acquisition and Reconnaissance*) dans le cadre d'opérations à l'étranger.[42] Le Comité soulignait que, vu l'augmentation du nombre de missions à l'étranger, la création du bataillon correspondait à un besoin croissant de capacités *battlefield intelligence*. Le Comité rappelait que la Loi du 30 novembre 1998 ne reconnaissait que deux services de renseignement. Il avait signalé au Parlement, au ministre de la Défense et au CHOD que ce bataillon développait des activités qui sont en partie des activités de renseignement. Dans la mesure où aucune solution légale ou structurelle n'était envisageable à court terme, une solution transitoire a été mise en œuvre et s'est traduite par la conclusion d'un protocole d'accord entre le SGRS et le CHOD.[43] Ce protocole définit les attributions et les compétences du Bataillon ISTAR en matière de HUMINT et de capacités d'analyse. L'organisation d'un contrôle technique et juridique y est également développée. Cette mission incombe au SGRS. Le Comité permanent R a été désigné pour exercer un contrôle – même indirect, puisqu'il s'exerce par le biais des rapports du SGRS – sur les activités du Bataillon ISTAR.

Le Comité a pu constater que, conformément à ses recommandations et à celles de la Commission 'Attentats Terroristes', les éléments du Bataillon ISTAR présents dans la zone d'opération concernée étaient détachés au SGRS pour la durée de leur déploiement et étaient donc considérés administrativement comme des éléments organiques du SGRS.

---

42 En 2013, la Commission de suivi du Sénat a été informée du point de vue juridique du Comité à ce propos (COMITÉ PERMANENT R, *Rapport d'activités 2013*, 92).

43 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.

I.2.3. CONCLUSIONS

Excepté le non-respect par le SGRS de certaines conditions formelles pour la mise en œuvre d'une méthode de collecte, le Comité n'a constaté aucune illégalité. Tous les membres du personnel déployés ont démontré leur professionnalisme et leur engagement. Les activités du SGRS ont permis de collecter des données essentielles dans le cadre d'événements ou d'incidents impliquant des belges ou des intérêts belges ou européens. Le Comité permanent R a également constaté que la collaboration entre les directions du SGRS reposait sur une concertation informelle, très étroite.

Les conditions de travail et de sécurité ont été analysées. Le Comité a quand même relevé certaines faiblesses susceptibles de constituer un risque pour la sécurité des opérations ou du personnel. En termes de niveau de contrôle, le Comité a dû constater que lors de la première rotation des éléments du Bataillon ISTAR, le SGRS n'avait pas effectué le contrôle prévu dans les règlements.

I.3. LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT AVANT L'ATTENTAT COMMIS À LIÈGE

I.3.1. CONTEXTUALISATION

Le 29 mai 2018, Benjamin Herman a ôté la vie à deux agents de police à Liège. Toutes deux ont été attaquées au couteau avant d'être abattues. L'auteur est ensuite monté dans un véhicule à l'arrêt, dont le passager est également décédé. Il s'est retranché dans une école où il a pris une personne en otage. Lors de l'échange de tirs qui a suivi, plusieurs agents ont été blessés et l'auteur a été tué par balle.

Benjamin Herman était déjà connu de la justice depuis son adolescence. Au moment des faits, il purgeait une peine de longue durée pour des faits de droit commun. L'intéressé a séjourné dans plusieurs établissements pénitentiaires et devait en principe être libéré dans le courant de l'année 2018. La veille des faits, il avait obtenu un congé pénitentiaire en vue de préparer sa libération définitive. Il a été hébergé pour la nuit chez une connaissance, et il est apparu par la suite que cette personne a également été abattue.

Début juin 2018, la Commission parlementaire de suivi a demandé aux deux Comités permanents R et P d'ouvrir une enquête de contrôle.[44] En effet, des éléments indiquaient que courant 2017, Benjamin Herman présentait des signes

[44] La Commission a également demandé aux deux Comités d'ouvrir une enquête commune sur le rôle de l'OCAM dans le suivi de l'auteur. Voir à ce propos : 'I.4. 'La position d'information de l'OCAM avant l'attentat commis à Liège'.

de radicalisation à la prison de Lantin. Mi-juin 2018, la Commission de suivi a précisé la question posée au Comité permanent R et lui a demandé d'ouvrir une enquête de contrôle *'sur la position d'information de la VSSE et sur les échanges d'informations entre la VSSE et ses partenaires concernant l'auteur et les éventuels co-auteurs ou complices des incidents de Liège'*.[45]

En ce qui concerne les services de renseignement et de sécurité[46], les questions posées étaient les suivantes :

- L'auteur était-il connu de la VSSE et/ou du SGRS avant l'attentat ? Quelles informations étaient disponibles à son sujet et quel service était à la base de ces informations ?
- Avec quels services des informations ont-elles été échangées ou avec quels services se sont-ils concertés ?
- A-t-on parlé de l'auteur lors de réunions au niveau local et au niveau national (Local Task Force (LTF), National Task Force (NTF)[47], ou encore la Cellule Sécurité Intégrale Locale (CSIL)[48]) ?
- La VSSE et/ou le SGRS ont-ils été contactés concernant l'intéressé avant le 29 mai 2018 ?
- En particulier pour la VSSE : comment les échanges se sont-ils déroulés avec la Direction générale des Établissements pénitentiaires (DG EPI) en application du Protocole d'accord ?

---

45 Le Comité permanent P a lui aussi effectué une enquête sur l'échange d'informations au niveau des services de police. Le rapport final commun aux deux Comités a été approuvé le 16 juillet 2018.

46 La compétence de contrôle des deux Comités permanents se limite aux services de police et de renseignement et de sécurité. Les Comités peuvent néanmoins inviter des membres d'autres services (tels que la DG EPI) pour une audition, lorsqu'ils l'estiment nécessaire (art. 24 et 49 L.Contrôle). Les Services d'Enquêtes des deux Comités ont également pris contact avec la cellule administrative du Cabinet du ministre de la Justice (SAT Justice) afin de se faire une idée de la manière dont les informations relatives aux détenus sont mises la disposition. Par ailleurs, des réunions se sont tenues avec la Cellule Extrémisme (service CelEx) de la DG EPI et avec un représentant de la direction générale en vue d'obtenir des informations contextuelles sur la manière dont les détenus extrémistes sont suivis dans les prisons.

47 Une LTF est une plateforme de concertation, instaurée à un niveau déconcentré, au sein de laquelle les services de police et de renseignement échangent des informations et des renseignements sur la radicalisation violente et concluent des accords de coordination sur la collecte de ces informations (cf. Circulaire ministérielle GPI 78 du 31 janvier 2014 relative au traitement de l'information au profit d'une approche intégrée du terrorisme et de la radicalisation violente par la police, *M.B.* 17 février 2014). Elles sont coordonnées par une National Task Force.

48 La CSIL ou CSIL-R est une plateforme communale de concertation multidisciplinaire composée d'acteurs socio-préventifs dans la lutte contre la radicalisation violente. Ces acteurs détectent à un stade précoce les personnes entrées dans un processus de radicalisation et élaborent pour eux des trajets de suivi sur-mesure.

I.3.2. LE SUIVI DES DÉTENUS EXTRÉMISTES

I.3.2.1. Une diversité d'acteurs

Plusieurs services interviennent dans le suivi des détenus aux opinions extrémistes ou condamnés pour terrorisme. Leur collaboration consiste à échanger et/ou à se concerter pour faire le point sur la question ou à déterminer les actions à entreprendre.

La DG EPI s'est vu attribuer un rôle important dans ce cadre. Les détenus sont quotidiennement en contact avec le personnel pénitentiaire dans les institutions et avec les directions locales. Un dossier personnel est conservé pour chaque détenu et est actualisé lorsqu'un fait survient. Au sein de la direction centrale de la DG EPI se trouve la Cellule Extrémisme (Service CelEx), qui est chargée d'effectuer un suivi particulier des détenus présentant un profil radical.

La VSSE s'intéresse elle aussi à ces personnes, que ce soit pendant la durée de leur détention ou après leur libération. Depuis 2015, une cellule créée au sein de la VSSE, la Cellule Prisons, est en contact étroit avec la DG EPI.[49] Les services extérieurs (postes de province) de la VSSE ont eux aussi un rôle à jouer en la matière en recueillant, par le biais de leurs contacts avec les autorités pénitentiaires, des informations sur les détenus qui justifient une attention de la VSSE.

Dans le cadre de sa mission de police administrative, la police ayant une prison sur son territoire est tenue de coopérer avec les services locaux de la prison. Elle est chargée d'évaluer les risques de transfert de détenus (p. ex. la sortie de détenus) et d'assurer la fonction de police de base, notamment le travail de proximité. L'article 20 LFP prévoit une surveillance, par la police, des condamnés qui bénéficient d'une modalité de mise en liberté.[50]

L'Organe de coordination pour l'analyse de la menace (OCAM) n'intervient que lorsque le nom d'un détenu est repris dans une banque de données commune (BDC)[51] (*(foreign) terrorist fighter*, *home grown terrorist* ou prédicateur de haine) ou lorsque des éléments – fournis par les services d'appui de l'OCAM – indiquent l'existence d'une menace terroriste ou extrémiste.

Enfin, les instances judiciaires – plus particulièrement les Parquets – peuvent également jouer un rôle lorsqu'elles reçoivent des informations des différents

---

49 Depuis la création de la Cellule Prisons, sa taille a quadruplé : de trois personnes, dont un analyste en 2015, le nombre est passé à douze en 2015, dont trois analystes.

50 La Circulaire commune du ministre de la Justice, du ministre de l'Intérieur et du Collège des procureurs généraux COL 11/2013 précise que les missions de surveillance policières qui y sont décrites ne doivent pas être obligatoirement exécutées dans les cas de permission de sortie et de congé pénitentiaire notamment. Dans ces derniers cas, la mission des services de police se limite à l'exercice de la surveillance policière générale.

51 Voir art. 44/11/3*bis* LFP, qui prévoit la création de banques de données communes. Voir à ce propos *in extenso* : 'Chapitre VI. Le contrôle des banques de données communes'.

services sur les activités de détenus qui revêtent un caractère pénal, ou quand ceux-ci sont impliqués dans ce genre d'activités, ou encore lorsque des actions judiciaires doivent être menées.

I.3.2.2. Une diversité de banques de données

La banque de données SIDIS Suite, gérée par la DG EPI, 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 communautaire pour mineurs. L'objectif est de faciliter une gestion adéquate de la détention et des institutions. La banque de données permet l'échange d'informations et les flux de données nécessaires entre, notamment, la police, le Parquet, les services de renseignement et les Maisons de Justice. SIDIS Suite contient des informations, entre autres, sur la durée de l'incarcération, les empreintes digitales, le parcours et le régime pénitentiaires, les visiteurs et les congés. La VSSE, la Police judiciaire fédérale, la DGA/DAO, la DGJ/DJO, le service de communication et d'information de l'arrondissement (SICAD) et les zones de police qui ont sur leur territoire une prison ou un palais de justice ont accès à toutes les données ou à certaines d'entre elles.[52, 53] Les services de police n'ont toutefois pas accès à toutes les données.

En outre, la DG EPI tient à jour une liste 'CelEx'.[54, 55] Cette liste – basée sur la note intitulée 'instructions spécifiques extrémisme' de la DG EPI – est établie à l'attention des directions des prisons mais aussi de tous les membres du personnel, afin qu'ils portent une attention constante sur les signes de radicalisation et d'extrémisme. Le placement d'une personne sur cette liste se traduit par une surveillance accrue du détenu. La liste CelEx comporte quatre

---

52 Les signalements judiciaires de personnes libres ou libérées moyennant le respect de conditions font l'objet de la COL 11/2013 et de la Circulaire FTF de 2015. En matière de congés pénitentiaires octroyés par le ministre de la Justice, la COL 11/2013 ne prévoit pas l'envoi automatique d'informations de la prison aux zones de police.

53 À propos du SIDIS Suite et de la manière dont les services (excepté la DG EPI) y accèdent, voir également la réponse du ministre de la Justice en Commission Justice de la Chambre des représentants, le 20 juin 2018, *Doc. parl.*, Chambre, CRABV, COM 930. À noter que l'accès à SIDIS Suite n'est pas le même pour tous les services. En sa qualité d'Autorité de protection des données, le Comité permanent R a formulé un avis, conjointement avec le Comité permanent P, sur un avant-projet de loi relatif à un accès à Sidis Suite pour l'OCAM, en octobre 2018 (www.comiteri.be, Avis 007/2018 – Droit de lecture Sidis Suite OCAM). Le Comité permanent R a également formulé un avis sur le droit de lecture dans Sidis Suite pour la VSSE, le SGRS et les autorités de sécurité (www.comiteri.be, Avis 006/2018 – Droit de lecture Sidis Suite).

54 Abréviation de 'Cellule Extrémisme', qui établit et conserve la liste. Début juillet 2018, la liste totalisait 234 noms (voir la réponse du ministre de la Justice, *Doc. parl.*, Chambre 2017-2018, 4 juin 2018, COM 910, 34 : *'er zouden ongeveer 250 geradicaliseerden in onze gevangenissen opgesloten zitten'* (*'Dans nos prisons, il y aurait environ 250 radicalisés'* (traduction libre)).

55 La DG EPI parle plutôt du 'rapport CelEx' que de la liste CelEx.

catégories de détenus.[56] Dès qu'une personne est placée sur cette liste, un message est envoyé aux services partenaires (VSSE, DJSoc Terro, OCAM) afin de partager les informations, mais aussi de savoir si cette personne est déjà connue des services de police et de renseignement. Dans certains cas, un message est également envoyé à différents services lorsqu'un détenu se trouve hors de l'enceinte de la prison. Benjamin Herman ne figurait pas dans la liste CelEx.

La DG EPI (CelEx), la VSSE, l'OCAM et la Police fédérale (DJSOC/terro) se réunissent deux fois par mois au niveau fédéral dans le cadre du Groupe de travail Prisons du Plan Radicalisme afin de se concerter, entre autres, sur la composition de la liste CelEx. La VSSE a fait remarquer qu'il n'existe aucune procédure formelle sur le placement (ou l'effacement) de personnes sur cette 'liste', que le rôle consultatif des services partenaires de la DG EPI est plutôt informel et qu'il a évolué grâce à la collaboration quotidienne. La VSSE s'est prononcée en faveur d'une formalisation de la procédure et d'un élargissement de l'*ownership* encore détenu entièrement par la DG EPI.

Enfin, il convient de signaler que la VSSE ne se limite pas au suivi des détenus figurant dans la liste CelEx. La 'Cellule Prisons' travaille aussi avec une 'liste de targets', par prison. Au moment où l'enquête a été réalisée, ce sont donc quelque 500 détenus qui figuraient dans la 'liste de targets' de la VSSE en raison de leur lien éventuel avec le terrorisme (accès à des armes, financement du terrorisme avec l'argent de la drogue, etc.). L'existence de deux listes tient notamment au fait que la VSSE ne veut pas dévoiler l'identité de certains détenus, ce qui s'explique soit par les risques encourus par la source ou la règle du tiers service, soit par le souci de ne pas mettre en péril des enquêtes de renseignement ou judiciaires en cours. Par ailleurs, il faut tenir compte de la différence de finalité entre la VSSE et la DG EPI : la VSSE peut procéder plus en amont au recueil de renseignements sur certains détenus, c'est-à-dire sans qu'il existe au préalable, dans le chef de la DG EPI, des motifs suffisants pour les reprendre dans la liste CelEx. Benjamin Herman ne figurait pas non plus dans ces listes de targets.

---

56 (a) les condamnés pour infractions terroristes ou inculpés ; (b) les assimilés à des infractions terroristes ; (c) les *(foreign) terrorist fighters* et *home grown terrorists* de la liste OCAM, que leur écrou soit ou non motivé par leur caractère FTF (beaucoup de droit commun) ; et enfin (d) la liste renferme une quatrième catégorie subsidiaire D. La Cellule Extrémisme évalue, avec l'appui de ses partenaires, si les détenus doivent être placés dans cette catégorie. Les partenaires privilégiés de la cellule sont l'OCAM, la DJSOC Terro et la VSSE.

I.3.3. LES INFORMATIONS DÉTENUES PAR LES SERVICES DE RENSEIGNEMENT[57]

Benjamin Herman n'était pas repris dans les banques de données du SGRS. Si le SGRS était bien présent et destinataire d'un rapport d'une réunion d'une LTF le 22 février 2015 à Marche-en-Famenne (dans lequel le nom de Benjamin Herman était cité), il n'y avait cependant pas le moindre lien à caractère militaire. Il n'est donc pas anormal que le nom de l'intéressé n'ait pas été introduit dans la banque de données du SGRS.

À la VSSE, Benjamin Herman apparaissait dans sept documents.[58] Les notes disponibles montrent que les données dont disposait la VSSE sur l'intéressé étaient plutôt vagues et limitées en termes de contenu. Les dernières informations provenant de la propre collecte du service remontaient au 1er février 2017. Il y était établi que, selon une source, Benjamin Herman se radicalisait et qu'il se rapprochait de plus en plus d'une personne qui poursuivait ses activités de prosélytisme au sein de la prison. Les notes d'analyse qui ont suivi reprenaient ces informations et des informations antérieures. Ainsi, par exemple, une note d'analyse a été diffusée en mai 2017 à la Police fédérale, à l'OCAM et à la DG EPI.

I.3.4. LES FLUX D'INFORMATIONS RÉCIPROQUES

Le nom de l'intéressé a été mentionné lors de plusieurs réunions de concertation (LTF, Groupe de travail Prisons) qui se sont tenues à différents moments.

I.3.4.1. La Local Task Force (LTF)

Benjamin Herman a été cité dans deux rapports de réunion de la LTF de l'arrondissement de Luxembourg (février 2015 et mars 2017).

Plusieurs services de police et le SGRS étaient présents à la réunion qui a eu lieu en 2015, mais pas la VSSE, ni l'OCAM ni le Parquet. Le procès-verbal a été envoyé aux personnes présentes ainsi qu'à la VSSE, mais pas à l'OCAM.[59] Dans ce rapport, il était fait référence à Benjamin Herman qui, semble-t-il, pratiquait la prière de façon intensive avec deux codétenus, mais le rapport signalait aussi qu'aucune pression n'était exercée sur d'autres codétenus pour qu'ils s'y associent.[60]

---

57 Le Comité permanent P a fait rapport des informations dont disposaient les services de police (www.comitep.be).

58 Il s'agissait de cinq rapports opérationnels (OR) des services de collecte qui n'ont pas directement été diffusés à l'extérieur, mais qui ont été traités par les services d'analyse, d'une fiche de synthèse (FS) et de deux 'Notes aux autorités' (NA).

59 À ce moment-là, les rapports des Local Task Forces ne devaient pas être envoyés à l'OCAM. L'OCAM ne recevait que les informations pertinentes concernant les *foreign terrorist fighters*.

60 Ces informations sont les mêmes que celles qui avaient été reprises le mois précédent dans un rapport d'information de la police (RIR).

Lors de la réunion de la LTF de mars 2017, une liste de plus de 50 personnes faisant l'objet d'un suivi a été reprise. Plusieurs services de police, la VSSE, l'OCAM et le Parquet étaient présents, mais pas le SGRS. Le rapport, dans lequel figure le nom de Benjamin Herman, a été envoyé à tous les services. Dans la colonne 'Personne', ce n'est pas le nom de l'intéressé qui apparaît explicitement, mais bien celui d'une autre personne détenue à la prison de Marche-en-Famenne. Au sein de la prison, ce détenu adoptait un comportement menaçant et arrogant et voulait se faire passer pour un djihadiste pur et dur. Il est mentionné que cette personne était incarcérée pour des faits de droit commun commis, entre autres, avec Benjamin Herman.[61] Ces informations provenait d'un RIR de la zone de police locale de Famenne-Ardenne. Il est vrai que Benjamin Herman lui-même ne faisait pas l'objet du RIR. Au cours de ce genre de réunions, aux dires des répondants, il est d'usage de ne citer le nom d'une personne que si les services concernés ont un élément utile à relever ou à ajouter à son sujet. Or, Benjamin Herman n'attirait en rien l'attention. L'inspecteur de la VSSE présent à la réunion a établi un rapport interne pour sa hiérarchie, rapport dans lequel le nom de Benjamin Herman ne figurait pas. L'interprétation qui a été faite était, selon la VSSE, qu'il s'agissait de faits de droit commun, ce qui ne relève pas des points d'attention de ce service. Il n'y avait donc aucune raison pour la VSSE de reprendre spécifiquement, dans un rapport interne, le nom de Benjamin Herman sur la base de la liste de la LTF.

I.3.4.2. Le Groupe de travail Prisons du Plan Radicalisme

Benjamin Herman ne figurait pas dans la liste CelEx. Son cas n'a jamais été évoqué lors des discussions bimensuelles du Groupe de travail Prisons du Plan Radicalisme, entre la VSSE (pilote), la DG EPI (CelEx), l'OCAM et la Police fédérale (DJSOC/terro). La VSSE se limitait à rédiger un rapport de ces réunions à usage interne.[62]

Début août 2017, des e-mails ont bien été échangés entre différents services – la VSSE, la DG EPI, DJSOC Terro, l'OCAM – à propos d'un détenu X de la prison de Leuze (Hainaut). En août 2017, la VSSE a produit une note d'analyse sur ce détenu X, mentionnant le nom de Benjamin Herman et, entre autres, (succinctement) sa radicalisation.[63] Le jour de l'envoi de la note, la VSSE et Cellule Extrémisme ont été en contact, non pas concernant Benjamin Herman, mais concernant la personne X. Dans l'échange d'e-mails qui a suivi entre la VSSE et la DG EPI, il a néanmoins été

61 Le 13 mars 2017, Benjamin Herman se trouvait encore à la prison de Lantin ; son transfert à Marche-en-Famenne n'a eu lieu que quelques jours plus tard.

62 La VSSE affirmait que, dans le passé, les résultats des discussions étaient suffisamment couverts dans les échanges d'e-mails très fréquents entre les services, mais que la formalisation récente – sous la forme d'un rapport officiel – est une évolution normale.

63 La note d'analyse a été envoyée à la DG EPI, à DJSOC Terro et à l'OCAM. Cette note ne fait pas mention de la liste CelEx.

question de Benjamin Herman, qui a été cité nommément. Dans cet échange d'e-mails, la DG EPI demandait si Benjamin Herman, notamment, '*best op de CelEx-lijst worden geplaatst*',[64] tout en faisant remarquer que depuis 2017 aucun signe apparent de radicalisation plus poussée n'avait été observé.[65] La VSSE a répondu que la DG EPI '*de administratieve beslissing zelf neemt, op basis van de door de VSSE aangereikte inlichtingen*'.[66] Et la VSSE d'ajouter que même lorsque des personnes ne figurent pas dans la liste CelEx, elles sont quand même suivies par la VSSE.

Lors des réunions de concertation qui ont eu lieu ultérieurement, le cas de Benjamin Herman n'a manifestement plus été évoqué. Les services de police et de renseignement n'ont d'ailleurs plus reçu aucune information à son sujet jusqu'au 29 mai 2018, date de la commission des faits.

I.3.5. L'ÉVALUATION DU PROTOCOLE DG EPI/VSSE

Dès 2014, le Comité permanent R a ouvert une enquête de contrôle sur la manière dont la VSSE met en application le *'protocole d'accord réglant la coopération entre la Sûreté de l'État et* [ce qui était] *la Direction générale Exécution des Peines et des Mesures*'.[67] À l'époque, le Comité permanent R n'était pas encore en mesure de présenter les chiffres exacts de l'échange de données. Dans le cadre de la présente enquête, l'intensité des contacts entre les deux services a pu être quantitativement démontrée.[68]

Dans la première enquête, aucun manquement notable ni manifestation d'insatisfaction n'a pu être constaté(e) concernant la collaboration existante. Ce constat a pu être confirmé.

Dans ses recommandations, le Comité soulignait l'importance d'utiliser les différentes listes avec prudence et de veiller à en établir clairement la finalité, qu'il convenait de respecter. Un élément important à souligner concernant l'interaction entre la liste CelEx et la liste de la VSSE est qu'il arrivait souvent qu'un détenu soit informé que son nom figure dans la liste CelEx. En effet, il en subit les conséquences au quotidien. À noter également qu'un suivi discret par la VSSE est rendu plus compliqué.

---

64 *'Ne devrait pas être placé dans la liste CelEx'* (traduction libre).

65 Reprendre le nom d'un détenu dans la liste CelEx a certaines répercussions sur l'intéressé. La DG EPI doit donc motiver minutieusement un placement dans la liste. À cet égard, un problème peut survenir lorsque la DG EPI agit sur la base d'informations 'douces' ou d'informations classifiées. Celles-ci ne peuvent dès lors être utilisées sans raison valable pour motiver une décision.

66 *'Que [la DG EPI] prend elle-même la décision administrative, sur la base des renseignements transmis par la VSSE'* (traduction libre).

67 COMITÉ PERMANENT R, *Rapport d'activités 2016*, 57-63 ('La VSSE et le protocole de coopération avec les établissements pénitentiaires').

68 Le nombre d'e-mails sortants de la VSSE vers la CelEx oscillait, entre janvier 2017 et juin 2018, entre 100 et 270 ; le nombre d'e-mails entrants pour la même période oscillait entre 200 et 450. On remarque une courbe ascendante pour les deux flux au fil du temps.

Par ailleurs, un échange d'informations a une nouvelle fois été examiné dans le cadre de l'évaluation du protocole (en particulier la diffusion d'informations brutes). La VSSE n'a pas diffusé de rapports opérationnels internes mentionnant Benjamin Herman, contrairement aux services de police qui ont diffusé des rapports d'information (RIR) rédigés par leurs soins, qui reprenaient aussi des informations brutes.[69]

I.3.6. CONCLUSIONS DES COMITÉS PERMANENTS R ET P

I.3.6.1. En ce qui concerne la position d'information des services

Force est de constater que les informations dont disposaient les services de police et de renseignement, ainsi que l'OCAM, à propos de Benjamin Herman, étaient très limitées en nombre, mais aussi sommaires et peu alarmantes. Le terme 'radicalisation' concernant Benjamin Herman est apparu pour la première (et la dernière) fois dans le rapport opérationnel de la VSSE datant de février 2017. Les informations étaient particulièrement sommaires. Certains comportements religieux, sans être extrémistes, ont été observés chez l'auteur de l'attaque, mais aucun prosélytisme n'a pu être constaté. Indépendamment de son passé de criminel de droit commun, on ne pouvait déduire que Benjamin Herman était susceptible de représenter une menace extrémiste ou terroriste.

Le suivi de Benjamin Herman, que ce soit par les services ou au sein de la prison, ne laissait pas présager qu'il planifiait un attentat pendant son congé pénitentiaire. Pendant cette période et jusqu'au moment où il a commis l'attaque, il n'était plus apparu sur les radars.

Il y a peu de variations entre les informations que détenaient les services de police et celles dont disposait la VSSE, et donc peu de variations avec les informations transmises par ces services à l'OCAM. Cela tient au fait que les services n'ont qu'une vue directe limitée sur les détenus.

Les diverses listes – liste OCAM, liste CelEx, listes de targets de la VSSE – ne présentent pas une parfaite cohérence. Il a toutefois été démontré que les informations étaient partagées. Le ministre de la Justice a indiqué son intention

69 La VSSE ne diffuse que des informations qui ont été analysées ('renseignements'), sur la base des informations issues de sa propre collecte, ou des informations qu'elle reçoit d'autres sources/partenaires. Tous les rapports de collecte ne donnent pas automatiquement et immédiatement lieu à une note d'analyse envoyée aux autorités. La manière dont les informations issues de la collecte sont traitées dans des notes d'analyse et le moment de la rédaction d'une note d'analyse dépendent notamment de la qualité des informations brutes et de leur nombre. Dans le cas présent, les informations figurant dans les notes de collecte ont effectivement été traitées dans des notes d'analyse et ont donc été diffusées.

de remanier la liste CelEx et de l'intégrer dans la banque de données commune de l'OCAM pour ainsi supprimer les différences entre les listes.[70]

I.3.6.2. En ce qui concerne l'échange de données

Les services, chacun de leur côté, disposaient d'informations sur l'intéressé et les transmettaient à l'OCAM. À cet égard, on remarque que les services de police et la VSSE n'opéraient pas de la même manière. Après un contrôle de qualité interne, la DJSOC de la Police fédérale communiquait à l'OCAM les rapports d'information (RIR) rédigés par les services de la Police fédérale, mais ceux-ci étaient dépourvus d'analyse. Pour sa part, la VSSE ne communiquait pas les rapports opérationnels internes (OR) des services de collecte avant d'avoir effectué une analyse ; le service transmettait donc à l'OCAM les informations traitées (notes d'analyse). La différence s'explique notamment par différence de logique et de finalité des documents : la logique policière selon laquelle les informations de base doivent demeurer intactes *versus* la logique de renseignement selon laquelle l'analyse et la mise en commun d'informations provenant de plusieurs sources jouent un rôle essentiel. La VSSE envoyait également ces notes d'analyse à la Police fédérale.

Les informations que recevait l'OCAM étaient enregistrées dans la banque de données interne. Cette banque de données n'est pas accessible aux autres services sauf dans le cas des personnes qui sont reprises dans la banque de données consolidée TF[71] ou prédicateurs de haine. Mais puisque dans le chef de Benjamin Herman, aucun lien ne pouvait être établi avec une quelconque menace extrémiste ou terroriste, les informations n'ont pas été traitées dans cette banque de données et n'étaient pas consultables par tous.

Ce qui apparaît par ailleurs, c'est la position très importante et le rôle éventuel de la DG EPI dans la collecte d'informations sur des détenus.[72]

I.3.6.3. En ce qui concerne les rôles des services

Les Comités permanents R et P estiment que les différents services ont traité les informations comme il se doit. Les informations dont ils disposaient étaient

---

70 Voir à ce propos la réponse du ministre de la Justice en Commission Justice de la Chambre des représentants, le 20 juin 2018, où il déclarait que *'een KB wordt opgesteld dat de CelEx-lijst zal opnemen in de gemeenschappelijke databank van het OCAD'*, (*'un A.R. est rédigé en vue de reprendre la liste CelEx dans la banque de données commune de l'OCAM'* (traduction libre)), *Doc. parl.*, Chambre, CRABV, 54 COM 930, 5. Dans sa réponse au projet de rapport, la VSSE suggère que la révision du Plan d'action Radicalisme dans les prisons de mars 2015 peut constituer une base.

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

72 Dans sa réponse au projet de rapport, la VSSE affirmait qu'on ne saurait assez souligner l'importance de la CelEx. Et le service de plaider depuis un certain temps déjà en faveur d'un renforcement de la CelEx, associé au recrutement de 'Coordinateurs locaux radicalisme'.

limitées en nombre et sans véritable contenu, mais ont bien été échangées. On ne pouvait toutefois en déduire que Benjamin Herman avait des projets extrémistes-radicaux ou terroristes, ou qu'il constituait une menace de cette nature. Pour l'OCAM, aucune analyse de risques individuelle ne se justifiait à propos de l'intéressé. Aucun service ne pouvait prévoir, sur la base des informations en sa possession, que Benjamin Herman commettrait un attentat.

La gestion de la liste CelEx par la DG EPI ne relève pas de la compétence des Comités permanents R et P, qui ne peuvent donc pas se prononcer.

Même si ce n'était pas l'objet des enquêtes de contrôle, les deux Comités ont eu connaissance d'une note interne rédigée au sein de l'administration pénitentiaire trois jours avant les faits (le 25 mai 2018). Le contenu de cette note confirmait ce qui avait été mentionné. Dans cette note non plus, Benjamin Herman n'était pas 'LE' target, contrairement à d'autres personnes. Benjamin Herman ne jouait pas un rôle central, et aucun élément n'indiquait une menace ou un projet extrémiste ou terroriste. Il s'agissait d'une simple note d'information destinée à la direction de la prison. Il était clair que même si cette note avait été connue des autres services avant le passage à l'acte, on n'aurait pas pu en déduire que Benjamin Herman constituait une menace ou avait l'intention de commettre un attentat.[73]

I.4. LA POSITION D'INFORMATION DE L'OCAM AVANT L'ATTENTAT COMMIS À LIÈGE

I.4.1. L'OUVERTURE D'UNE ENQUÊTE DE CONTRÔLE COMMUNE

Au lendemain de l'attentat perpétré à Liège, fin mai 2018, par Benjamin Herman[74], la Commission parlementaire de suivi des Comités permanents R et P ont demandé que soit également ouverte une enquête commune sur la position d'information de l'OCAM.[75] Les questions suivantes ont été posées au service :

- De quelles informations disposait l'OCAM sur l'auteur avant le 29 mai 2018 (moment de l'attentat) ? L'auteur était-il connu comme étant radicalisé ? Quelles informations l'OCAM a-t-il reçues de ses partenaires/services d'appui ?
- L'OCAM a-t-il échangé des informations avec ses partenaires/services d'appui ? Des informations relatives à l'auteur ont-elles été mises à disposition via une banque de données ? L'intéressé a-t-il fait l'objet de concertations ?

---

73 Il est évident que si l'attentat n'avait pas été perpétré, au vu du contenu de la note, il n'y aurait eu, en principe, aucune raison d'en informer spécialement la VSSE.

74 Voir à ce propos : 'I.3. La position d'information des services de renseignement avant l'attentat commis à Liège'.

75 En vertu de l'article 53, alinéa 1er, 6° de la Loi Contrôle du 18 juillet 1991, les Comités permanents R et P exercent conjointement leurs missions de contrôle à l'égard de l'OCAM et de ses services d'appui.

– L'OCAM a-t-il réalisé une évaluation de la menace ou une analyse de risques concernant l'auteur ?

Les deux services d'enquêtes se sont rendus ensemble à l'OCAM pour vérifier quelles informations y étaient disponibles. Ils se sont également entretenus avec le directeur et des membres de l'organe de coordination.

I.4.2. LES SOURCES D'INFORMATIONS

L'intervention de l'OCAM n'est prévue que lorsqu'un détenu figure dans la banque de données commune (BDC) (*(foreign) terrorist fighter, home grown terrorist* ou prédicateurs de haine) ou lorsque des éléments – fournis par les services d'appui de l'OCAM – indiquent l'existence d'une menace terroriste ou extrémiste relevant du domaine de compétences de l'OCAM.

Concernant Benjamin Herman, l'OCAM n'était en possession que d'un nombre limité d'informations. Il s'agissait de :
– Trois rapports d'information (RIR) de la Police judiciaire fédérale de Luxembourg (2015), de la Police judiciaire fédérale de Liège (2016) et un dernier RIR établi par la zone de police Famenne-Ardenne (2017) ;
– Deux notes d'analyse de la Sûreté de l'État (2017) ;
– Le rapport de la *local task force* de Neufchâteau de mars 2017.[76]

L'OCAM peut obtenir des informations émanant de l'administration pénitentiaire par plusieurs canaux : directement par les prisons elles-mêmes – par exemple lors des réunions sur les détenus CelEx – ou encore via d'autres types de communications[77], mais aussi indirectement via les services de police (dans un RIR), via la VSSE (dans une note d'analyse), via une LTF[78], etc. Au moment de l'enquête a été menée, la DG EPI n'était pas encore un service d'appui de l'OCAM.[79, 80]

---

76 Un précédent rapport LTF de 2015 n'a pas été transmis à l'OCAM ; l'OCAM ne recevait, à ce moment-là, que les informations pertinentes concernant les *foreign terrorist fighters*.

77 Par exemple, des e-mails lorsqu'il s'agit spécifiquement d'un détenu repris dans la liste CelEx.

78 L'OCAM a signalé qu'à l'instar de la DJSOC/T et de la VSSE, il reçoit des informations et des questions de la DG EPI, et ce conformément aux accords conclus entre ces services dans le Groupe de travail Prisons. L'OCAM n'intervient cependant pas dans les questions qui touchent aux compétences opérationnelles des services concernés.

79 L'Arrêté royal 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) y a remédié.

80 Il n'y a pas de feedback garanti vers la DG EPI : si les services de police ou la VSSE font rapport ou communiquent sur un détenu, en interne ou à l'extérieur (par exemple, l'OCAM), la DG EPI ne le sait pas nécessairement, pas plus qu'elle ne sait si les informations qu'elle a fournies ont donné d'une manière ou d'une autre un résultat.

I.4.3. LES INFORMATIONS DISPONIBLES À L'OCAM

Les Comités ont pu constater que les informations que détenait l'OCAM étaient identiques à celles des services de police et de renseignement. Benjamin Herman n'apparaissait jamais 'directement' dans ces informations, mais toujours en relation et en marge d'autres personnes qui avaient attiré plus directement l'attention des services. L'OCAM ne savait rien des opinions de l'auteur, hormis le fait qu'il était un musulman pratiquant (dans le sens où il participait aux prières). L'OCAM ne pouvait pas conclure des données disponibles qu'il constituait ou pouvait constituer une menace.

Benjamin Herman était pourtant repris comme entité dans la banque de données interne de l'OCAM, dans laquelle figuraient les documents susmentionnés. Toutefois, cette banque de données n'est pas accessible aux autres services.[81] Comme indiqué au point I.3, les différentes listes (liste OCAM, liste CelEx, listes de targets parmi les détenus établies par la VSSE) ne présentent pas une parfaite cohérence.

Les informations disponibles ne contenaient pas suffisamment d'éléments répondant aux critères prédéfinis pour faire figurer le nom de l'intéressé dans la banque de données commune, dont la gestion opérationnelle est assurée par l'OCAM (banque de données consolidée *foreign terrorist fighters*, *home grown terrorists*, propagandistes de haine). Pour la même raison, l'OCAM n'a pas rédigé de document interne ni établi d'analyse de risques concernant Benjamin Herman. Les deux Comités ont approuvé ce raisonnement et ont conclu qu'au vu de la nature des informations, une analyse de la menace ne s'imposait pas. L'information relative à la radicalisation de l'intéressé[82], qui remontait à 2017, était trop sommaire pour se pencher sur son cas. Par ailleurs, Benjamin Herman n'avait plus attiré l'attention depuis lors.

I.5. UN PRÉTENDU ENGAGEMENT PRIS PAR UN SERVICE DE RENSEIGNEMENT VIS-À-VIS D'UN TIERS

En 2018, le Comité permanent R a reçu une plainte, dans laquelle le plaignant prétendait qu'un service de renseignement s'était engagé à faire de lui un

81 Si la banque de données commune devait être élargie, intégrant des détenus en voie de radicalisation et ceux qui quittent la prison après une condamnation pour des faits liés au terrorisme, comme c'est apparemment l'intention des ministres de la Justice et de l'Intérieur (voir réponse du ministre de la Justice, *Doc. parl.*, Chambre, CRIV, 54, COM 910 du 4 juin 2018, 34), ce problème serait résolu et les services externes à l'OCAM pourraient eux aussi consulter ces informations.

82 Voir 'I.3. La position d'information des services de renseignement avant l'attentat commis à Liège'.

informateur. Le Comité a procédé aux vérifications requises auprès du service de renseignement concerné et n'a pas trouvé la moindre preuve d'un tel engagement.

I.6. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ EFFECTUÉS EN 2018 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2018

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

En 2016 déjà, à l'occasion d'une réunion internationale à laquelle participaient plusieurs organes de contrôle européens[83], 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 contre les *foreign terrorist fighters* (FTF). Par la suite, cette initiative a reçu le soutien explicite du président de la Commission de suivi. L'idée est que chaque organe de contrôle étudie cette thématique de son point de vue et en fonction de sa compétence, tout en adoptant la même philosophie et certainement une approche commune. Le volet belge de l'enquête[84] consiste à avoir la vision la plus précise et complète possible de l'échange d'informations bilatéral ou international, tant formel qu'informel, entre la VSSE et le SGRS, d'une part, et les services étrangers, les groupes de travail ou les structures de coopération, d'autre part, et ce concernant la problématique des FTF.

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

Pendant trois ans, les organes de contrôle participants se sont régulièrement réunis pour discuter des méthodes, des meilleures pratiques, des problèmes juridiques et pratiques, mais également pour échanger leurs expériences dans le cadre des enquêtes nationales. Il n'y a pas eu de partage de données classifiées.

---

83 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.

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

Début novembre 2018, ces organes ont diffusé une déclaration commune et un communiqué de presse.[85] Le volet belge de l'enquête a été finalisé début 2019.

I.6.2. 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 de fiabilité suffisantes.

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

Dans le cas présent, c'est une plainte qui est à l'origine de l'enquête de contrôle. Un collaborateur de l'aéroport de Bruxelles National s'était vu retirer son badge d'accès suite à un avis négatif[86] de l'Autorité nationale de sécurité (ANS). Il avait introduit un recours devant l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité ainsi qu'un recours en suspension et en annulation devant le Conseil d'État. L'Organe de recours avait jugé la plainte irrecevable car elle avait été introduite contre la décision du SPF Mobilité et Transports et non contre l'avis émis par l'ANS. Le Conseil d'État a lui aussi rejeté la plainte. Le plaignant s'était alors tourné vers le Comité permanent R, sans toutefois définir l'objet de sa plainte. Il déclarait ne pas comprendre les raisons de l'avis négatif, qui avait eu pour effet de le priver de son travail et, de surcroît, de voir sa licence de pilote suspendue.

Le Comité estimait légitime, en partant d'un cas individuel, d'ouvrir une enquête de contrôle plus large sur la manière dont les services de renseignement réalisent les screenings de sécurité.[87]

---

85 Voir Annexe D. 'Renforcement du contrôle des échanges internationaux de données entre les services de renseignement et de sécurité'.

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

87 'Enquête de contrôle sur la manière dont la VSSE et la SGRS procèdent aux vérifications de sécurité et à l'évaluation des données nécessaires à l'octroi des attestations de sécurité, en application des articles 22*bis* à 22*sexies* de la Loi du 11 décembre 1998 relative à la

En raison d'autres priorités, les premiers devoirs d'enquête n'ont pu démarrer que fin 2017. De janvier à mai 2018, des entretiens ont été organisés avec les responsables des sections qui traitent les screenings de sécurité au sein des deux services de renseignement, ainsi qu'avec quelques-uns de leurs collaborateurs. Ces entretiens se sont déroulés en plusieurs sessions et ont permis d'obtenir des précisions et de déceler des particularités. En outre, le Comité a réalisé une analyse juridique détaillée de la législation pertinente pour l'enquête, en plus des chiffres et autres documents qui ont été demandés aux services.

En novembre 2018, un projet de rapport a été envoyé tant à la VSSE qu'au SGRS ; en décembre, le Comité a reçu les remarques des services et a adapté son rapport en conséquence. L'enquête de contrôle a été finalisée en mars 2019.

I.6.3. 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/ou contre la Belgique, et de leur permettre de réagir de manière adéquate.[88] Le *core business* de l'OCAM consiste à réaliser des évaluations ponctuelles ou stratégiques. Cette tâche incombe à des analystes et à des experts, détachés de ce que l'on appelle les 'services d'appui'. Ces services d'appui constituent la principale source d'informations pour l'organe de coordination. Ce sont la VSSE, le SGRS, la Police intégrée, l'Administration des Douanes et Accises du SPF Finances, l'Office des étrangers du SPF Intérieur, le SPF Mobilité et le SPF Affaires étrangères (art. 2, 2. L.OCAM). Il s'agit de services très variés, de culture et de taille différentes.

Précédemment, en 2010, le Comité permanent R avait effectué une enquête, conjointement avec le Comité permanent P, sur les flux d'informations entre l'OCAM et les services d'appui, en mettant l'accent sur les deux services de renseignement et sur la Police fédérale et les Polices locales.[89]

Lors de la réunion plénière commune de décembre 2017, les Comités permanents R et P ont décidé d'ouvrir une enquête de contrôle sur les 'autres'

---

classification et aux habilitations, attestations et avis de sécurité (L.C&HS)'. L'enquête a été ouverte le 13 février 2017.

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

89 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').

services d'appui.[90] Les Comités souhaitaient ainsi établir un *status quaestionis* du flux d'informations entre l'OCAM et les quatre[91] 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 2018. Par exemple, sur la base d'une liste de questions structurée et détaillée, des entretiens ont eu lieu avec les responsables de l'Office des étrangers (SPF Intérieur), du SPF Mobilité, du SPF Affaires étrangères ainsi que de l'Administration des Douanes et Accises (SPF Finances) détachés auprès de l'OCAM. Les points de contact des différents services d'appui ont eux aussi été interrogés. Enfin, plusieurs concertations ont été organisées avec l'équipe d'enquête du Comité permanent P.

L'enquête de contrôle commune sera finalisée au second semestre 2019.

I.6.4. L'EXAMEN DU FONCTIONNEMENT DE LA SECTION I/H DU SGRS

Une enquête judiciaire du Parquet fédéral, menée sur le terrain par le Service d'Enquêtes du Comité permanent R, a révélé plusieurs dysfonctionnements structurels au sein de la Section I/H (*Human intelligence*) du SGRS. Cette section est une composante de la Direction I(intelligence) du service de renseignement militaire et a pour mission de créer des réseaux de sources et d'informateurs pour permettre au SGRS de recueillir des renseignements sur des phénomènes étrangers. Plusieurs de ces dysfonctionnements ont déjà été traités dans le cadre d'une enquête de contrôle précédente.[92] La description des tâches, la gestion stratégique, les compétences et la qualité du personnel, le *tradecraft*, entre autres, étaient considérés comme problématiques. Il était également question de la Section I/H dans l'enquête sur le fonctionnement de la Direction Counterintelligence (I.1). Cette enquête a en effet démontré qu'en l'absence de directives et d'accords clairs, les deux services risquaient à tout le moins de se contrecarrer.

Début mai 2018, le Président de la Commission de suivi, le ministre de la Défense et le SGRS ont respectivement été informés de l'ouverture d'une *'enquête de contrôle sur le fonctionnement du service 'I/H' du SGRS'*.

---

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

91 Motivé par la nécessité de réglementer au plus vite les flux d'informations des services concernés vers l'OCAM et inversement, la Direction générale du Centre de crise (SPF Intérieur), la Direction générale des Établissements pénitentiaires (SPF Justice), le Service Laïcité et Cultes de la Direction générale de la Législation et des Libertés et Droits fondamentaux (SPF Justice) et l'Administration générale de la Trésorerie (SPF Finances) ont complété la liste des 'services d'appui' (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. Ces services d'appui n'entraient pas dans le champ d'investigation des Comités.

92 Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2017*, 4-11 ('II.1. Une plainte concernant trois opérations du SGRS').

Un premier briefing général a rapidement été organisé, associé à toute une série de devoirs d'enquête. L'enquête s'est poursuivie en 2019.

I.6.5. LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT SUR LE SCIENTIFIQUE PAKISTANAIS KAHN

Un article de presse[93] 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 avait séjourné en Belgique à la fin des années 60 et au début des années 70.

Une des questions qui se posaient était de savoir si, à l'époque, les services de renseignement belges avaient suivi cette problématique. À l'initiative d'un parlementaire, la Commission de suivi de la Chambre a chargé le Comité permanent R, le 12 juin 2018, d'étudier la thématique. Le 2 juillet, l'enquête 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*' a été ouverte.

Divers devoirs d'enquête ont été effectués au second semestre 2018 et cette enquête a été finalisée début 2019.

I.6.6. CARLES PUIGDEMONT ET LES ÉVENTUELLES ACTIVITÉS MENÉES PAR DES SERVICES DE RENSEIGNEMENT ÉTRANGERS EN BELGIQUE

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. Quelques jours plus tôt, une balise de

93 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.

géolocalisation avait été retrouvée, dissimulée sous le véhicule de l'intéressé.[94] Après avoir détecté ce dispositif, les conseillers de M. Puigdemont ont 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 ont 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 (VSSE et SGRS) face aux activités éventuelles de services de renseignement et de sécurité étrangers sur le territoire belge lors du séjour de M. Puigdemont en Belgique.

Divers devoirs d'enquêtes ont été effectués au second semestre 2018. Cette enquête a elle aussi été clôturée début 2019.

94 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'). On pouvait y lire notamment 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*'.

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 particulières et de certaines méthodes ordinaires, pour lesquelles le Comité permanent R s'est vu confier une mission spécifique. Il est également fait rapport de la manière dont le Comité a rempli sa mission de contrôle juridictionnel sur ces méthodes.

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

Entre le 1er janvier et le 31 décembre 2018, 2445 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 2315 par la VSSE (1971 spécifiques et 344 exceptionnelles) et 130 par le SGRS (102 spécifiques et 28 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

Le nombre total de méthodes mises en œuvre a connu une hausse de plus de 25 % en 2018, passant de 1923 à 2445. L'augmentation qui a été constatée tient surtout à la forte hausse de l'utilisation de méthodes particulières par la VSSE. Ce qui est frappant à cet égard, c'est principalement l'augmentation du nombre de méthodes exceptionnelles. Le SGRS a lui aussi davantage recouru aux méthodes particulières de renseignement en 2018, retrouvant ainsi les chiffres atteints il y a plusieurs années.

Cette tendance s'observe également pour la méthode ordinaire qui consiste à adresser une réquisition à des opérateurs afin d'identifier certains moyens de communication. La VSSE a formulé 6482 réquisitions, ce qui représente une hausse substantielle. En ce qui concerne le SGRS, le nombre de réquisitions a pratiquement doublé.

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

Dans son précédent rapport annuel, le Comité indiquait à ce propos : '*Indépendamment du fait qu'il est pratiquement impossible de comparer les chiffres en matière d'identifications sur base annuelle, le Comité ne peut nier qu'un nombre beaucoup plus élevé d'identifications ont été effectuées depuis l'introduction de la procédure assouplie visée à l'article 16/2 L.R&S. S'appuyant sur sa compétence générale de contrôle, le Comité demandera à la VSSE d'examiner en interne dans quelle mesure ce nombre élevé de réquisitions tient (en partie) à l'assouplissement de la procédure. Il convient à cet égard d'être attentif à la nature des menaces qui justifient les réquisitions et à la question de savoir si et dans quelle mesure de telles réquisitions ont lieu à la demande d'autorités étrangères ou de services partenaires étrangers.*'[95] Le Comité a réitéré cette volonté vis-à-vis de sa Commission parlementaire de suivi.[96] Le Comité n'a cependant pas reçu de réponse (SGRS) ou n'a pas reçu de réponse adéquate (VSSE[97]) à ses questions à ce sujet. Aussi, il a décidé de

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

96 *Doc. parl.* Chambre 2018-19, n° 54-3375/001 (Rapport d'activités 2017 du Comité permanent de contrôle des services de renseignement et de sécurité, Rapport fait au nom de la Commission spéciale d'accompagnement parlementaire du Comité permanent de contrôle des services de police et des services de renseignement et de sécurité).

97 Selon la VSSE, l'augmentation ne s'expliquait que partiellement par un assouplissement de la procédure par le législateur. En outre, le nombre de réquisitions était plus élevé parce qu'elles donnaient plus de résultats (entre autres la suppression du caractère anonyme des cartes prépayées). La dernière raison avancée était que, bien que ces demandes ne relèvent pas de l'art. 16/2 L.R&S, le même format était utilisé pour suivre les targets dans les médias sociaux. C'est pourquoi ces demandes figurent (hélas) également dans les statistiques. Enfin, la VSSE a

reprendre cette thématique dans son 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.'*

Dans ce qui suit, le Comité se limite 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.

II.1.1. MÉTHODES UTILISÉES PAR LE SGRS

II.1.1.1. Les méthodes ordinaires

Identification de l'utilisateur de télécommunications

Par la Loi du 5 février 2016, l'identification de l'utilisateur de télécommunications (p. ex. un numéro de GSM ou une adresse IP) ou d'un moyen de communication utilisé est considérée – sur recommandation du Comité permanent R[98] – 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. La modification a été opérée en insérant un nouvel article 16/2 à la Loi du 30 novembre 1998.[99] Il y est prévu 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. Cet aspect sera également examiné dans l'enquête de contrôle initiée en 2019 (*supra*).

Identification du détenteur d'une carte prépayée

En outre, une nouvelle méthode ordinaire a été introduite à l'article 16/2 L.R&S par la Loi du 1er septembre 2016 (*M.B.* 7 décembre 2016) : *'§ 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*

spécifié que le nombre de réquisitions par les questions émanant de partenaires étrangers n'a pas augmenté proportionnellement au nombre total de réquisitions.

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

99 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 loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.' Comme dans le cadre de l'identification de l'utilisateur de télécommunications ou d'un moyen de communication utilisé, la VSSE et le SGRS doivent tenir un registre reprenant toutes les identifications requises.

Accès aux données PNR

La Loi du 25 décembre 2016 (*M.B.* 25 janvier 2017) 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.[100]

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).

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).[101] En l'absence d'arrêté d'exécution, cette disposition n'est pas encore entrée en vigueur.[102]

100 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.

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

102 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).

Les chiffres

Méthodes ordinaires (SGRS)	**Nombre d'autorisations**
Identification de l'utilisateur de télécommunications	502
Identification du détenteur d'une carte prépayée	0
Recherches ciblées de données PNR	18
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)[103]	8
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)	1
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)	5
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)	45
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)	43
TOTAL	**102**

[103] 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.1.1.3. 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 les méthodes exceptionnelles suivantes :

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)[104]	0
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)	1
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)	1
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	12
S'introduire dans un système informatique (article 18/16 L.R&S)	1
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	13
TOTAL	**28**

II.1.1.4. Les missions et les menaces justifiant le recours aux méthodes ordinaires et particulières[105]

Le SGRS est autorisé à employer les méthodes spécifiques et exceptionnelles dans le cadre de quatre missions, en 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 :

---

104 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.

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

- 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).**

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 (p. 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).

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

NATURE DE LA MISSION	NOMBRE EN 2018
Mission de renseignement	18
Sécurité militaire	19
Protection de secrets	4
Suivi des activités des services étrangers en Belgique	89

Deux tiers des méthodes spécifiques et exceptionnelles sont utilisés 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 2018
Espionnage	85
Terrorisme (et processus de radicalisation)	26
Extrémisme	1
Ingérence	18
Organisations criminelles	–
Autre	0

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.[106] Étant donné que ce n'est pas encore le cas, le Comité réitère cette recommandation.

II.1.2. MÉTHODES UTILISÉES PAR LA VSSE

II.1.2.1. Les méthodes ordinaires

Méthodes ordinaires (VSSE)	Nombre d'autorisations
Identification de l'utilisateur de télécommunications	6482
Identification du détenteur d'une carte prépayée	0
Recherches ciblées de données PNR	7
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

Pour rappel, le Comité se penchera sur la manière dont ces méthodes ont a été mises en œuvre dans l'enquête de contrôle qu'il a initiée en 2019.

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

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)	236
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)	1
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)	81
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)	55
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)	882
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)	776
TOTAL	**1971**

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)	13
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)	25
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)	5

Méthodes exceptionnelles (VSSE)	Nombre d'autorisations
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	80
S'introduire dans un système informatique (article 18/16 L.R&S)	40
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	181
TOTAL	**344**

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 2018
Espionnage	815
Terrorisme (et processus de radicalisation)	1159
Extrémisme	312
Prolifération	5
Organisations sectaires nuisibles	0
Ingérence	24
Organisations criminelles	0
Suivi des activités des services étrangers en Belgique	(Inclus dans les chiffres ci-dessus)
TOTAL	**2315**

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.

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.

INTÉRÊTS PROTÉGÉS	NOMBRE EN 2018
La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel	106
La sûreté extérieure de l'État et les relations internationales	10
La sûreté intérieure *et* extérieure de l'État	1375
La sauvegarde des éléments essentiels du potentiel économique et scientifique	3
Activités des services de renseignement étrangers	821
TOTAL	**2315**

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[107], mais d'autres priorités ont eu raison de ce projet. Le

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

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.'*

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 2018.

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*[108] et un contrôle *a posteriori*.[109] 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

---

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

109 *'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.'*

méthodes exceptionnelles. Un rapport en est fait à l'intention du Comité, ce qui lui permet d'avoir une meilleure vue sur ces méthodes.[110]

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

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.

110 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 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.

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) ;
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	2013	2014	2015	2016	2017	2018
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	0	3	2	1	0	0
4. Information complémentaire de la Commission BIM	0	0	0	0	0	0
5. Information complémentaire du service de renseignement	0	1	1	4	0	0
6. Mission d'enquête confiée au Service d'Enquêtes R	50	54	48	60	35	52
7. Audition membres de la Commission BIM	0	0	2	0	0	0
8.Audition membres des services de renseignement	0	0	2	0	0	0
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	9	3	3	6	9	4
12. Cessation partielle de la méthode	5	10	13	4	6	6
13. Levée (partielle) de l'interdiction de la Commission BIM	2	0	4	11	0	0
14. Non compétent	0	0	0	0	0	0
15. Autorisation légale/Non- cessation de la méthode/Non-fondement51	7	4	6	2	1	1
Avis préjudiciels	**0**	**0**	**0**	**0**	**0**	**0**
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 2018 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 légalité de la méthode concernant les techniques utilisées, les données collectées, la durée de la mesure et la nature de la menace ;
- La légalité de l'exécution d'une méthode légale ;
- Les conséquences d'une méthode (mise en œuvre) illégale(ment).

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

Une méthode sans décision préalable

Dans le dossier 2018/7250, le service de renseignement concerné avait lui-même constaté une irrégularité lors d'un contrôle interne, en l'occurrence une réquisition à un fournisseur en vue d'obtenir des données d'identification et de localisation en l'absence de toute décision du dirigeant du service. En outre, la méthode portait sur un journaliste, ce qui aurait requis l'avis préalable de la Commission BIM. Informée de ce qui précède, la Commission BIM a suspendu la méthode. Le Comité a confirmé cette décision et fait procéder à la destruction des données collectées dans le cadre de la réquisition.

Pas de décision du dirigeant du service

Un service de renseignement souhaitait mettre en œuvre une méthode spécifique donnée à compter d'une date bien déterminée, et ce pendant deux mois. Un agent de ce service a toutefois avancé de quelques jours la date de début de mise en œuvre de la méthode. Le Comité a décidé '*que les "rectifications" effectuées par un agent de la VSSE n'ont pas été contresignées par l'administrateur général lui-même et n'ont en conséquence aucune valeur légale*'. Les données qui ont été collectées avant la date initialement validée par le dirigeant du service étaient donc illégales. De surcroît, il n'a pas été automatiquement mis fin à la méthode au terme du délai prévu, la méthode ayant été maintenue deux jours supplémentaires. Ces données n'ont pas non plus été collectées légalement (2018/6794).

Légalité de la méthode concernant les techniques utilisées, les données collectées, la durée de la mesure et la nature de la menace

Défaut de motivation de la décision

Lorsque le service de renseignement concerné a signalé à la Commission BIM qu'une partie de la motivation initiale d'une méthode spécifique ne correspondait pas à la réalité, la commission a revu sa décision et a suspendu la méthode (dossier 2018/7684). Le Comité a lui aussi constaté que la motivation de la décision MRD en question contenait de très nombreuses inexactitudes. '*Dat de onjuistheden in de motivering van die aard zijn dat zij de motivering zelf fundamenteel en ernstig aantasten. Aangezien daardoor moet worden vastgesteld dat niet is voldaan aan artikel 18/3 W.I&V, dat onder andere stelt dat de beslissing van het diensthoofd de feitelijke omstandigheden die de specifieke methode rechtvaardigen (…) moet vermelden. […] Aangezien de motiveringsverplichting is voorgeschreven op straffe van een onwettigheid.*'[111] Par conséquent, les données collectées devaient être détruites.

Un objet erroné

Dans le dossier 2018/7167, il est apparu que le service de renseignement avait indiqué par mégarde un numéro de téléphone erroné, tant dans la décision que dans la réquisition adressée à l'opérateur. Le service s'en est lui-même aperçu, a suspendu la méthode et en a avisé la Commission BIM. Celle-ci a suspendu à son tour la méthode, après quoi le Comité a décidé que les données collectées illégalement devaient être détruites.

La durée d'une mesure

Un service de renseignement souhaitait procéder à la prise de connaissance de données de communication et de localisation pendant exactement un an (dossier 2018/7464). Au vu de la nature de la menace, il s'agissait de la période maximale autorisée. Mais la loi stipule que cette période d'un an doit être calculée à partir du moment où la décision a été prise par le dirigeant du service (art. 18/8 § 2, alinéa 1er, 3° L.R&S). La date de début ne peut donc pas être choisie librement si l'on veut disposer de données d'une année complète. Résultat : la méthode a dû être 'écourtée', de sorte que le début se situe au moment de la décision du dirigeant du service et la fin, précisément un an avant.

---

111 *'Que les inexactitudes dans la motivation sont de nature à porter fondamentalement et sérieusement atteinte à la motivation même. Étant donné qu'il faut donc constater qu'il n'est pas satisfait à l'article 18/3 L.R&S, qui dispose notamment que la décision du dirigeant du service doit mentionner les circonstances de fait qui justifient la méthode spécifique'. […] Dans la mesure où l'obligation de motivation est prescrite à peine de nullité'.* (traduction libre)

Le même problème s'est posé dans le dossier 2018/7493 : un service de renseignement souhaitait obtenir des informations sur un numéro de téléphone, et ce pour une durée de neuf mois. Au vu de la menace (espionnage), ce délai était autorisé, mais il commençait obligatoirement à courir à compter du moment où la décision a été prise (art. 18/8 § 2, 2°, L.R&S). Une omission du service a eu pour conséquence que le recueil de données téléphoniques n'était pas couvert par une méthode légale pendant une durée de six jours.

Dans un autre dossier (2018/7470), le problème était que la décision même ne mentionnait pas explicitement le délai souhaité pour le recueil de données spécifiques. '*[Q]ue la méthode précise une période en se référant à la période d'une autre méthode*'. Dans cette autre méthode particulière de renseignement, une période était bel et bien déterminée, si bien que le Comité avait l'assurance de la durée proposée. En outre, la mention du délai n'est pas prescrite à peine de nullité : '*Considérant qu'en vertu de l'art. 18/3, § 2, alinéa 1er, 5° de la L.R&S, la décision du dirigeant du service mentionne la période pendant laquelle la méthode spécifique peut être appliquée, à compter de la notification de la décision à la Commission ; Considérant cependant que seules les mentions visées aux 1° à 4°, 7°, 9°, 10°, 11° et 14° de l'article 18/3, § 2, alinéa 1er, de la L. R&S sont prescrites sous peine d'illégalité*. La méthode était donc légale, mais le Comité fait néanmoins part de sa préoccupation dans les termes suivants : *'Considérant, in fine, que le procédé consistant à ne pas mentionner de période propre à la méthode, mais à faire référence à celle d'une autre méthode en cours, non simultanée de surcroit, ne permet pas au Comité permanent R de contrôler de facto, d'une part, le principe de proportionnalité devant être respecté pour toute méthode et, d'autre part, le respect de l'article 18/8 de la L. R&S ; Considérant que le procédé critiqué nuit par conséquent au principe général de bonne administration et doit être évité*'.

L'objet de la méthode

Le dossier 2018/7464 décrit ci-avant présentait une autre lacune. La décision ne faisait pas mention du numéro de GSM sur lequel porterait la méthode. '*Considérant qu'en vertu de l'art. 18/3, § 2, alinéa 1er, 2° de la L. R&S, la décision du dirigeant du service doit mentionner, sous peine d'illégalité, l'objet sur lequel la méthode spécifique peut être appliquée ; qu'en l'espèce, l'objet n'est pas mentionné*'.

Légalité de l'exécution d'une méthode légale

Différence entre la décision du dirigeant du service et la réquisition

Dans quatre décisions, il est apparu que l'autorisation du dirigeant du service pour la mise en œuvre d'une méthode spécifique ou exceptionnelle était parfaitement légale, mais qu'un problème se posait au niveau de l'exécution, en ce sens que la réquisition des données n'était pas conforme au mandat initial.

Dans le dossier 2018/6951, le Commission BIM avait ainsi remarqué une différence entre la décision du dirigeant du service de procéder à une prise de connaissance de moyens de communication et la réquisition adressée à l'opérateur : les deux documents visaient partiellement une autre période. Par conséquent, le Comité a décidé que les données qui portaient sur les jours tombant en dehors de la période prévue initialement avaient été collectées illégalement.

Dans le dossier 2018/7107, la décision du dirigeant du service présentait une différence avec la réquisition adressée à l'opérateur. Ici aussi, le Comité a décidé que toutes les données collectées qui sortaient du cadre de la décision devaient être détruites.

Dans le dossier 2018/7769, le dirigeant du service a autorisé la collecte de données d'un numéro de compte bancaire spécifique. Cependant, la réquisition qui a ensuite été adressée à l'institution bancaire avait une portée plus large : le service réclamait tous les numéros de comptes bancaires, les coffres forts et les instruments financiers du target. Aussi, le Comité a constaté que seule la réquisition des données du numéro de compte bancaire était légale.

Dans le cadre d'une méthode spécifique, un service de renseignement a reçu d'une autre instance des données non sollicitées sur le contenu de conversations, et pas seulement les métadonnées souhaitées (dossier 2018/7650). Le service de renseignement a mis de côté le contenu des conversations et en a avisé la Commission BIM, qui a interdit l'exploitation de ces données. Le Comité est arrivé à la conclusion suivante : '*Considérant, après une enquête menée conformément à l'article 43/5 §§ 1er et 2 de la L.R&S, qu'il apparaît que dans le réquisitoire adressé à [X] en exécution de la décision précitée du dirigeant du service, il n'est fait aucune mention d'une interception téléphonique en application de l'article 18/17, § 1er, de la L.R&S et que la mise en œuvre de cette méthode repose exclusivement sur une erreur de la [X] ; que cela exonère [le service de renseignement] de toute responsabilité ; que de surcroît, [ce service] a sollicité immédiatement [X] d'interrompre cette méthode dès qu'[il] en a eu connaissance ; Considérant que les données de communications téléphoniques interceptées ont été communiquées illégalement [aux services de renseignement] à défaut de décision valable.*'

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

Dans dossier (2018/7250) déjà mentionné sous le point 'une méthode sans décision valable', dans lequel des données collectées sur la base d'une réquisition illégale ont dû être détruites, il s'est en outre avéré que la méthode avait donné lieu à la rédaction de deux rapports de renseignement. Le Comité a recommandé '*que les deux rapports, non référencés, ainsi que tout autre document y faisant référence, traitant des résultats du réquisitoire […] ne puissent pas être exploités et soient détruits*'.

II.3. CONCLUSIONS ET RECOMMANDATIONS

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

- Le SGRS s'est, comme toujours, davantage concentré sur l'espionnage, ensuite sur le terrorisme et l'ingérence. La VSSE a, quant à elle, focalisé son attention sur le terrorisme, suivi par l'espionnage et l'extrémisme.
- En 2018 également, le nombre de méthodes particulières mises en œuvre par la VSSE a poursuivi sa courbe ascendante marquée. Proportionnellement, l'augmentation concerne surtout les méthodes exceptionnelles.
- Le SGRS a lui aussi eu recours à davantage de méthodes particulières de renseignement en 2018 et contredit ainsi la tendance baissière de ces dernières années. Le SGRS continue toutefois d'employer nettement moins de MRD que la VSSE.
- Même constat en ce qui concerne les réquisitions adressées à des opérateurs dans le cadre de méthodes ordinaires aux fins d'identification de moyens de communication donnés : la VSSE a formulé 6482 réquisitions en 2018, et le SGRS, 502. Le Comité ne peut nier que depuis l'introduction de la procédure assouplie visée à l'article 16/2 L.R&S, les services ont de nouveau procédé à beaucoup plus d'identifications. Le Comité n'a reçu aucune réponse (SGRS) ou aucune réponse adéquate (VSSE) à ses questions à ce propos. Il a donc décidé de reprendre cette thématique dans une enquête de contrôle initiée en 2019.
- Contrairement à la mise en œuvre des méthodes particulières, le Comité ne dispose pas des chiffres relatifs à la menace visée et aux intérêts à défendre en ce qui concerne les méthode ordinaires visées à l'article 16/2 L.R&S. Le Comité recommande aux services de consigner également ces données et de les tenir à la disposition du Comité permanent R.
- Le Comité n'a dû constater une illégalité que dans 11 dossiers. Ainsi, le nombre de décisions prises par le Comité continue à diminuer, et ce malgré l'augmentation significative du nombre de MRD mises en œuvre. En outre, toutes les saisines, à une exception près, résultent d'une suspension décidée par la Commission BIM. L'analyse de la jurisprudence montre que dans plusieurs cas, la décision d'utiliser une MRD était parfaitement légale, mais qu'un problème se posait au niveau de l'exécution, en ce sens que la réquisition des données n'était pas conforme au mandat initial. D'autres illégalités concernaient un défaut de motivation, l'absence de décision préalable par le dirigeant du service ou encore un objet erroné de la méthode, cas dans lesquels le Comité a décidé que les données collectées illégalement devaient être détruites.

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

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

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

En 2010, la Loi a encore été modifiée[112] : outre '*l'interception, l'écoute, la prise de connaissance ou l'enregistrement*', le SGRS a pu, à partir de ce moment-là, '*rechercher*' des communications. Avant de procéder à l'interception, à l'écoute, à la prise de connaissance ou à l'enregistrement, le SGRS doit, en effet, être en mesure de surveiller l'ensemble du spectre électromagnétique et le cyberespace, par exemple pour rechercher de nouvelles possibilités (d'exploitation) ou pour disposer de suffisamment d'informations afin de s'assurer de la légalité de certaines interceptions.

---

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

En 2017, les compétences du SGRS ont été étendues pour la troisième fois, tout comme la mission de contrôle du Comité permanent R.[113] La première partie de ce chapitre revient brièvement sur la modification de la loi, tandis que la seconde partie propose un résumé de la manière dont le Comité a assuré sa mission de contrôle en 2018.

III.1. LES COMPÉTENCES DU SGRS ET LA MISSION DE CONTRÔLE DU COMITÉ PERMANENT R[114]

En 2017, la compétence du SGRS dans le cadre des interceptions de sécurité a été élargie. Depuis lors, les interceptions peuvent porter sur des communications '*émises ou reçues à l'étranger*'. Avant la modification de la loi, les interceptions étaient limitées aux communications émises à l'étranger. De plus, cette possibilité vaut pour presque toutes les missions du SGRS.[115] Il est d'ailleurs intéressant d'observer que les descriptions des missions ont, elles aussi, été élargies par la même modification de loi.[116]

En outre, la loi introduit deux autres méthodes, à savoir l'intrusion dans un système informatique à l'étranger[117] et la prise d'images animées'.[118]

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

Le contrôle *préalable* aux interceptions, prises d'images fixes ou animées s'effectue sur la base d'une liste établie annuellement.[119] Cela signifie qu'en plus du plan d'interception annuel, le SGRS doit également élaborer un plan d'intrusion et d'images. Le SGRS y dresse une liste d' '*intrusions dans leurs systèmes informatiques ou de prises d'images fixes ou animées dans le courant de l'année à venir. Ces listes justifieront pour chaque organisation ou institution la raison pour laquelle elle fera l'objet d'une interception, intrusion ou prise d'images*

113 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 46-47.

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

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

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

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

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

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

fixes ou animées en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°, et mentionneront la durée prévue' (art. 44/3 L.R&S). Le SGRS doit envoyer ces listes au ministre de la Défense au mois de décembre pour autorisation. Le ministre prend une décision endéans les dix jours ouvrables et doit la communiquer au SGRS[120], qui transmet à son tour les listes pourvues de l'autorisation ministérielle au Comité permanent R.[121]

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

Le contrôle réalisé *après* l'exécution a été sensiblement renforcé. Il s'effectue '*sur base de listes mensuelles des pays ou des organisations ou institutions ayant effectivement fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images durant le mois écoulé'* et qui justifient '*la raison pour laquelle l'écoute, l'intrusion ou la prise d'images a été effectuée en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°*'. Ces listes doivent être notifiées au Comité permanent R. Le contrôle *ex post* s'effectue aussi sur 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.*' Mais un tel arrêté n'a pas encore été pris, ce que le Comité recommande de faire le plus rapidement possible. Le Comité doit de toute manière motiver sa décision de manière circonstanciée et la communiquer au ministre et au SGRS.

---

120 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.

121 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 la méthode. Le SGRS communique cette décision le plus rapidement possible au Comité permanent R.

III.2. LES CONTRÔLES EFFECTUÉS EN 2018

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

Le Comité permanent R a formulé, une série de remarques importantes concernant le 'Plan d'interception 2017'. Les principales remarques portaient sur les différences en termes de priorité entre, d'une part, le Plan Directeur du Renseignement[122] et, d'autre part, les interceptions SIGINT prévues ainsi que le caractère trop général de la description des organisations et institutions qui feraient l'objet d'interceptions. Dans le 'Plan d'interception 2018', qui a été transmis au Comité fin avril 2018, 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.

À la mi-février 2018, le Comité permanent R a également reçu le plan d'intrusion et de prise d'images, qui s'est avéré être plutôt sommaire. 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

Fin 2018, le Comité a visité les installations d'où sont effectuées les interceptions. Le Comité en a profité pour contrôler la concordance entre les targets autorisés dans le plan d'interception et les interceptions effectuées à ce moment-là. Aucune irrégularité n'a été constatée.

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

Le Comité a reçu neuf '*listes mensuelles*[123] *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*

122 Il s'agit d'un plan établi par la Direction Intelligence du SGRS reprenant les pays à suivre et leur degré de priorité.

123 Ces neuf rapports portaient sur les douze mois de l'année.

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°.

Le contrôle des listes mensuelles d'intrusions et de prises d'images sera effectué dans le cadre de 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.'*

Comme l'exige la loi, le Comité a également procédé à la vérification des journaux de bord obligatoires dans le cadre des interceptions. Seules quelques irrégularités d'ordre administratif ont été relevées.

Enfin, le Comité a effectué pour la première fois un contrôle sur les produits d'analyse réalisés dans le cadre d'une coopération SIGINT au niveau international.

III.2.4. CONSTATATIONS ET CONCLUSIONS

Au cours des réunions de travail et des inspections, le Comité a pu constater que le SGRS mettait tout en œuvre pour poursuivre les réformes initiées au niveau de la coopération nationale et internationale ainsi qu'au niveau technique.

Afin d'atteindre ses objectifs et d'être en mesure d'accomplir ses missions légales, le SGRS doit pouvoir disposer de moyens humains et techniques suffisants en matière de SIGINT. Autre constat dressé en 2018 : le recrutement de personnel chargé des traductions doit constituer une priorité à cet égard.

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

Comme mentionné dans un chapitre précédent[124], 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, vu 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 le Comité rappelait également 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[125] 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 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

124 Voir 'Chapitre I.2. Les activités du SGRS dans une zone d'opération à l'étranger'.

125 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.

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 est 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 CHOD et au Comité permanent R un rapport sur toute mission d'enquête. Le Comité en a reçu quelques-uns en 2018. L'analyse de ces rapports fera l'objet d'un examen ultérieur.

IV.2. CONTRÔLE DES FONDS SPÉCIAUX

Au nom de la Chambre des représentants, la Cour des comptes contrôle l'utilisation des moyens financiers par les services publics. Elle 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 compter de l'arrêt des comptes de 2018.

Le contrôle des fonds spéciaux du SGRS est effectué par un représentant du Cabinet du ministre de la Défense, et ce à raison de quatre fois par an. Depuis 2010, ce contrôle se déroule en présence du président du Comité permanent R. En 2018, le président a assisté à ces quatre contrôles.

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.

Auparavant, deux directives obligeaient la VSSE à informer le ministre de la Justice lorsque des responsables politiques faisaient l'objet d'activités de renseignement : une directive ministérielle du 25 mai 2009 – établie dans la foulée des recommandations du Comité permanent R émises dans le cadre

d'une enquête précédente[126, 127] – et une instruction interne du 27 mars 2012. Conformément à la directive du 25 mai 2009, le ministre de la Justice devait être informé chaque fois que le nom d'un député siégeant au Parlement fédéral était cité dans un rapport. Le champ d'application de l'instruction interne du 27 mars 2012 était à la fois plus étroit et plus large que celui de l'instruction ministérielle : d'une part, cette instruction ne portait que sur des mentions dans des rapports des services extérieurs de la VSSE, mais, d'autre part, sur tous les ministres et mandataires politiques, y compris ceux des Communautés et des Régions.[128]

Depuis le 1er janvier 2018, une nouvelle note de service datée du 13 décembre 2017 est d'application au sein de la VSSE. 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 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.

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*'.[129] Dans le cadre de l'obligation de notification, le Comité a été informé par la VSSE des deux types de rapports.

Malgré ses demandes répétées, le Comité n'a reçu aucune information du SGRS en ce sens.

Le Comité permanent R a l'intention de soumettre ces dossiers à un contrôle de légalité, et ce de manière aléatoire.

---

126 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.).

127 La recommandation était formulée comme suit : *'De manière plus générale, le Comité permanent R souhaite que la Sûreté de l'État élabore des directives claires et univoques quant au recueil, au traitement, à la consultation (y compris le cloisonnement interne éventuel), au stockage et à l'archivage des données de certaines catégories de personnes qui assument ou ont assumé des responsabilités particulières. Lors de l'élaboration de ces directives et du suivi concret des (ex-)mandataires politiques, la Sûreté de l'État doit tenir compte des indications fournies dans l'arrêt que la Cour européenne des droits de l'homme a rendu dans l'affaire Segerstedt-Wiberg and others'.*

128 Pour plus de détails à ce propos, voir : COMITÉ PERMANENT R, *Rapport d'activités 2013*, 37 et suiv. ('II.4. Le suivi de mandataires politiques par les services de renseignement'). Voir également COMITÉ PERMANENT R, *Rapport d'activités 2013*, 25 et suiv. ('II.2. Notes secrètes sur l'Église de Scientologie dans la presse') et 31 et suiv. ('II.3. Un informateur au sein du Vlaams Belang ?').

129 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'.

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.

Des décennies durant, toutes sortes de théories ont été émises sur la cause de ce crash.[130] Dans une publication de Susan Williams, enquêtrice à l'Université de Londres[131], différentes hypothèses ont été examinées ; l'auteur a conclu que tous les indicateurs convergent vers une intervention délibérée d'un ou de plusieurs avions. Des noms de Belges qui étaient actifs dans la région ont également été cités. Williams a plaidé pour que toute la lumière soit faite sur ce crash en ouvrant les '*intelligence, security and defence archives*' des pays impliqués dans le conflit qui faisait rage à ce moment-là au Congo, tels que les États-Unis, le Royaume-Uni, la France, l'Allemagne, l'Afrique du Sud, mais aussi la Belgique.

L'ancien Secrétaire général des Nations Unies Ban Ki-Moon a repris cette idée et a ouvert une nouvelle enquête sous la direction de la 'Personnalité éminente', Mohamed Chande Othman. Le 24 décembre 2017, les Nations Unies ont adopté une résolution à ce sujet.[132] Dans cette résolution, 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 Juge Othman souhaitait également que les personnes désignées par les États membres lui fassent part des écueils qu'ils avaient rencontrés au cours de leurs enquêtes respectives (p. ex. un refus d'accès à certaines archives).

Le 16 avril 2018, les ministres de la Justice et de la Défense ont désigné Guy Rapaille, 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. Le Président de la Commission de suivi a été informé de ces désignations en avril 2018. Le président du Comité s'est chargé du volet des informations classifiées provenant des archives de la Sûreté de l'État et du Service Général du Renseignement et de la Sécurité, tandis que le

130 Notamment par l'enquête de G. BJÖRKDAHL (J. BORGER, *The Guardian*, 17 Aug 2011, 'Dag Hammeskjöld : evidence suggests UN chief's plan was shot down').

131 S S. WILLIAMS, *Who killed Hammarskjöld ? The UN, the cold war and white supremacy in Africa*, Hurst Publishers, Londres, 2016.

132 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).

Prof. Quanten a examiné les archives de la Défense. Fin septembre 2018, ils ont adressé leur rapport aux Nations Unies en concluant que *'after a thorough and meticulous analysis of these archives, is that they do not contain any direct information related to the death of Dag Hammerskjöld. Although, some elements which may shed an additional light on the proposed research, have been selected'*.

Début novembre 2018, le Juge Othman a transmis un premier rapport intermédiaire à l'Assemblée générale des Nations Unies.[133] Il est notamment apparu qu'aucun expert n'avait été désigné ni par l'Afrique du Sud ni par le Royaume-Uni. En ce qui concerne le volet belge, il était mentionné que les deux experts *'provided a comprehensive interim report indicating the substantial work undertaken by them. The interim report confirms that full access*[134] *was given by Belgium to all files and archives kept by the Ministry of Defence, the State security Service (VSSE) and the General Intelligence and Security service (GISS, military intelligence service). The report observes that the mandate has not covered a review of the archives of non-state actors or private organisations. The interim report from Belgium identifies information relevant to the presence of foreign paramilitary and intelligence personnel in and around the Congo at the relevant time, as well as to the capacity of the aerial forces of Katanga*.'[135]

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

---

133 Voir : www.hammarskjoldinquiry.info/pdf/ham_187_EP_interim_report_081118.pdf. Le rapport a été présentée oralement le 3 décembre 2018 (Oral briefing by Mr. Miguel de Serpa Soares, Under-Secretary-General for Legal Affairs and United Nations Legal Counsel). La thématique a fait une nouvelle fois l'objet de publications début 2019 (E. GRAHAM HARRISON et al., *The Observer*, 12 Jan 2019, 'Man accused of shooting down UN chief').

134 Le rapport belge établissait toutefois que '*the searching of archives of the military intelligence service GISS and of het Ministry of Defence has yielded less useful documentation than at the State Security Service, can be called somewhat astonishing. […] It should be noted that, at this stage, all GISS sub-archives have not yet been fully investigated*.'

135 Voir : www.hammarskjoldinquiry.info/pdf/ham_187_EP_interim_report_081118.pdf.

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. NOUVEAUX INSTRUMENTS JURIDIQUES EUROPÉENS ET LEURS IMPLICATIONS IMPORTANTES AU NIVEAU NATIONAL

Le 4 mai 2016, deux instruments juridiques importants ont été publiés au Journal Officiel de l'Union européenne concernant le traitement des données à caractère personnel : le Règlement Général sur la Protection des Données 2016/679 (RGPD)[136] et la Directive 2016/680 (Directive).[137] Ces deux instruments règlent la manière dont les acteurs publics et privés doivent opérer lorsqu'ils collectent, sauvegardent, conservent et communiquent des données à caractère personnel : Quand un traitement est-il loyal et licite ? Quels sont les droits de la personne concernée et quels sont les exceptions à ces droits ? Qui est le responsable du traitement et le sous-traitant ? Les données à caractère personnel peuvent-elles être transmises à des pays tiers ? Qui est l'autorité de contrôle ? Quelles sanctions sont possibles en cas d'infraction ?…

Le RGPD, qui est entré en vigueur le 25 mai 2018, et la Directive ont donné lieu à quelques modifications de loi substantielles au niveau national. Ainsi, la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des

136 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.

137 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.

traitements de données à caractère personnel a été abrogée, et la Commission de la protection de la vie privée (Commission vie privée) a été remplacée par l'Autorité de protection des données (APD) par la Loi du 3 décembre 2017 (APD).[138] Une toute nouvelle Loi relative à la protection des données a été votée ultérieurement.[139]

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 protection des données pour les traitements de données à caractère personnel qui entrent dans le cadre de la 'sécurité nationale'. De tels traitements ne relèvent pas du droit européen et ne sont donc pas inclus dans le RGPD ou la Directive. Le législateur a néanmoins choisi de soumettre, dans une certaine mesure, les services qui effectuent ce genre de traitements aux mêmes règles en matière de protection des données.

En réalité, c'était déjà le cas auparavant : la Loi de 1992 relative à la vie privée ne s'appliquait que partiellement aux traitements effectués par la VSSE, le SGRS, les officiers de sécurité du Comité permanent R et son Service d'Enquêtes. Il n'était pas étonnant que certaines règles en matière de protection des données s'appliquaient à ces services, et pour cause, la Belgique est liée par la Convention n°108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.[140] En ce qui concerne la Belgique, cette Convention s'applique également aux services qui traitent des données en matière de sécurité nationale.[141] Elle renferme des règles spécifiques relatives aux organes de contrôle indépendants et à l'échange d'informations au-delà des frontières nationales.

La section suivante explique tout d'abord le nouveau rôle du Comité permanent R. Ce rôle est décrit dans la Loi portant création de l'Autorité de protection des données (Loi APD), dans la Loi relative à 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), qui a subi une série de modifications. Le Comité a été impliqué, dans un premier temps de manière informelle et ensuite formelle, dans la confection de cette nouvelle réglementation.[142] Comme il apparaîtra par la suite, le

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

139 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.

140 Https ://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/convention_108.pdf.

141 Https ://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/protocole_additionnel_convention_108.pdf.

142 L'avis du Comité rendu à la demande de la Commission de la Justice de la Chambre peut être consulté sur le site Internet du Comité (www.comiteri.be). Le 26 juin 2018, le président du Comité a exposé son avis oralement lors d'une séance de la commission compétente de la Chambre. Voir également à propos de cet avis le 'Chapitre VII. Avis'.

Parlement a apporté quelques modifications au texte. Néanmoins, plusieurs points importants de la nouvelle réglementation devront être encore modifiés ou complétés. La seconde partie de ce chapitre sera consacrée, même brièvement, au Comité permanent R en tant que sous-traitant de données à caractère personnel. Enfin, les premières activités du Comité en tant qu'Autorité de contrôle compétente' (ACC) seront expliquées.

V.2. NOUVELLES MISSIONS POUR LE COMITÉ EN SA QUALITE D'AUTORITÉ DE CONTRÔLE COMPÉTENTE

Les nouvelles missions du Comité et la manière dont elles doivent être accomplies, découlent de diverses dispositions de la Loi relative à la protection des données et de la Loi Contrôle. Ces dispositions sont résumées ci-après. Il convient toutefois de préciser au préalable pour quels traitements le Comité est compétent et comment il se situe par rapport aux autres Autorités de contrôle compétentes.

V.2.1. À L'ÉGARD DE QUELS TRAITEMENTS DE QUELS SERVICES ET DE QUELLES PERSONNES ?

Le Comité permanent R est compétent pour contrôler tous les traitements ou certains traitements de données à caractère personnel par toute une série de services, autorités et personnes. Ceux-ci sont énumérés au Titre 3 de la Loi relative à la protection des données.

- Le sous-titre 1. porte spécifiquement sur tous les traitements effectués par la VSSE et le SGRS (art. 73 et 95 LPD) ;
- Le sous-titre 3. vise tout traitement de données à caractère personnel dans le cadre des habilitations, attestations et avis de sécurité visés par la Loi du 11 décembre 1998 par l'Autorité nationale de sécurité (ANS) et chaque autorité membre de cette autorité, les autres autorités de sécurité telles que visées aux articles 15, alinéa 2 et 22*ter* L.C&HS et les officiers de sécurité visés à l'article 13, 1°, L.C&HS ou leurs sous-traitants (art. 107 et 128 LPD)[143] ;
- Le sous-titre 4. s'applique à tout traitement de données à caractère personnel effectué par l'OCAM et ses sous-traitants, '*dans le cadre des missions visées par la loi du 10 juillet 2006, ainsi que par ou en vertu de lois particulières*'

[143] Ce sous-titre s'applique également à tout traitement de données à caractère personnel effectué par l'Organe de recours dans le cadre des procédures de recours visées par la Loi du 11 décembre 1998 portant création de l'Organe de recours. Toutefois, le Comité ne remplit pas le rôle d'Autorité de contrôle compétente dans ce contexte (art. 128 § 2 LPD).

(art. 139 et 161 LPD). Les traitements effectués par les services d'appui de l'OCAM ne sont donc pas visés ici ;
- Le sous-titre 5. s'applique à tout traitement de données à caractère personnel effectué par l'Unité d'information des passagers (UIP) dans le cadre des finalités visées à l'article 8, § 1er, 4°, de la Loi du 25 décembre 2016[144], ou en d'autres termes, les traitements en vue '*du suivi des activités visées 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 renseignements et de sécurité*' (art. 169 et 184 LPD)[145, 146] ;
- Enfin, le sous-titre 6 vise les traitements effectués par la Commission BIM (art. 185 LPD).

Chacun de ces services ou chacune de ces personnes est soumis(e) à des obligations spécifiques en matière de protection des données. Ces obligations sont en grande partie semblables, mais il y a quand même quelques différences. Par exemple, il est uniquement stipulé, en ce qui concerne la Commission BIM, que le Comité permanent R est l'ACC. La Loi relative à la protection des données ne décrit que sommairement les règles que cette commission est tenue de respecter dans le cadre du traitement des données à caractère personnel et des droits du citoyen. Néanmoins, les quelques dispositions générales figurant dans la Loi Contrôle s'appliquent également à la Commission BIM.

V.2.2. QUELLE 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) – qui a succédé à la Commission Vie privée – 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).

144 Voir également le Protocole d'accord du 13 novembre 2018 relatif à la collaboration entre l'Unité d'information des passagers et le SGRS dans le cadre de la loi relative au traitement des données des passagers (Diffusion restreinte, art. 20 AR 24 mars 2000).

145 En ce qui concerne la relation entre le délégué de l'UIP et le Comité permanent R, voir également l'article 27 de l'A.R. relatif à l'exécution de la loi du 25 décembre 2016 relative au traitement des données des passagers, reprenant diverses dispositions concernant l'Unité d'information des passagers et le délégué à la protection des données, *M.B.* 29 décembre 2017.

146 Aucune disposition similaire n'a été reprise dans la LPD pour les autres services que le Comité permanent R doit contrôler. Le Comité part du principe qu'il s'agit d'un oubli.

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, dans certains cas, la possibilité ou l'obligation de coopérer ou encore d'échanger des informations. Ainsi, les articles 98 et 131 LPD disposent que les autres ACC doivent informer le Comité permanent R des infractions à la réglementation en matière de traitement de données à caractère personnel commises par les services de renseignement ou les autorités de sécurité, et ce dès qu'ils en ont connaissance. Les autres ACC doivent également se concerter avec le Comité lorsqu'elles sont saisies dans un dossier susceptible d'avoir des conséquences pour le traitement de données à caractère personnel par une de ces instances.[147] En outre, les ACC doivent, dans certains cas, échanger des rapports d'enquête (*infra*).

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. Cette fonction sera assumée par l'Autorité de protection des données. Par ailleurs, les ACC doivent conclure un protocole afin de réaliser la coopération requise.

Enfin, le législateur a prévu 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 à cet égard est la coopération entre les différentes ACC.

V.2.3. QUELLES SONT LES NOUVELLES MISSIONS ?

V.2.3.1. Effectuer des enquêtes

Qui peut initier une enquête ?

Le Comité peut, d'initiative ou à la demande d'une autorité compétente, enquêter sur les traitements de données à caractère personnel par les services de renseignement (ainsi que par les personnes et les autorités susmentionnées[148]) et leurs sous-traitants (art. 33 L.Contrôle). Il *'surveille [l'application] […] afin de protéger les libertés et les droits fondamentaux des personnes physiques à l'égard dudit traitement.*' (art. 95 et 128 LPD ; voir aussi l'art. 144 LPD).

147 Aucune disposition similaire n'a été reprise dans la LPD pour les autres services que le Comité permanent R doit contrôler. Il s'agit clairement d'un oubli de la part du législateur.

148 L'art. 33 L.Contrôle ne mentionne que les services de renseignement, mais pas les autres personnes et autorités dont le Comité est l'autorité de protection des données compétente. Le Comité part du principe qu'il s'agit d'un oubli.

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 art. 79, 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).[149] 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.[150]

Par ailleurs, l'article 51/1 LPD prévoit que le Comité '*[e]n sa qualité d'autorité de protection des données, […] agit soit d'initiative, soit à la demande d'une autre autorité de protection des données, soit à la requête de toute personne concernée*'. Cette disposition offre donc la possibilité à l'APD, au C.O.C. ou au Comité permanent P de saisir le Comité permanent R. On parlera notamment d'une saisine par l'APD ou par le C.O.C. lorsque l'APD (art. 11 § 5 LPD) ou le C.O.C. (art. 45 § 6 LPD) sera saisi d'une requête ou d'une plainte où le responsable du traitement fait état du fait qu'il traite des données d'un service de renseignement ou de l'OCAM, par exemple.[151] Dans ce cas-là, l'APD ou le C.O.C. ne peut assurer le traitement et doit le renvoyer au Comité permanent R. Le Comité effectuera alors les vérifications nécessaires.

De quelles compétences et possibilités d'enquête le Comité permanent R dispose-t-il ?

Le contrôle sur les traitements de données est effectué *'selon les modalités fixées par la loi du 18 juillet 1991'* (art. 95 LPD; voir également les articles 106, 5°, 161 et 174 LPD). En d'autres termes, le Comité peut faire usage, ici aussi, de toutes les compétences qui lui ont été attribuées dans le cadre de sa mission de contrôle traditionnelle.

En outre, le Comité peut, si nécessaire, coopérer avec les autres autorités de contrôle belges, sans que cela ne porte atteinte *'à l'intégrité physique d'une personne, ou aux missions des services de renseignement et de sécurité et de la loi*

149 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 art. 80, 114, 146 et 174 LPD).

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

151 Le premier paragraphe de l'article 11 LPD ne mentionne que des données des deux services de renseignement et de l'OCAM. Dans le reste de la disposition et à l'article 45, qui est similaire, il est fait mention de '*données à caractère personnel émanant directement ou indirectement des autorités visées au titre 3*'. Ceci semble davantage correspondre à l'intention du législateur.

du 11 décembre 1998' (art. 96 LPD) ou à condition que cela ait lieu '*dans le respect de la loi du 11 décembre 1998*' et '*sans que cela ne porte atteinte aux intérêts visés à l'article 5 de la loi du 11 décembre 1998 portant création d'un organe de recours*' (art. 129 LPD).

Enfin, la Loi relative à la protection des données impose dans deux cas (les autres cas sont clairement oubliés) une obligation de collaboration aux services contrôlés (art. 97 et 130 LPD).

Les décisions du Comité permanent R

Une nouvelle section du Chapitre III de la Loi Contrôle, la Section 4, décrit les décisions que peut prendre le Comité permanent R en sa qualité d'autorité de protection des données (art. 51/3 L.Contrôle). Il peut :

- Conclure que le traitement est effectué en conformité avec les dispositions de la réglementation relative au traitement des données à caractère personnel ;
- Avertir le service concerné ou son sous-traitant du fait qu'un traitement envisagé de données à caractère personnel est susceptible de violer la réglementation relative aux traitements des données à caractère personnel ;
- Rappeler à l'ordre le service concerné ou son sous-traitant lorsqu'un traitement a entraîné une violation d'une disposition de la réglementation relative aux traitements des données à caractère personnel ;
- Ordonner au service concerné ou à son sous-traitant de mettre un traitement en conformité avec les dispositions de la réglementation relative au traitement des données à caractère personnel, le cas échéant, de manière spécifique et dans un délai déterminé ;
- Imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ;
- Ordonner la rectification ou l'effacement de données à caractère personnel ;
- Transmettre le dossier au parquet du procureur du Roi de Bruxelles, qui informe le Comité des suites données au dossier.

La communication et les rapports du Comité permanent R

Diverses règles définissent quelle personne, quels services ou instances le Comité doit informer sur le résultat de ses contrôles.

Ainsi, le rapport relatif à chaque mission d'enquête, ouverte d'initiative ou à la demande d'une autorité compétente, est remis au ministre compétent ou à l'autorité compétente ainsi qu'à la Chambre des représentants (art. 33, alinéa 3 L. Contrôle). Les conclusions de l'enquête sont, selon le cas, communiquées au fonctionnaire dirigeant du service de renseignement ou au directeur de l'OCAM (art. 34, dernier alinéa L. Contrôle) ou – ici aussi, le législateur a oublié de prévoir une réglementation globale – à une autre personne ou un autre service.

En cas d'enquête ou de plainte d'un citoyen, le Comité répond uniquement que *'les vérifications nécessaires ont été effectuées'*.[152] 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).

Si une autre autorité de contrôle est à l'origine de l'ouverture d'une enquête (p. ex. art. 11 § 5, 45 § 6 et 51/1 LPD), le Comité envoie sa '*réponse*' à cette autre autorité qui, à son tour, informe la personne concernée, mais uniquement '*des résultats de la vérification portant sur les données à caractère personnel n'émanant pas du service de renseignement ou de l'OCAM*'.[153]

En outre, les articles 96 et 128 LPD prévoient que *'[d]ans le cadre de l'exercice du contrôle visé à l'article 95, le Comité permanent R communique le résultat de celui-ci en termes généraux aux autres autorités de contrôle compétentes'*. Aucune obligation similaire n'a été introduite pour les enquêtes liées à d'autres instances. De surcroît, il a uniquement été précisé que pour les enquêtes liées aux services de renseignement, les autres ACC ne pouvaient informer la personne concernée des résultats de l'enquête menée par le Comité (art. 95 LPD).

Enfin, il convient de tenir compte de l'article 51/4 L.Contrôle. Conformément à cette disposition, le service de renseignement concerné doit être informé lorsqu'une enquête porte sur un de ses sous-traitants. Cette disposition prévoit également ce qui suit : *'Lorsqu'il en prend connaissance, le Comité permanent R informe également le service concerné des violations de la réglementation relative aux traitements de ses données à caractère personnel par d'autres responsables du traitement'*.

V.2.3.2. Rendre des 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 données et doit donc être distingué de la compétence d'avis générale qui porte, par exemple, sur l'efficacité et la coordination.[154] 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.

---

152 Voir également les articles 80, 114, 146 et 174 LPD. Lors de la clôture d'une enquête 'ordinaire' faisant suite à une plainte, le Comité peut en communiquer le résultat *'en termes généraux'* (art. 34 L.Contrôle).

153 Si la requête ou la plainte ne porte que sur des données à caractère personnel émanant d'un service de renseignement ou de l'OCAM, l'APD ou le C.O.C. répond, après réception de la réponse du Comité permanent R, que les vérifications nécessaires ont été effectuées.

154 Voir à ce propos 'Chapitre VII. Avis'.

V.2.3.3. Assurer, via le Service d'Enquêtes R, la gestion des infractions portées à sa connaissance

Lorsqu'un membre du Service d'Enquêtes R a connaissance d'un crime ou d'un délit, il en dresse un procès-verbal qui est transmis au procureur du Roi (art. 46 L. Contrôle). Cette règle ne s'applique pas aux infractions décrites aux articles 226, 227 et 230 LPD.[155] Dans ces cas de figure, le service informe le Comité permanent R dans les meilleurs délais qu'il '*assure le suivi selon les modalités fixées à l'article 54*[156] *[L.Contrôle]*'.

V.2.3.4. Informer les services contrôlés

Les services contrôlés par le Comité permanent R doivent tenir ou mettre à sa disposition toute une série de données[157], c'est-à-dire :

- De journaux ou d'autres données si un service de renseignement ou la Commission BIM dispose d'un accès direct ou d'une interrogation directe à une banque de données, d'un acteur privé ou public (art. 13 et 47 LPD);
- 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 (art. 89, 122, 155 et 180 LPD) ;
- Un registre reprenant les informations sur les banques de données utilisées ou les activités de traitement menées (art. 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 (art. 91, 124 et 127 LPD[158]).

V.2.3.5. Décider du renvoi d'un Data Protection Officer

Chaque service contrôlé par le Comité est obligé de désigner un délégué à la protection des données (DPO), qui doit pouvoir opérer en toute indépendance. Il ne peut donc pas être sanctionné dans le cadre de l'exercice de ses fonctions. Il ne peut qu'être relevé de sa fonction en cas de faute grave ou si les conditions nécessaires à l'exercice de sa fonction ne sont plus remplies. Il peut s'adresser au Comité permanent R pour contester cette décision (art. 91, 124 et 157 LPD[159]).

---

155 La même exception a été prévue lorsque le Service d'Enquêtes R constate une infraction telle que visée à l'art. 13/1 L.R&S.

156 Selon toute vraisemblance, il s'agit d'une erreur et il convient de se référer à l'art. 51/3 L. Contrôle.

157 Chaque service ne doit pas conserver ou tenir à disposition toutes les données mentionnées ici. Telle n'était probablement pas l'intention du législateur. Cela s'applique manifestement à la Commission BIM, qui ne doit pas communiquer d'informations au Comité permanent R.

158 Aucune disposition similaire n'a été reprise pour l'UIP. Selon toute vraisemblance, il s'agit d'un oubli de la part du législateur.

159 *Idem.*

V.2.3.6. La rédaction d'un rapport annuel

Conformément à l'article 35 § 3 L. Contrôle, 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*'. Une copie de ce rapport est destinée aux ministres compétents et aux deux services de renseignement[160], qui ont la possibilité d'attirer l'attention du Comité permanent R sur leurs observations.

V.3. LE COMITÉ PERMANENT R EN TANT QUE SOUS-TRAITANT DE DONNÉES À CARACTÈRE PERSONNEL

La Loi relative à la protection des données contient une disposition qui permet au Comité permanent R, entre autres autorités publiques, '*dans la mesure nécessaire à l'exercice de [ses] missions, de traiter des données à caractère personnel de toute nature, en ce compris celles qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que les données génétiques et biométriques, les données concernant la santé, celles qui portent sur la vie sexuelle ou l'orientation sexuelle et celles relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes' (…) dans le cadre de ses missions visées à la loi du 18 juillet 1991 organique du contrôle des services de renseignement et de sécurité et de l'Organe de coordination pour l'analyse de la menace, à la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et de l'Organe de Coordination pour l'analyse de la menace, et aux lois particulières*' (art. 185 § 1er LPD).

Afin de garantir la confidentialité et l'efficacité de l'exécution de ces missions, l'accès des personnes concernées à ces données à caractère personnel est limité à ce qui est prévu dans les lois particulières. La personne concernée a néanmoins le droit de demander la rectification ou la suppression d'éventuelles données à caractère personnel incorrectes.

Enfin, l'article 185 § 4 LPD dispose que le Comité '*dans le cadre de [ses] missions d'autorité de contrôle n'est pas soumis au contrôle de l'Autorité de protection des données visée dans la loi du 3 décembre 2017 portant création de l'Autorité de protection des données.*'

La réglementation susmentionnée porte uniquement sur les traitements liés à la sécurité nationale. D'autres traitements, tels que la gestion du personnel en interne, relèvent des règles ordinaires de protection des données.

---

160 Ici non plus, la loi ne fait pas mention, à tort, des autres personnes et autorités reprises au Titre 3 de la Loi relative à la protection des données.

Une dernière remarque porte sur le fait que le Service d'Enquêtes R relève de la responsabilité du C.O.C en sa qualité d'Autorité de contrôle compétente.

V.4. ACTIVITÉS DU COMITÉ PERMANENT R EN SA QUALITÉ D'AUTORITÉ DE CONTRÔLE COMPÉTENTE

V.4.1. TRAVAUX PRÉPARATOIRES

En 2018, le Comité permanent R a mené toute une série d'activités préparatoires afin d'être en mesure d'assumer sa nouvelle tâche et ses nouvelles obligations.

Dans un premier temps, un Data Protection Officer (DPO) a été désigné pour tous les traitements qui ne relèvent pas de la 'sécurité nationale' (par exemple, les traitements effectués dans le cadre de la gestion du personnel et de la logistique).

En outre, le Comité s'est réuni à plusieurs reprises avec trois autres autorités de contrôle compétentes. Au menu des discussions figuraient la rédaction d'un protocole qui développera le 'principe de guichet unique', des accords de travail pratiques et l'échange des meilleures pratiques.

Les premiers accords ont été conclus avec le Comité permanent P afin de concevoir 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 une série de processus de travail internes pour la fonction d'avis et les enquêtes faisant suite aux plaintes introduites par des citoyens.

V.4.2. HUIT AVIS APD

En 2018, le Comité a rendu, seul ou avec le Comité permanent P, huit avis concernant des projets de loi ou d'arrêté. Ces avis peuvent être consultés en intégralité sur le site Internet du Comité. On se limitera ici à une énumération des avis rendus :

- Avis 001/CPR-ACC/2018 du 26 septembre 2018 concernant '*des projets d'Arrêtés royaux relatifs à l'exécution de la loi de 25 décembre 2016 relative au traitement de données des passagers, reprenant les obligations respectivement pour les transporteurs de bus et pour les transporteurs HST distributeurs de tickets HST*' ;
- Avis 002/CPR-ACC/2018 du 26 septembre 2018 concernant '*l'avant-projet de loi concernant l'organisation des services pénitentiaires et le statut du personnel pénitentiaire*', dans lequel figuraient des dispositions en matière de screening des candidats fonctionnaires pénitentiaires ;

- Avis 003/CPR-CPP-ACC/2018 du 26 septembre 2018 concernant le même avant-projet de loi, rendu avec le Comité permanent P puisque cet avant-projet prévoyait que le screening des candidats fonctionnaires pénitentiaires devaient également s'appuyer sur des données émanant de l'OCAM ;
- Avis 004/CPR-ACC/2018 du 1er octobre 2018 concernant '*l'avant-projet de loi portant modification de la loi du 12/12/2013 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 voyages belge*' ;
- Avis 005/CPR-CPP-ACC/2018 du 1er octobre 2018 concernant le même avant-projet, rendu avec le Comité permanent P puisque ce projet portait également sur l'OCAM ;
- Avis 006/CPR-ACC/2018 du 24 octobre 2018 concernant '*l'avant-projet de loi portant des dispositions diverses en matière d'informatisation de la justice et de modernisation du statut des juges consulaires*', dans lequel il était question d'un droit de lecture des services de renseignement dans SIDIS-Suite ;
- Avis 007/CPR-CPP-ACC/2018 du 24 octobre 2018 concernant le même avant-projet de loi, rendu avec le Comité permanent P puisqu'il était question d'un droit de lecture dans SIDIS-Suite pour l'OCAM ;
- Avis 008/CPR-ACC/2018 du 16 novembre 2018 concernant '*l'avant-projet de loi portant des dispositions diverses en matière pénale*', qui comportait de nouvelles méthodes de renseignement ainsi que des mesures de protection et d'appui.

V.4.3. DEUX PLAINTES APD INDIVIDUELLES

En 2018, le Comité a reçu cinq plaintes APD de citoyens concernant d'éventuels traitements de données à caractère personnel par la VSSE et le SGRS. Deux de ces plaintes ont été traitées en 2018, et les plaignants ont été informés que les vérifications requises avaient été effectuées.[161]

161 *'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 DES BANQUES DE DONNÉES COMMUNES

La Loi du 5 août 1992 sur la fonction de police (LFP) a été modifiée en 2016, instaurant une base légale en vue de la création de banques de données communes dans le cadre de la prévention et du suivi du terrorisme et de l'extrémisme pouvant mener au terrorisme.[162] L'idée était de permettre à différents services de partager leurs données et informations afin d'être plus efficaces dans le cadre de la lutte qu'ils mènent contre ces phénomènes.

S'appuyant sur cette possibilité, les ministres de l'Intérieur et de la Justice ont créé, en 2016, la banque de données commune '*foreign terrorist fighters*' (BDC FTF).[163] 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[164] : 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 nouvelle catégorie visant les '*homegrown terrorist fighters*'. Toujours en 2018[165], une banque de données commune distincte a été créée pour 'les propagandistes de haine' (BDC PH). Ces différentes modifications intervenues cette année-là sont explicitées dans la première section de ce chapitre (VI.1).

L'article 44/6 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. Ce contrôle est détaillé dans la deuxième section (VI.2).

---

162 Loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme, *M.B.* 9 mai 2016.

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

164 A.R. du 23 avril 2018 modifiant l'A.R. du 21 juillet 2016 précité et modifiant la banque de données commune '*foreign terrorist fighters*' vers la banque de données commune '*terrorist fighters*', *M.B.* 30 mai 2018 (AR TF).

165 A.R. 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 PH).

Les deux instances ont par ailleurs rendu un avis conjoint sur deux 'déclarations préalables', introduites en 2018 par les deux ministres compétents. Comme la loi l'exige, ces déclarations règlent en détail le fonctionnement de la nouvelle banque de données et de la banque de données élargie. La troisième section résume les avis rendus dans ce contexte (VI.3).

VI.1. LES MODIFICATIONS INTERVENUES EN 2018

VI.1.1. L'ÉVOLUTION DE *FOREIGN TERRORIST FIGHTERS* VERS *TERRORIST FIGHTERS*

La banque de données a été modifiée en ce sens qu'elle est désormais composée de fiches de renseignements concernant les '*foreign terrorist fighters*' (soit la catégorie initiale de 2016) et les '*homegrown terrorist fighters*' (catégorie ajoutée en 2018).

Sous réserve des deux modifications ultérieurement commentées, l'A.R. du 23 avril 2018 n'a pas modifié le fonctionnement de la banque de données commune créée en 2016.[166]

L'élargissement a été jugé nécessaire en raison des nombreux attentats à caractère djihadiste ou liés à l'extrême droite qui ont été perpétrés depuis 2016 en Europe, mais qui n'étaient pas directement liés à une zone de conflit djihadiste. Ainsi, la modification vise à permettre d'inclure également dans la banque de données commune les données et les informations relatives aux '*homegrown terrorist fighters*'.

Il s'agit de toute personne physique ayant un lien avec la Belgique et à propos de laquelle au moins une des deux conditions suivantes est remplie :

a) il existe des indications sérieuses que cette personne a l'intention de recourir à la violence à l'encontre de personnes ou d'intérêts matériels, pour des motifs idéologiques ou politiques, dans le but d'atteindre leurs objectifs par la terreur, l'intimidation ou les menaces ;
b) il existe des indications sérieuses que la personne donne intentionnellement un soutien, notamment logistique, financier ou aux fins de formation ou recrutement, aux personnes visées au a) ou aux personnes enregistrées en tant que FTF et pour lesquelles il existe des indications sérieuses qu'elles ont l'intention de commettre un acte violent (art. 6, § 1er, 1°/1 AR TF).

Les données des personnes répondant à ces conditions peuvent être encodées dans la banque de données. Il en va de même concernant les personnes à propos desquelles il existe de sérieux indices qu'elles puissent remplir ces critères. L'idée

166 Pour un commentaire approfondi sur le fonctionnement des banques de données communes, voir COMITÉ PERMANENT R, *Rapport d'activités 2016*, 129-140 (www.comiteri.be).

est de pouvoir récolter des données ou des informations supplémentaires confirmant ou non que l'intéressé répond aux critères des *terrorist fighters*.

VI.1.2. LA CRÉATION D'UNE BANQUE DE DONNÉES COMMUNE POUR LES PROPAGANDISTES DE HAINE (PH)

Une nouvelle BDC relative aux 'propagandistes de haine' a été créée par l'A.R. du 23 avril 2018 (AR PH).

Cette banque de données est complémentaire à la BDC TF et se concentre plus particulièrement sur l'influence radicalisante qui est souvent à la base du passage au terrorisme ou à l'extrémisme pouvant mener au terrorisme. L'objectif est de mettre en commun, dans la banque de données, les données et les informations relatives aux vecteurs de la radicalisation (personnes physiques, personnes morales, associations de fait), ainsi que l'ensemble des moyens utilisés par ceux-ci.[167] Les données et les informations partagées doivent contribuer à l'analyse, à l'évaluation et au suivi des entités concernées.[168]

La BDC PH vise tout d'abord les personnes physiques ou morales, nonobstant leur nationalité, leur lieu de résidence ou leur siège, qui remplissent les critères cumulatifs suivants :

a) elles ont pour objectif de porter atteinte 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. Il n'est pas nécessaire que l'objectif de porter atteinte soit réalisé, la potentialité de cet objectif étant suffisante ;
b) elles justifient l'usage de la violence (physique, psychique, intra et extra familiale, homophobe, cyberattaques…) ou de la contrainte comme moyen d'action afin de réaliser cet objectif. Le PH manifeste son intention de porter préjudice, ainsi que la justification du recours à la violence ou la force, par le biais d'actions ou de canaux concrets. L'intention doit être extériorisée publiquement (par exemple, via une publication) ;
c) elles propagent leurs convictions aux autres en vue d'exercer une influence radicalisante. Le PH souhaite soutenir ou participer à une radicalisation ;
d) elles ont un lien avec la Belgique.

Les personnes à propos desquelles il existe des indices sérieux qu'elles remplissent ces critères sont reprises pour six mois maximum dans la BDC PH. Passé ce délai, elles sont supprimées, sauf s'il apparaît que l'entité répond aux critères.

---

167 Par exemple, un site Internet, des tracts, des messages radio ou télévisés, des chaînes de radio ou de télévision, des centres de propagandes ou culturels, des locaux….

168 Cette banque de données remplace la précédente '*Joint Information Box*' (JIB) qui était gérée par l'OCAM. La JIB a fait l'objet d'une enquête commune des Comités permanents R et P (COMITÉ PERMANENT R, *Rapport d'activités 2015*, 7-11).

Le fonctionnement de cette banque de données est identique à celui de la BDC TF. Les principaux protagonistes sont les mêmes : les ministres de l'Intérieur et de la Justice ont été désignés comme responsables de traitement, la Police fédérale a été désignée comme gestionnaire (art. 3 AR PH), et l'OCAM, comme responsable opérationnel (art. 4 AR PH). La fonction de conseiller en sécurité et en protection de la vie privée est elle aussi prévue (art. 5 AR PH). Néanmoins, il n'est pas précisé quelle personne ou quel service est appelé(e) à assumer cette mission.

VI.1.3. LA TRANSMISSION DE LA CARTE D'INFORMATION AUX CSIL-R

Une autre adaptation intervenue en 2018 résultait de la création des cellules de sécurité intégrales locales en matière de radicalisme, d'extrémisme et de terrorisme (ci-après 'CSIL-R').[169] La CSIL-R est la plateforme au sein de laquelle des spécialistes de l'administration locale et des organisations de prévention sociale se réunissent afin d'aboutir à une approche orientée sur les cas d'individus radicalisés. L'organisation de la CSIL-R relève de la compétence du bourgmestre. L'article 4 de la loi précitée autorise le chef de corps de la Police locale (ou son représentant à la CSIL-R) à communiquer aux membres de la CSIL-R la carte d'information d'une personne dont le cas est discuté. Une carte d'information est un extrait de la fiche de renseignements et contient les données et les informations strictement limitées aux besoins du destinataire (art. 44/11/3*quater* LFP et art. 11 AR FTF).

VI.1.4. UN ACCÈS DIRECT POUR L'AUTORITÉ NATIONALE DE SÉCURITÉ

Par les A.R. du 23 avril 2018, l'Autorité nationale de sécurité s'est vu attribuer un accès direct aux banques de données, et ce dans le cadre de sa compétence de délivrance des habilitations, attestations et avis de sécurité.

VI.1.5. UNE NOUVELLE DIRECTIVE CONCERNANT L'ÉCHANGE D'INFORMATIONS

Le 22 mai 2018, les ministres de l'Intérieur et de la Justice ont promulgué une circulaire concernant l'échange de informations autour des *terrorist fighters* et

[169] Loi du 30 juillet 2018 portant création de cellules de sécurité intégrale en matière de radicalisme, d'extrémisme et de terrorisme, *M.B.* 14 septembre 2018.

des propagandistes de haine et concernant le suivi de ceux-ci. Cette directive, qui s'est vu attribuer la classification 'Diffusion restreinte', règle en détail le fonctionnement des banques de données communes et définit le rôle de tous les acteurs, tels que les services de police, les services de renseignement, l'OCAM, la *Task Force* locale, la CSIL-R, etc.

VI.2. LA MISSION DE CONTRÔLE

VI.2.1. L'OBJET DU CONTRÔLE

Le C.O.C. et le Comité permanent R ont contrôlé conjointement le suivi réservé à certaines recommandations qu'ils avaient formulées en 2017. Ils ont par ailleurs décidé de vérifier comment les bourgmestres et les tiers étaient informés respectivement par les chefs de corps des Polices locales et les services de base.[170]

VI.2.2. LE SUIVI DES RECOMMANDATIONS FORMULÉES EN 2017

VI.2.2.1. Une base légale pour le traitement des HTF et des PH

Dans leur rapport de 2017, le C.O.C et le Comité permanent R avaient constaté que des données relatives à des 'propagandistes de haine' et à des '*homegrown terrorist fighters*' avaient été traitées en l'absence de nouvel arrêté royal. La publication des arrêtés royaux, en mai 2018, a remédié à cette lacune.

Les déclarations préalables nécessaires n'avaient cependant pas été effectuées. Après l'envoi d'un rappel aux responsables de traitement, les déclarations susmentionnées ont été encore réceptionnées fin novembre 2018 (voir *infra*, VI.3).

VI.2.2.2. La désignation d'un conseiller en sécurité

Après une nouvelle demande des deux instances de contrôle en 2018, les ministres ont indiqué ne pas encore avoir procédé à la désignation d'un conseiller en sécurité et en protection de la vie privée, dans l'attente de l'adaptation du cadre légal en matière de vie privée.[171,172]

---

170 Le rapport a été approuvé par les deux instances le 20 décembre 2018.

171 Entre-temps, tous les services avaient procédé à une désignation en interne.

172 Le C.O.C. et le Comité permanent R ne pouvaient souscrire à cette justification. En effet, ils exercent un contrôle *de lege lata* et ne peuvent se référer à d'éventuelles adaptations ultérieures de la réglementation. Le C.O.C. et le Comité permanent R ont donc réitéré leur recommandation.

VI.2.2.3. La mise en place d'un mécanisme de signalement des incidents de sécurité

En sa qualité de gestionnaire de la banque de données, la Police fédérale a indiqué qu'une procédure était déjà mise en place en 2018 afin de permettre à chaque utilisateur de signaler un incident de sécurité. Et la Police fédérale d'ajouter qu'une procédure était en cours d'élaboration au sein du Comité de pilotage de la BDC afin de pouvoir suivre et gérer les éventuels incidents de sécurité qui seraient déclenchés par un utilisateur.

Le C.O.C et le Comité permanent R ont salué cette initiative, tout en rappelant que la sécurité informatique relève de la compétence de professionnels : ne traiter que les incidents de sécurité déclenchés/détectés/signalés par les utilisateurs n'est pas suffisant. Et pour cause, la sécurité informatique n'est pas leur *core business*.

À cet égard, la persistance de l'absence de désignation d'un conseiller en sécurité, jouant le rôle principal en matière de sécurité du système d'informations, était jugée préoccupante.

VI.2.2.4. Le développement d'un outil informatique complémentaire

Les personnes pour lesquelles il n'existe que des 'indices sérieux' d'appartenance à l'une des catégories FTF de la banque de données peuvent figurer dans la banque de données pour une durée maximale de six mois. Si, dans ce délai, aucune information supplémentaire ne vient justifier l'appartenance à l'une des cinq catégories, il convient d'effacer les noms de ces personnes. Aussi, le C.O.C. et le Comité permanent R avaient recommandé un système de notification automatique. Suite à cette recommandation, un système d'avertissement avait été instauré.

En outre, 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. En 2017, l'organe de coordination avait précisé un tel outil technique n'était pas (encore) une priorité. Interrogée à ce propos en 2018, la Police fédérale a indiqué que tant que l'OCAM ne décide pas de retirer une entité, ses données demeurent exploitables dans la BDC. En d'autres termes, si l'OCAM ne prend pas l'initiative d'intervenir, une personne peut être maintenue pour une durée indéterminée dans la banque de données commune, ce qui est en contradiction avec l'obligation (minimale) de vérifier tous les trois ans si l'enregistrement d'une entité est toujours opportun. La recommandation de développer un outil informatique a dès lors été maintenue.

VI.2.2.5. Les cartes d'information et la communication à des tiers

En vertu de la loi, le bourgmestre est le destinataire des cartes d'information de FTF qui ont établi leur résidence ou leur domicile dans sa commune, la

fréquentent régulièrement ou y organisent régulièrement des activités. En 2017, l'OCAM n'avait aucune vue sur la manière dont cette obligation était respectée, ce qui avait conduit le C.O.C. et le Comité permanent R à recommander le développement d'un outil de suivi informatique devant permettre de contrôler le suivi de cette obligation.

En ce qui concerne les communications vers les services tiers, le C.O.C. et le Comité permanent R rappelaient déjà en 2017 que la lecture conjointe des articles 44/11/3*quater* LFP et 11 § 2 AR (F)TF imposait que ce genre de communications fasse préalablement l'objet d'une évaluation par la Police fédérale (en sa qualité de gestionnaire de la banque de données), par l'OCAM (en sa qualité de responsable opérationnel et service visé à l'art. 44/11/3*ter* § 1er LPF) et par les services de renseignement. Le C.O.C. et le Comité permanent R soulignaient que cette évaluation devait nécessairement inclure l'aspect 'sécurité des informations'. L'OCAM a été réinterrogé à ce propos en 2018 et a détaillé les mesures d'application prises à son niveau.

L'OCAM ne mentionnait pas explicitement le fait que l'évaluation visée à l'article 44/11/3*quater* LFP est (systématiquement et) préalablement effectuée en ce qui concerne la transmission (d'extraits) de la carte d'information à des instances tierces (c'est-à-dire des instances qui ne sont pas visées par l'art. 44/11/3*ter* LFP). Il convient de noter à cet égard que depuis le précédent contrôle réalisé en 2017, l'article 11 de l'AR (F)TF a été modifié par l'AR du 23 avril 2018 en ce qui concerne l'extraction et la transmission de listes.[173, 174] Il ressort de cette modification que l'extraction de listes est explicitement autorisée pour les services disposant d'un accès direct, mais uniquement à des fins de traitement interne effectué par un membre du personnel titulaire d'une habilitation de sécurité. Dès le moment où cette extraction sera techniquement possible (ce qui ne semblait pas encore être le cas au moment où l'enquête a été menée), la transmission de listes par l'OCAM à ces services perdra son utilité.

Concernant la transmission des listes à d'autres services ou à d'autres institutions (c'est-à-dire qui ne disposent pas d'un accès direct), elle n'est en principe pas autorisée, sauf si certaines conditions sont réunies. Lors du contrôle effectué mi-2018, l'OCAM a précisé avoir pris des mesures à son niveau en ce qui concerne la transmission des listes. Le C.O.C. et le Comité permanent R ont rappelé l'observation qu'ils avaient formulée quant à la nécessaire sécurisation technique de la transmission si elle est effectuée par e-mail. En outre, ils ont jugé opportun que le service de base assurant la communication informe comme il se doit le destinataire de la liste sur les conditions de communication de celle-ci.[175]

---

173 Une liste contient au minimum les données anonymes de plusieurs FTF (statistiques) et au maximum toutes les données à caractère personnel et les informations contenues dans les cartes d'information de ces FTF.

174 Finalité de la liste au regard de la mission légale du destinataire, utilisation de la liste exclusivement dans ce contexte, conservation limitée de la liste, sécurisation, etc.

175 Ceci peut-être par exemple réglé dans un protocole.

VI.2.2.6. L'exécution d'un contrôle spontané des loggings

En 2017, le C.O.C. et le Comité permanent R tiraient la conclusion suivante : '*même si les loggings ne sont pas immédiatement disponibles pour les services utilisateurs, ils doivent, par le biais de leur conseiller en sécurité et en protection de la vie privée respectif, les demander au gestionnaire de la banque de données commune (soit la police fédérale). Cette démarche proactive permettrait au service concerné d'exercer un contrôle sur la légitimité des accès à la banque de données commune.*'
À l'exception d'un service audité, la recommandation d'exécuter spontanément un contrôle des loggings n'a pas été suivie.

VI.2.3. L'UTILISATION DE LA BANQUE DE DONNÉES FTF PAR LES SERVICES PARTENAIRES ET LES MAISONS DE JUSTICE

VI.2.3.1. Un accès insuffisant à la version en production

À la mi-2018, un nombre significatif de services partenaires et de Maisons de Justice ne disposaient toujours pas de l'accès à la version en production de la BDC et, partant, ne l'utilisait pas.[176] Selon le C.O.C. et le Comité permanent R, cette situation était de nature à nuire, d'une part, à la complétude de la BDC et, d'autre part, à la prise d'une mesure adéquate par les services ou les autorités concernés.

Le C.O.C. et le Comité permanent R ont formulé les clarifications suivantes à cet égard :
- Conformément à la réglementation, la Direction générale du Centre de crise est un service qui (doit) dispose(r) d'une interrogation directe de la banque de données. Si ce n'est déjà fait, des mesures doivent être prises pour concrétiser ce droit (cette obligation).
- Dans la pratique, tous les établissements pénitentiaires, en réalité quelques services de l'administration centrale de la DG EPI, ont un accès direct aux banques de données. Le règlement prévoit cependant l'obligation pour tous les établissements pénitentiaires d'alimenter les BDC. En cas de maintien de cette pratique, le cadre législatif doit être adapté en conséquence.

VI.2.3.2. La situation au niveau des habilitations de sécurité

Au moment du contrôle, les membres des services qui avaient accès à la banque de données commune disposaient de l'habilitation de sécurité requise. Le C.O.C.

[176] Techniquement parlant, certains services n'y avaient tout simplement pas accès (p. ex. l'Administration générale des Maisons de Justice de la Communauté française).

et le Comité permanent R ont recommandé de lancer rapidement les procédures (assez longues) de demandes des habilitations de sécurité. À l'inverse, il faudra systématiquement signaler toute perte du *need to know* d'un membre du personnel, de manière à éviter le maintien de droits d'accès que ne sont plus nécessaires ou la poursuite d'enquêtes de sécurité devenues inutiles.

VI.2.3.3. La désignation d'un conseiller en sécurité au sein de chaque service

Tous les services qui disposaient de l'accès direct ou de l'interrogation directe au moment du contrôle avaient procédé à la désignation d'un conseiller en sécurité.

VI.2.3.4. La satisfaction des services partenaires

Plusieurs acteurs ont souligné l'aspect utile et collaboratif de la banque de données. Toutefois, au niveau pratique, plusieurs services ont émis le souhait de pouvoir travailler dans le cadre d'un système permettant la comparaison automatique des personnes comprises dans la banque de données commune avec leur propre banque de données. Conformément à la modification de l'article 11 de l'AR (F)TF en 2018, les services ayant un accès direct ont à désormais la possibilité d'extraire des listes, '*et ce, exclusivement pour un traitement interne*'. Cette disposition a également été modifiée pour permettre, après la vérification requise, la communication de listes par les services de base '*à d'autres services ou institutions*' (c'est-à-dire les services ou institutions qui ne disposent pas d'un accès direct).

Au niveau opérationnel, cette demande de disposer d'une application IT est compréhensible : les comparaisons automatiques permettent d'économiser du temps et des capacités. Il n'en reste pas moins que les comparaisons automatisées, d'une part, présupposent des tests approfondis et, d'autre part, nécessitent une intervention et une validation humaines avant la prise de décision. Des mesures doivent par ailleurs être prises pour que l'utilisation de ces listes par les tiers répondent à des conditions de sécurité requises (confidentialité, intégrité, etc.).

La Police fédérale prévoyait la mise en production de cette fonctionnalité pour début 2019. Le C.O.C. et le Comité permanent R suivront cet aspect.

VI.2.3.5. L'adaptation des procédures de validation suite à la modification du cadre juridique

Les procédures de validation communiquées par certains services avant ou lors du contrôle effectué par le C.O.C. et le Comité permanent R ne concernaient que les FTF et devaient être mises à jour pour les HTF et les PH. En outre, la *Vlaamse Agentschap Jongerenwelzijn* doit procéder à la mise en place du système de validation interne prévu à l'article 8 de l'AR TF.

VI.2.4. L'INFORMATION DES BOURGMESTRES ET LA TRANSMISSION (D'EXTRAITS) DES CARTES D'INFORMATION OU DE LISTES À DES INSTANCES TIERCES

En l'absence de moyens de contrôle fiables, le contrôle effectué par le C.O.C. et le Comité permanent R sur la transmission par les chefs de corps des Polices locales de la carte d'information aux bourgmestres a été reporté. Dans ce cadre, et afin de faciliter le contrôle futur, les deux instances ont recommandé à l'OCAM et à la Police fédérale de veiller à sensibiliser les services de base (et en particulier les zones de police) à systématiquement compléter les indicateurs informatisés (dates de transmission d'une carte d'information ou de sa mise à jour).

Au cours de l'enquête, l'OCAM n'a effectué aucune transmission (d'extraits) de carte d'information à des autorités ou à des entités tierces (c'est-à-dire, selon les travaux préparatoires de la loi, à des instances qui ne relèvent pas de l'article 44/11/3*ter* LFP).[177]

En juillet 2018, l'OCAM a fait savoir qu'il transmettait mensuellement des listes comprenant les noms des personnes se trouvant dans la banque de données commune *'à un nombre limité de services'*, sans préciser de quels services il s'agissait. Ce service a mis en avant le fait que *'l'envoi des listes vers ces 'partenaires' a été approuvé en consensus par les quatre services de base'*.

La réglementation concernant l'extraction et la transmission de listes a été modifiée en 2018. L'extraction de listes est désormais explicitement autorisée pour les services disposant d'un accès direct, mais uniquement à des fins de traitement interne et lorsque ce traitement est effectué par un membre du personnel titulaire d'une habilitation de sécurité. La transmission des listes à d'autres services ou institutions n'est en principe autorisée que sous certaines conditions (*supra*). Le C.O.C. et le Comité permanent R s'assureront du respect de cette nouvelle réglementation lors d'un contrôle ultérieur.

VI.3. LES DEUX AVIS COMMUNS

Conformément aux modifications introduites par les deux A.R. du 23 avril 2018 et à l'article 44/11/3*bis* § 3 LFP, les ministres de l'Intérieur et de la Justice ont soumis deux 'déclarations préalables' à l'avis du C.O.C. et du Comité permanent R.[178] Les principales observations sont résumées comme suit :

---

177 Cette transmission aurait nécessité une évaluation préalable conjointe de la Police fédérale, de l'OCAM et des autres services de base (art. 44/11/3*quater* LFP). Aucune précision n'a été apportée par l'OCAM à propos d'éventuelles transmissions par les autres services de base dans ce contexte (il n'est d'ailleurs pas certain que l'OCAM dispose de ces données).

178 Les deux avis communs 001/CPR-C.O.C./2018 et 002/CPR-C.O.C./2018 peuvent être consultés sur le site www.comiteri.be.

- Les traitements de données et d'informations concernant respectivement les HTF et les PH avaient déjà débuté en l'absence de création ou d'adaptation du cadre juridique (art. 44/11/3*bis* § 4, al. 2, LFP) et avant l'introduction les déclarations préalables (art. 44/11/3*bis* § 3 LFP). Le C.O.C. et le Comité permanent R rappelaient que le respect de ces deux dispositions était essentiel pour l'exercice du contrôle sur les banques de données communes ;
- Alors que les AR TF et PH étaient publiés depuis de nombreux mois, les déclarations ne renseignaient aucun élément concret concernant l'accès direct de l'ANS ;
- Les déclarations passaient également sous silence la possibilité d'extraire de la banque de données des listes contenant des données et informations à caractère personnel, alors qu'il s'agissait d'une modification importante ;
- Le C.O.C. et le Comité permanent R relevaient de nouveau l'absence de mention de la désignation d'un conseiller en sécurité ;
- Les deux instances regrettaient qu'au niveau de la communication de la carte d'information aux bourgmestres, la déclaration n'apportait pas de précisions sur la fréquence d'application de l'article 12 des AR TF et PH.[179] En outre, la déclaration ne faisait pas mention de la Loi du 30 juillet 2018 portant création de cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme (les 'CSIL-R'), qui prévoit que le chef de corps et/ou le représentant de la Police locale puisse transmettre aux membres des CSIL-R la carte d'information relative aux personnes dont le cas est soumis à discussion.

[179] En effet, que faut-il entendre exactement par 'communes fréquentées *régulièrement* par une entité' ou par 'une commune dans laquelle une entité organise *fréquemment* des activités' ?

CHAPITRE VII
AVIS

L'article 33, alinéa 7, L. Contrôle stipule que le Comité *'ne peut rendre un avis sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant les orientations politiques des ministres compétents, qu'à la demande de la Chambre des représentants ou du Ministre compétent.'* Sur la base de cette disposition, la Commission de la Justice de la Chambre n'a sollicité l'avis du Comité qu'une seule fois en 2018 (*infra*).

Par ailleurs, le Comité doit rendre des avis en tant qu'autorité de contrôle compétente (ACC) dans le cadre des traitements de données à caractère personnel ainsi que dans le cadre de la réglementation légale relative aux banques de données communes, et ce conjointement avec l'Organe de contrôle de l'information policière (C.O.C.). Ces deux compétences d'avis sont traitées respectivement au Chapitre V et au Chapitre VI.

VII.1. AVIS SUR LE PROJET DE LOI RELATIF AUX TRAITEMENTS DE DONNÉES À CARACTÈRE PERSONNEL

Le 14 décembre 2017, la Commission de la Justice de la Chambre des représentants a demandé au Comité permanent R de lui rendre un avis sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. Ce projet, qui était particulièrement complexe et technique et qui portait sur un thème d'une grande importance sociétale, contenait pas moins de 280 articles. Le Comité n'a jamais pu examiner en détail l'ensemble du projet. Effet, le texte a fait l'objet d'un débat politique jusque peu avant son introduction au Parlement ; certaines options devaient encore y être discutées et certaines modifications ont été apportées.

Par conséquent, le Comité était dans l'impossibilité de formuler un avis approfondi sur tous les aspects de la réglementation qui l'intéressaient. Il a essentiellement souligné deux éléments, d'une part, la complexité et la portée de la réglementation proposée – où la question était de savoir si un contrôle effectif sur les traitements de données à caractère personnel était toujours la première préoccupation – et la rédaction parfois illogique et incompréhensible du projet

et, d'autre part, la nécessité absolue d'une extension du cadre du Comité pour lui permettre d'accomplir les tâches nombreuses et importantes qui lui sont confiées dans le projet.[180]

Dans son avis, le Comité a souligné qu'il se réjouissait du choix de ne pas totalement exclure les données qui portent sur la 'sécurité nationale' de tous les mécanismes de protection. Il n'en reste pas moins que la manière dont cette option a été concrétisée (notamment par la création de plusieurs autorités de protection des données) a engendré un système de contrôle particulièrement complexe qui générerait inévitablement une confusion pour tous les acteurs concernés : les autorités administratives, les différentes autorités de protection des données et, naturellement, le citoyen pour qui la protection est instaurée.

180 La Loi du 3 décembre 2017, qui a créé l'Autorité de protection des données, prévoyait une structure élargie composée de six entités différentes, mais pour le Comité, il n'était question nulle part de moyens supplémentaires, en termes de budget, de personnel et d'outils informatiques. Le Comité a insisté pour obtenir un renforcement immédiat de ses effectifs. En l'absence de soutien, non seulement les autres missions du Comité, de plus en plus nombreuses, en subiraient les conséquences, mais les nouvelles missions ne pourraient, elles non plus, être remplies comme il se doit. Une telle situation met sérieusement en péril le contrôle indépendant et démocratique exercé sur le secteur du renseignement.

CHAPITRE VIII
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). En ce qui concerne les membres des autres 'services d'appui', cette disposition s'applique uniquement à l'obligation de communiquer à l'OCAM tout renseignement pertinent (art. 6 et 14 L.OCAM).

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le directeur du Service d'Enquêtes R sont soumis à l'autorité du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a aucune autorité sur eux. Le président du Comité doit cependant veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle. La raison en est évidente : l'organe de contrôle a beaucoup d'autres missions légales. Celles-ci pourraient être mises en péril si les dossiers judiciaires nécessitaient un investissement trop important. 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 2018 également, le Service d'Enquêtes R a effectué des devoirs d'enquête dans le cadre de missions judiciaires, plus précisément dans le cadre de trois informations judiciaires.

En premier lieu, le Service d'Enquêtes R a poursuivi l'enquête ouverte en 2017. Cette enquête a été menée sur réquisition du Parquet fédéral et portait sur

l'éventuelle implication d'un membre d'un service de renseignement dans un délit ou un crime contre la sûreté intérieure et extérieure de l'État. L'enquête n'a pas été finalisée en 2018.

Un deuxième dossier concernait le suivi d'une plainte introduite en 2014 par un particulier auprès du Comité permanent R contre un membre du personnel du SGRS. Le Comité a ici aussi effectué une enquête à ce propos dans le cadre de sa compétence générale de contrôle.[181]

Dans le troisième cas, le Service d'Enquêtes R a prêté son assistance dans le cadre d'une enquête menée par le Service chargé des missions de police judiciaire spécialisées en milieu militaire sur des faits présumés de harcèlement au sein d'un service de renseignement.

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 2018, le Service d'Enquêtes a reçu un seul signalement de ce genre.

[181] 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 IX
EXPERTISE ET CONTACTS EXTERNES

IX.1. EXPERT DANS DIVERS FORUMS

En 2018, 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 :

- Fin février 2018, le greffier a participé, à l'invitation du *Geneva Centre for the Democratic Control of Armed Forces* (DCAF), à Skopje (Macédoine), à un panel de discussion intitulé 'Why, When and How to engage in Oversight Fields Visits' dans le cadre du 'DCAF Assistance Program for the Parliament of the Republic of Macedonia'. Y a notamment été présenté le projet de 'Guidelines for intelligence oversight for parliamentary committees in the Assembly of the Republic of Macedonia'[182] ;
- En février 2018, l'ancien président du Comité a fait partie du jury de défense d'un doctorat à la Faculté des sciences économiques, sociales, politiques et de communication de Université catholique de Louvain (UCL)[183] ;
- À la demande de la *Tweede Kamer* néerlandaise, le Comité a collaboré à l'exploration d'un contrôle parlementaire des services de renseignement et de sécurité à l'étranger ;
- Le 25 mai 2018, le Comité permanent R et le Comité permanent P ont organisé une séance au Parlement à l'occasion de leur 25ème anniversaire. Outre quelques responsables politiques et orateurs internationaux, des représentants des services contrôlés ont également été invités à exprimer leur point de vue.
- Du 24 au 31 mai 2018, Fionnuala Ní Aoláin, la Rapporteuse spéciale des Nations Unies sur la protection des droits de l'homme dans le contexte de la lutte contre le terrorisme, était en visite officielle en Belgique. Le Comité permanent R a également eu l'honneur de la recevoir et a pu lui exposer sa vision.[184]

---

182 DCAF, *Guidelines for intelligence oversight for parliamentary committees in the Assembly of the Republic of Macedonia*, mai 2018, (www.dcaf.ch).

183 A. LELIÈVRE, *La communication web des services de renseignement. Étude sémio-pragmatique. Thèse présentée dans le cadre du Doctorat en Information et Communication*, UCL, février 2018.

184 Voir à ce propos : Human Rights Council, Report of the Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism – Visit to Belgium, A/HRC/40/52/Add. 5, 27 février 2019, 33 p.

- Un président honoraire du Comité permanent R exerce depuis 2011 la présidence du *Belgian Intelligence Studies Centre* (BISC). Ce centre s'est assigné l'objectif de rapprocher les services de renseignement et de sécurité et le monde académique, et de contribuer à la réflexion en matière de renseignement. En juin 2018, le BISC a organisé une journée d'étude sur le thème suivant : 'International collaboration regarding intelligence services and intelligence studies'.[185]
- Le Directeur du Service d'Enquêtes R a mené une réflexion sur le fonctionnement du Comité permanent R depuis 2013 dans les *Cahiers inlichtingenstudies*[186] ;
- Début avril 2018, l'ancien président du Comité a animé le panel de discussion sur 'L'Europe et le renseignement' lors du colloque 'Le renseignement et son contrôle', organisé par le Conseil d'État français et la Commission nationale de contrôle des techniques de renseignement (CNCTR) ;
- Le greffier du Comité a participé à l'*European Intelligence Oversight Network* (EION), où des experts de plusieurs autorités de contrôle, d'ONG (p. ex. *la Stiftung Neue Verantwortung*) ou encore du milieu académique réfléchissent sur l''oversight innovation' et l'échange d'informations entre les organes de contrôle nationaux ;
- En septembre 2018, Paris a accueilli un colloque de trois jours intitulé 'SIGINT intelligence transnational activities and national security in France and Europe – a changing landscape'. Un président honoraire, en sa qualité d'orateur principal, y a parlé de 'SIGINT Intelligence, Surveillance, Ethics and Control'. Ce colloque a également été l'occassion d'expliquer le rôle du Comité permanent R comme organe de contrôle et de mettre l'accent sur l'importance croissante du SIGINT dans le contexte 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) ;
- Le Comité permanent R a procédé à un échange de vues avec la *Stiftung Neue Verantwortung* sur les 'New challenges and changes to democratic control of intelligence in Belgium and Germany' ;
- Le Comité a été sollicité pour son expertise juridique lors d'un séminaire pratique destiné à la police, à la magistrature et au barreau autour du thème 'classification et habilitations de sécurité' ;

---

185 Le BISC a consacré son 9ème cahier au président honoraire du Comité permanent R (M. COOLS et al, eds., *Methodologie inlichtingenstudies – Méthodologie des études de renseignement. Liber Amicorum Guy Rapaille*, Gompel&Svacina, Oud-Turnhout, 2018, 280 p.

186 F. FRANCEUS, 'Et demain ? Het Vast Comité I sinds 2013', in M. COOLS et al, *o.c.*, 2018, 19-26.

– Le chef du service juridique a publié, en 2018, une contribution scientifique sur les 25 ans de contrôle belge sur les services de renseignement et de sécurité.[187]
– Le président, le président honoraire ainsi que les conseillers du Comité permanent R ont pris la parole lors de la 'Conférence européenne des autorités de contrôle du renseignement' (Paris, 6 et 7 décembre 2018).

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

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, n'était encore concrétisé par la Belgique en 2018.[188] L'instauration effective d'un tel institut n'a pu être approuvée qu'après la ratification du protocole par le Parlement fédéral, mais aussi par toutes les entités fédérées. Il s'en est suivi la parution au Moniteur des actes d'assentiment des Communautés flamande, Wallonie-Bruxelles et germanophone, ainsi que de la Région wallonne et la publication de l'acte de l'Assemblée réunie de la Commission communautaire commune.

En attendant l'instauration de l'institut, les réunions de différentes institutions dotées d'un mandat en matière de droits de l'homme[189] ont donné lieu, en janvier 2015, à la conclusion d'un protocole de coopération.[190] Les instances participantes s'y sont accordées pour échanger des pratiques et des méthodes, pour examiner des questions communes et pour promouvoir la coopération mutuelle.

En 2018, les activités de cette plateforme ont consisté à organiser des réunions de concertation. Y ont été abordés tant les problématiques générales (p. ex. la Belgique et la promotion et la protection des droits de l'homme, la création du Conseil central de surveillance pénitentiaire et commissions de surveillance, une présentation des différents instituts participants…) que

187 W. VAN LAETHEM, 'The Rule of Law and 25 Years of Intelligence Oversight in an Ever-changing World : the Belgian Case' in I. LEIGH en N. WEGGE (eds.), *Intelligence Oversight in the Twenty-First Century. Accountability in a Changing World*, Londen, Routledge, 2018, 208 p.

188 Avec la 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), la question a également été réglée au niveau fédéral.

189 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.

190 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.

l'échange de procédés et de méthodologies sur des dossiers individuels concrets. En 2018, Myria – anciennement le Centre interfédéral pour l'égalité des chances et la lutte contre le racisme et les discriminations – a repris la présidence jusque-là assurée par la Commission nationale pour les droits de l'enfant.

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

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 (au départ) cinq pays européens (la Belgique, le Danemark, les Pays-Bas, la Norvège et la Suisse)[191] collaborent afin de relever ces défis, en identifiant des méthodes de travail qui leur permettraient de limiter le risque de lacunes dans le contrôle.

Depuis 2015, ces organes de contrôle indépendants mènent simultanément, mais chacun dans le cadre de son mandat et de ses compétences, une enquête sur l'échange international de données à caractère personnel dans le cadre de la lutte contre les FTF (cf. I.6.1). L'année dernière, 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.

Début novembre 2018, les organes de contrôle participants ont rédigé une déclaration et un communiqué de presse communs.[192] La déclaration commune énumérait une série de moyens permettant d'aller de l'avant. En effet, prévenir le risque d'angles morts dans le contrôle requiert une intensification de la coopération entre les instances de contrôle. Limiter le secret entre les organes de contrôle est une étape utile et nécessaire vers une coopération plus étroite en matière de contrôle. Si les services de renseignement échangent fréquemment des données, cela doit être également possible pour les organes de contrôle ; ils doivent ensuite pouvoir discuter des renseignements échangés. Une autre étape dans la bonne direction consiste à élaborer de nouvelles méthodes de contrôle juridiques et techniques afin d'évaluer efficacement le système des échanges internationaux de données ainsi que l'existence et la mise en place des garanties communes de respect des droits fondamentaux.

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

192 Voir annexe D. 'Renforcement du contrôle des échanges internationaux de données entre les services de renseignement et de sécurité'.

IX.4. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

En 2018, le Comité permanent R a continué à entretenir des contacts étroits avec plusieurs organes de contrôle étrangers.

Le colloque qui s'est tenu début avril 2018 au Conseil d'État français – co-organisé par la Commission nationale de contrôle des techniques de renseignement (CNCTR) – et auquel le Comité permanent R était représenté, a encore permis de renforcer les relations. Non seulement des liens ont été tissés avec la Délégation parlementaire au renseignement (DPR) française, mais des échanges de vues ont été également eu lieu, entre autres, avec la *Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten* (CTIVD) néerlandaise, l'*Investigatory Powers Commissioner's Office* (IPCO) du Royaume-Uni, et le *Parlamentarisches Kontrollgremium PKgr* allemand.

En juin 2018, une visite de travail a été organisée entre une représentation du Comité permanent R et ce *Parlamentarisches Kontrollgremium PKgr*. Lors de cette visite, la délégation belge a expliqué ses rapports d'activités ainsi que les enquêtes menées après les attentats de Paris et de Bruxelles.

Toujours en juin, un briefing a été co-organisé avec le Président de la Chambre des représentants et l'*Office of the Personal Data Protection Inspector* de Géorgie ainsi que des représentants du Parlement géorgien. La Sûreté de l'État et l'Organe de coordination pour l'analyse de la menace ont été associés à cette initiative. L'objectif était de mieux comprendre l'organisation d'un contrôle indépendant des services de renseignement, en mettant l'accent sur la méthodologie, les moyens et les techniques utilisés afin de satisfaire aux exigences d'un contrôle démocratique efficace et efficient.

À la demande du ministère norvégien de la justice, une rencontre a eu lieu en octobre 2018 à l'Ambassade de Norvège à Bruxelles, avec des représentants de ce ministère et des collaborateurs de l'ambassade, sur la planification stratégique dans le cadre de la coopération entre services de renseignement.

Début novembre 2018, un entretien a été organisé à l'Ambassade de France à Bruxelles avec une délégation parlementaire composée de membres de la Délégation parlementaire au Renseignement, de la Commission de vérification des fonds spéciaux et de l'Assemblée nationale. L'échange de vues s'inscrivait dans le cadre de la préparation de l'initiative commune des présidents de l'Assemblée nationale et du Sénat sur '10 ans de contrôle parlementaire du renseignement : l'exigence démocratique est-elle satisfaite ?'

Toujours en novembre, l'*International Intelligence Oversight Forum* a été organisé à la Valette (Malte) par le *Special Rapporteur for Privacy* (SRP) des Nations Unies. Parmi les participants, figuraient des représentants d'organes de contrôle, de services de renseignement, d'universités et d'ONG. En 2018, le thème retenu était 'Latest Challenges to Intelligence Oversight in a Democracy'.

Le Comité permanent R était représenté et a entretenu des contacts informels avec divers organes de contrôle européens et d'outre-mer (Nouvelle Zélande, Canada, etc.). Ce forum visait à permettre, dans un cadre confidentiel, de mieux cerner les défis auxquels sont confrontés, entre autres, les organes de contrôle démocratiques.

Les 21 et 22 novembre 2018, le Comité était invité par l'organe de contrôle suisse, l'Autorité de surveillance indépendante des activités de renseignement, à effectuer une visite à Berne afin de renforcer les liens entre les deux organes de contrôle. La délégation belge a par ailleurs profité de sa présence dans la capitale helvétique pour se rendre à l'Ambassade de Belgique.

Le Comité permanent R a co-organisé avec la Commission nationale de contrôle des techniques de renseignement française une conférence de deux jours intitulée 'Conférence européenne des autorités de contrôle du renseignement' (Paris, 6 et 7 décembre 2018). Cette conférence, à laquelle 15 pays européens ont participé, s'est tenue à huis clos (*supra*).

Enfin, les premiers contacts exploratoires ont été établis avec plusieurs instances du BENELUX, et ce dans l'optique de créer un cadre normatif dans le contexte de la coopération internationale entre les services de renseignement et les organes de contrôle.

IX.5. PRÉSENCE DANS LES MÉDIAS

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

Date	Sujet/titre	Organe de presse
16 janvier 2018	Inteligencia estratégica, hoy	Defensa.com
27 janvier 2018	Eindelijk controle op kas Staatsveiligheid	De Tijd
27 janvier 2018	Militair geheime dienst ontsnapt aan Rekenhof	De Tijd
30 janvier 2018	Eddy Testelmans, l'ancien chef des renseignements de l'armée, sous le feu des critiques	La Libre Belgique
13 février 2018	'Bruxelles est un nid d'espions' : la capitale belge est un carrefour mondial de l'espionnage, confirme le patron du Comité R	Sud Presse
1er mars 2018	Belgische terroristen-databank rammelt nog	De Tijd
6 mars 2018	Ex-leden willen dat Comité I rol van Staatsveiligheid onderzoekt	Knack
6 mars 2018	Des anciens du Comité R réclament une enquête sur la Sûreté de l'État	Le Vif

Date	Sujet/titre	Organe de presse
13 mars 2018	Serge Lipszyc, seul candidat à la présidence du Comité R	Le Vif
23 mars 2018	Omstreden benoeming voor adviseur premier	De Standaard
23 mars 2018	Candidate to head security committee draws fire from the opposition	The Brussels Times
28 mars 2018	Adviseur premier Michel aan het hoofd van Comité I	De Standaard
13 avril 2018	België opent geheime archieven om mysterieuze dood VN-baas op te helderen	De Morgen
18 avril 2018	Comment la Belgique a rendu la liberté au commanditaire présumé des attentats de Paris et de Bruxelles	Paris Match
19 avril 2018	La Chambre désigne un collaborateur de Charles Michel à la tête du Comité R	Sudinfo.be
19 avril 2018	Kamer keurt omstreden benoeming van adviseur premier goed	De Standaard
24 mai 2018	Guy Rapaille, président du Comité R : 'Il a fallu attendre les attentats pour obtenir plus de moyens'	Rtbf.be
24 mai 2018	Contrôler la police et les renseignements : Guy Rapaille invité de Jeudi en Prime	Rtbf.be
25 mai 2018	Belgische militairen zetten in 2016 voet aan de grond in Syrië	Vrt.be
5 juin 2018	Ça roule entre le FBI et la Belgique	Le Soir
6 juin 2018	Wat vertellen Belgische archieven over dood Dag Hammarskjöld in 1961?	Mo.be
6 juin 2018	Rekenkamer : 'Privacycommissie, Comité P en andere aan Kamer verbonden instellingen moeten gesaneerd worden'	Het Laatste Nieuws
12 juni 2018	Guy Rapaille (Comité I) : 'Russische inmenging bij onze verkiezingen? Dat valt te vrezen, ja'	Knack
13 juin 2018	'Gare à l'action des services turcs et marocains'	Le Soir
13 juin 2018	Bélgica investiga si sus servicios de inteligencia conocían el supuesto espionaje del CNI a Puigdemont	Público
13 juin 2018	Belgique : interrogations sur un possible espionnage de Puigdemont par l'Espagne sans préavis	Le Point
13 juin 2018	België laat schaduwoperatie tegen Puigdemont onderzoeken	De Tijd
13 juin 2018	Guy Rapaille : 'Une ingérence russe lors des élections est à craindre '	Le Vif
13 juin 2018	Le renseignement belge s'inquiète d'une possible ingérence de la Russie lors des élections	Sudinfo.be
13 juin 2018	Steven Vandeput confirme un risque d'actions de désinformation russes en Belgique : 'on se prépare'	Rtbf.be
14 juin 2018	Militaire veiligheidsdienst draait vierkant	De Standaard

Date	Sujet/titre	Organe de presse
14 juin 2018	Dysfonctionnements au sein du service de renseignement militaire	Rtbf.be
15 juin 2018	Comité I-voorzitter Guy Rapaille spreekt	Apache
16 juin 2018	Guy Rapaille, président du Comité R : 'La Belgique doit craindre l'ingérence russe'	Le Soir – Le Vif
24 juin 2018	Élections en Turquie : la propagande passe aussi par les mosquées	La Libre Belgique
25 juillet 2018	À Bruxelles, une incroyable histoire de faux papier et d'espions russes	Le Monde
30 août 2018	Les services de renseignement doivent pouvoir déplaire au politique. Entretien avec Guy Rapaille	Le Vif
11 septembre 2018	Guy Rapaille 'Les services de renseignement doivent pouvoir déplaire aux politiques'	Rtbf.be
11 septembre2018	Au bout du jour : interview de Monsieur Rapaille	Rtbf.be
12 novembre 2018	Filip Dewinter, espion…pour la Chine ?	La Libre Belgique
12 novembre 2018	Filip Dewinter vraagt onderzoek van Comité I	De Standaard
2 décembre 2018	Guy Rapaille : 'La transparence des services de renseignements a été parfaite'	Le Soir
21 décembre 2018	Elk bedrijf moet info geven aan Staatsveiligheid	De Tijd
21 décembre 2018	Les entreprises doivent fournir des informations sur demande de la Sûreté de l'État	Rtbf.be

CHAPITRE X
L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ

L'Organe de recours est une 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.[193]

L'Organe de recours est composé du président du Comité permanent R, du président du Comité permanent P et, depuis mi-2018 (voir X.2.2.), 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 greffe est exercée par le greffier du Comité permanent R et par son administration.

Ces activités de l'Organe de recours ont un impact direct tant sur le budget que sur le personnel du Comité permanent R. En effet, tous les frais de fonctionnement sont supportés par le Comité permanent R. Il met à disposition non seulement son président et son greffier, mais aussi le personnel administratif requis, qui veille à la préparation, au traitement et au suivi des recours. Ces processus prennent beaucoup de temps.

---

193 Pour plus de détails, voir COMITÉ PERMANENT R, *Rapport d'activités 2006,* 87-115. Les règles qui y sont explicitées ne tiennent cependant pas compte des modifications intervenues en matière d'avis de sécurité introduites par les lois du 23 février 2018 et du 13 septembre 2018 et résumées ci-après (voir X.2.1.2 et X.2.2.).

X.1. UNE PROCÉDURE PARFOIS LOURDE ET COMPLEXE

La diminution du nombre de dossiers observée en 2018 (de 192 à 158) ne s'est pas traduite par une diminution de la charge de travail, bien au contraire. En effet, ces dossiers n'ont cessé de se complexifier du point de vue de la gestion administrative, des audiences et des décisions.

Ainsi, de nombreux envois ne respectent pas les articles 2 et 3 de l'AR Org. recours, qui stipulent respectivement que *'l'envoi à l'organe de recours de toutes pièces de procédure se fait sous pli recommandé à la poste'* et que *'le recours est signé et daté par le requérant ou par son avocat'*. Le greffier se voit dès lors contraint d'interpeller le requérant afin de régulariser la situation dans le délai légal.[194]

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. De plus, 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 nonobstant la jurisprudence constante de l'Organe de recours selon laquelle la L.Org.recours est une

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

lex specialis par rapport à la Loi Classification. Enfin, il y a 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, et ce 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 laisser tomber certains éléments dans la décision qui est communiquée à l'intéressé. L'autorité de sécurité doit spécifier, au moyen de la motivation, 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.
- En outre, il y a lieu de constater que, dans leurs décisions, diverses autorités de sécurité n'ont pas non plus respecté les principes de droit administratif sur le plan formel (décisions dépourvues de dates ou de l'identité du fonctionnaire qui les a adoptées, absence d'audition de l'intéressé, emploi de la langue en matière administrative).
- Les autorités de sécurité semblent accepter avec difficulté certaines décisions qui découlent d'une 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. Enfin, de nombreux dossiers doivent être repris lors d'une deuxième ou d'une troisième audience, soit parce que le requérant demande un report, soit parce qu'il faut attendre des informations complémentaires, ou encore en raison d'une modification du siège de l'Organe de recours.

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

X.2. L'ÉVOLUTION DU CADRE JURIDIQUE

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

Cette intention s'est concrétisée fin 2017 par le dépôt d'un projet de loi[195] visant à modifier la L.C&HS. Le Comité permanent R avait rendu un avis à ce propos.[196] Ce projet a finalement été adopté début 2018[197], entraînant également une légère modification de la L.Org.recours. Quatre Arrêtés royaux ont été pris en exécution de la loi. Certaines modifications ont porté sur la composition de l'Organe de recours. Par ailleurs, la nouvelle loi-cadre en matière de protection de la vie privée contient des règles s'appliquant (notamment) à l'Organe de recours. Ces adaptations du cadre juridique sont précisées dans la présente section.

X.2.1. LES MODIFICATIONS À LA RÉGLEMENTATION SUR LA CLASSIFICATION ET LES HABILITATIONS, ATTESTATIONS ET AVIS DE SÉCURITÉ

X.2.1.1. La compétence et le rôle de l'officier de sécurité

La modification de la L.C&HS élargit la fonction d'officier de sécurité dans le cadre des vérifications de sécurité (attestations et avis) et instaure également cette fonction au sein du Ministère public.

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

---

195 *Doc. parl.*, Chambre 2017-2018, n°54-2767/1.

196 Cet avis est publié sur le site Internet du Comité permanent R (www.comiteri.be). Le Comité y souligne le fait que le projet n'apporte pas de réponse à de nombreux problèmes générés par l'application de la réglementation actuelle (complexité, délais de recours beaucoup trop courts, etc.), et ce tant pour les administrations et les citoyens concernés que pour l'Organe de recours. Le Comité avait précédemment formulé des propositions pour remédier à certains de ces problèmes. Il relevait que non seulement le projet de loi ne les abordait pas, mais qu'il créait des problèmes supplémentaires pour tous les acteurs. Le Comité estimait qu'il était indiqué de réformer de manière cohérente les deux lois du 11 décembre 1998 (L.C.&HS et L.Org.recours).

197 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).

X.2.1.2. La réforme de la procédure d'avis de sécurité[198]

La procédure d'avis de sécurité a été réformée, que ce soit au niveau de la décision réglementaire de l'autorité administrative ou du mécanisme de décision individuelle. Cette nouvelle réglementation est entrée en vigueur le 1er juin 2018.

Au niveau de la décision réglementaire, le nouveau système prévoit qu'il appartient au Roi de déterminer les secteurs d'activités soumis à l'application de l'avis de sécurité ainsi que les autorités administratives (sectorielles) compétentes.[199] Les personnes morales de droit privé ou public relevant du secteur concerné réalisent ensuite, d'initiative ou à la demande de l'autorité administrative compétente, une 'analyse de risques' qui est transmise à cette dernière. L'autorité administrative demande alors une 'analyse' de la menace' spécifique 'aux services compétents'. Dès réception de cette analyse, l'autorité administrative compétente réalise une 'analyse d'impact' visant à identifier les dommages potentiels aux intérêts majeurs de l'État. Sur la base des analyses précitées, l'autorité administrative transmet un dossier de demande de vérification de sécurité à l'Autorité nationale de sécurité (ANS). Celle-ci décide en dernier ressort si des vérifications peuvent être ou non effectuées.

S'agissant du mécanisme de décision individuelle, le nouveau système prévoit que les personnes morales relevant du secteur concerné doivent informer l'intéressé de l'obligation de se soumettre à une vérification de sécurité. L'officier de sécurité des personnes morales doit au préalable recueillir le consentement de la personne concernée. L'officier de sécurité de l'autorité administrative compétente doit veiller à la conformité des demandes de vérification. Il les transmet à son tour à l'ANS, qui statue dans le délai prescrit (maximum un mois). À défaut, elle peut être mise en demeure de statuer dans un délai minimum équivalent au délai prescrit initialement. Si l'ANS laisse s'écouler ce nouveau délai sans prendre de décision, l'avis est réputé positif. La nouvelle réglementation prévoit que l'avis est délivré pour une durée maximale de cinq ans[200], sous réserve d'une réévaluation par l'ANS (sur la base de nouveaux éléments). L'autorité administrative informe l'officier de sécurité de l'employeur

---

198 Voir les articles 22*quinquies* et 22*quinquies*/1 L.C.&HS et l'A.R. du 8 mai 2018 modifiant l'Arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (*M.B.* 1er juin 2018).

199 Il s'agit là d'une différence notable par rapport au système initial des avis de sécurité dans lequel 'une' (n'importe quelle) autorité administrative pouvait initier la procédure.
Cette disposition a été mise en œuvre par l'Arrêté royal du 8 mai 2018 fixant les secteurs d'activités et les autorités administratives compétentes visées à l'article 22*quinquies*, 7, de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (*M.B.* 1er juin 2018).

200 Il s'agit ici aussi d'une différence avec le système précédent, puisque celui-ci ne prévoyait pas dans tous les cas de 'durée de validité maximale'. En outre, dans l'ancien système, la réalisation de l'avis de sécurité devait avoir lieu 'préalablement' à l'exercice d'une profession, d'une fonction, d'une mission ou d'un mandat. La modification introduit la possibilité de soumettre des personnes qui sont déjà en fonction à une vérification de sécurité.

de l'avis de sécurité. S'il est négatif, l'autorité administrative le notifie par pli recommandé à la personne concernée, à l'exception des motifs dont la divulgation serait susceptible de nuire à l'un des intérêts fondamentaux énoncés par la loi, à la protection des sources, au secret d'une information ou d'une instruction judiciaire ou à la protection de la vie privée de tiers.[201]

X.2.1.3. Le contenu de la vérification de sécurité

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

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

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

Enfin, la nouvelle loi étend les banques de données qui peuvent être analysées. L'article 22*sexies* L.C.&HS prévoyait déjà la consultation et l'évaluation des données judiciaires[202], des informations des services de renseignement, du casier judiciaire central, du casier judiciaire et des registres de la population et des étrangers tenus par les communes, du registre national, du registre d'attente des étrangers ainsi que des données policières accessibles aux fonctionnaires de police lors de l'exécution d'un contrôle d'identité. La modification y ajoute les données et les informations des banques de données policières internationales résultant de traités liant la Belgique, les données de police administrative, les données contenues dans les banques de données communes et d'"*autres données et informations*". La loi prévoit que le caractère adéquat, pertinent et non excessif de ces nouvelles données et informations, ainsi que la liste de celles-ci, doivent être déterminés par arrêté royal. Cet Arrêté est également paru dans le courant de l'année 2018.[203]

X.2.1.4. Les rétributions

Mi-2018, un Arrêté royal fixant les rétributions dues pour les habilitations, les attestations et les avis a également été adopté.[204] Concrètement, une habilitation

---

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

202 Communiquées avec l'accord des autorités judiciaires compétentes.

203 A.R. du 8 mai 2018 déterminant la liste des données et informations qui peuvent être consultées dans le cadre de l'exécution d'une vérification de sécurité (*M.B.* 1er juin 2018).

204 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

se rapportant à une personne physique coûte 150, 175 ou 200 euros selon le niveau demandé (respectivement confidentiel, secret ou très secret). En ce qui concerne les personnes morales, la rétribution s'élève, selon le cas, à 900, 1200 ou 1500 euros. Le coût d'une attestation ou d'un avis de sécurité s'élève à 50 euros. Ces montants sont ensuite partiellement redistribués entre les différentes autorités concernées selon une clé de répartition définie dans l'Arrêté royal.

X.2.2. LES MODIFICATIONS DU FONCTIONNEMENT DE L'ORGANE DE RECOURS[205]

En 2018, trois lois ont modifié la composition de l'Organe de recours ainsi que la procédure de recours.

Tout d'abord, la L.Org.recours a été modifiée de manière à l'aligner sur les adaptations introduites dans la L.C.&HS. Il s'agissait de garantir le maintien d'un droit de recours pour la personne destinataire d'un avis de sécurité négatif. Pour ce faire, ce dernier doit introduire son recours dans les huit jours de la réception de l'avis. En outre, l'article 12 de la L.Org.recours a été adapté de manière à permettre un recours à toute personne justifiant d'un intérêt légitime contre la décision réglementaire (positive ou négative)[206] de l'ANS relative au dossier de l'autorité administrative visant à imposer une vérification de sécurité. À l'inverse, l'autorité administrative concernée se voit également dotée d'une possibilité de recours devant l'Organe de recours, dans l'hypothèse où l'ANS a refusé sa demande de vérification. Ces recours doivent être introduits dans les huit jours suivant la prise de connaissance de la décision de l'ANS.

Par ailleurs, la composition de l'Organe de recours a été modifiée par la Loi du 13 septembre 2018 pour prendre en considération la suppression de la

---

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).

205 Loi du 13 septembre 2018 portant modification 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 (*M.B.* 5 octobre 2018).

206 Les travaux préparatoires précisent que : *'Ce recours est donc possible pour une personne physique qui exerce une fonction ou a un accès à un lieu concerné, mais aussi pour une personne morale de droit privée membre du secteur. […] Ce recours porte donc bien sur l'approbation ou le refus du dossier de l'autorité administrative. Sur base de l'article 12 de la loi sur les habilitations. C'est un recours d'opportunité par rapport aux aspects 'sécurité' du dossier. De facto, pour l'examen de ce recours les éléments du dossier de l'autorité administrative, concernant les aspects 'sécurité' seront aussi pris en compte. L'expérience et l'expertise des membres de l'organe de recours en matière de sécurité et de protection des libertés et droits fondamentaux justifient le recours auprès de cet organe. Il est évident que le secteur ou toute personne justifiant d'un intérêt peut aussi introduire un recours contre le dossier introduit par l'autorité administrative (l'analyse d'impact). Celui-ci est alors possible devant le Conseil d'État car il ne relève pas des compétences de l'organe de recours'* (*Doc. parl.*, Chambre 2017-2018, 54-3107/5, 4).

Commission de la protection de la vie privée. La L.Org.recours prévoit désormais que le président de la Chambre contentieuse de l'Autorité de protection des données (APD) siège à l'Organe de recours. Afin de veiller à la continuité, la Loi du 13 septembre 2018 avait prévu une disposition transitoire prévoyant que le président de l'APD continuerait à exercer son mandat au sein de l'Organe de recours jusqu'à la nomination du président de la Chambre contentieuse de l'APD. Cette nomination est intervenue à la fin du premier trimestre 2019.[207]

Enfin, compte tenu du fait que la Loi du 3 décembre 2017[208] ne prévoit pas que le président de la Chambre contentieuse de l'APD (ni aucun membre au sein de cette Chambre contentieuse) doit avoir la qualité de magistrat, l'exigence de cette qualité pour pouvoir faire partie de l'Organe de recours a été supprimée.[209]

X.2.3. LA NOUVELLE LOI-CADRE EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE

Le Titre 3 de la loi du 30 juillet 2018[210] (LPD) contient un sous-titre 3 consacré spécifiquement à la protection des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre de la L.C&HS (articles 106 à 137 LPD). Les règles contenues dans ce sous-titre s'appliquent aussi à chaque traitement de ce type de données par l'Organe de recours (article 107, al.2 LPD). Il convient toutefois de noter qu'en sa qualité d'autorité juridictionnelle, l'Organe de recours n'est pas soumis au contrôle d'une autorité de protection des données à caractère personnel (article 128, § 2 LPD).

X.3. LE DÉTAIL DES CHIFFRES

Cette section reprend les chiffres relatifs à la nature des décisions contestées, la qualité des autorités compétentes et des requérants[211], ainsi que la nature des décisions de l'Organe de recours dans le cadre des différentes procédures de

---

207 Hielke Hijmans a été nommé président de la Chambre contentieuse de l'Autorité de protection des données (*C.R.I.* Chambre 2018-2019, PLEN 278, 28 mars 2019) et a prêté serment le 24 avril 2019.

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

209 Selon les travaux préparatoires : *'Cela signifie donc que l'on suit les conditions édictées par les lois d'origine des organes concernés. L'organe de recours restera composé au minimum de 2 magistrats. En effet, la présence de 2 magistrats issus des Comités P et R au sein de cet organe est garantie par la loi d'origine de ces organes'* (*Doc. parl.*, Chambre 2017-2018, 54-3107/003, 9).

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

211 À noter que 10 'requêtes' de citoyens n'étaient pas conformes aux exigences minimales de la loi (l'exemple type est un défaut de signature) et ne pouvaient donc pas être considérées comme des recours recevables.

recours. À des fins de comparaison, les chiffres des cinq dernières années ont également été repris.

Trois tendances se dégagent en 2018. La première, à caractère général, est la diminution du nombre de dossiers après deux années de hausse sensible ; le nombre de dossiers est ainsi passé de 192 en 2017 à 158 en 2018. En outre, le nombre de dossiers concernant des militaires a chuté, passant de 20 en 2017 à 8 en 2018. Et enfin, la dernière tendance concerne, d'une part, l'augmentation du nombre de recours contre des refus d'attestations de sécurité liées au secteur nucléaire (7 en 2016 et 2017 et 11 en 2018), et d'autre part, la diminution marquée du nombre de recours contre des avis de sécurité négatifs (101 en 2016, 122 en 2017 et 92 en 2018).[212]

Quatorze audiences de l'Organe de recours ont été organisées en 2018.

Tableau 1. Autorités de sécurité concernées

	2014	2015	2016	2017	2018
Autorité nationale de sécurité	99	68	92	129	113
Sûreté de l'État	0	1	0	0	0
Service Général du Renseignement et de la Sécurité	60	47	68	53	32
Agence fédérale de Contrôle nucléaire	8	10	8	7	10
Police fédérale	3	3	1	3	3
Police locale	1	1	0	0	0
TOTAL	**171**	**130**	**169**	**192**	**158**

Tableau 2. Nature des décisions contestées

	2014	2015	2016	2017	2018
Habilitations de sécurité (art. 12 et s. L.C&HS)					
Confidentiel	5	9	5	1	2

212 Cette diminution du nombre de recours introduits contre des avis de sécurité s'explique par une jurisprudence de l'Organe de recours, rendue dans le courant de l'année 2017, selon laquelle, sur la base des éléments qui lui étaient (alors) soumis dans les dossiers de vérifications de sécurité, les avis de sécurité formulés par l'ANS pour le personnel externe des institutions européennes ne reposaient pas sur une base juridique suffisante. L'analyse de l'adaptation du cadre juridique (résumée ci-dessus) amène à supposer que la matière des avis de sécurité pour le personnel des institutions européennes va prochainement être (de nouveau) soumise à l'Organe de recours, dans la mesure où l'A.R. du 8 mai 2018 (voir *supra*) désigne le fonctionnaire dirigeant du SPF Affaires étrangères ou son délégué comme autorité administrative compétente pour les instances internationales.

	2014	2015	2016	2017	2018
Secret	43	35	38	33	31
Très secret	4	4	7	6	3
Refus	25	36	28	30	26
Retrait	9	7	9	7	4
Refus et retrait	0	0	0	0	
Habilitation pour une durée limitée	2	3	4	1	1
Habilitation pour un niveau inférieur	1	0	1	0	0
Pas de décision dans les délais	15	2	7	2	5
Pas de décision dans les nouveaux délais	0	0	1	0	0
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	**52**	**48**	**50**	**40**	**36**
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)					
Refus	4	6	1	3	3
Retrait	0	0	0	0	0
Pas de décision dans les délais	0	0	0	0	0
Attestations de sécurité lieu ou événement (art. 22*bis*, al.2 L.C&HS)					
Refus	16	12	9	20	15
Retrait	0	1	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
Retrait	–	–	1	0	0
Pas de décision dans le délai	–	–	0	0	1
Avis de sécurité (art. 22*quinquies* L.C&HS)					
Avis négatif	99	63	101	122	92
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

	2014	2015	2016	2017	2018
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	**119**	**82**	**119**	**152**	**122**
TOTAL DÉCISIONS CONTESTÉES	**171**	**130**	**169**	**192**	**158**

Tableau 3. Nature du requérant

	2014	2015	2016	2017	2018
Fonctionnaire	0	4	2	4	5
Militaire	17	29	23	20	8
Particulier	145	93	139	164	140
Personne morale	6	4	5	4	5

Tableau 4. Langue du requérant

	2014	2015	2016	2017	2018
Français	92	75	99	115	83
Néerlandais	76	54	70	77	75
Allemand	0	0	0	0	0
Autre langue	0	1	0	0	0

Tableau 5. Nature des décisions interlocutoires prises par l'Organe de recours[213]

	2014	2015	2016	2017	2018
Demande du dossier complet (1)	168	130	167	191	154
Demande d'informations complémentaires (2)	16	7	23	36	12

213 Le 'nombre de décisions interlocutoires' (tableau 5), les 'manières dont les requérants font usage de leurs droits de défense' (tableau 6), ou encore la 'nature des décisions de l'Organe de recours' (tableau 7) ne correspondent pas nécessairement au nombre de requêtes introduites (voir tableaux 1 à 4). En effet, certains dossiers ont par exemple déjà été ouverts en 2018, alors que la décision n'a été rendue qu'en 2019.

	2014	2015	2016	2017	2018
Audition d'un membre d'une autorité (3)	11	7	10	0	1
Décision du président (4)	0	0	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (5)	78	50	54	80[214]	72
Soustraction d'informations du dossier par le service de renseignement (6)	0	0	0	0	0

(1) L'Organe de recours peut demander l'intégralité du dossier d'enquête aux autorités de sécurité. Comme ce dossier contient davantage de données que le rapport d'enquête seul, cette requête est systématique.
(2) L'Organe de recours peut également demander tout complément d'informations qu'il juge nécessaire pendant la procédure.
(3) L'Organe de recours peut décider d'entendre les membres des services de renseignement et de police ou des autorités de sécurité qui ont participé à l'enquête ou à la vérification de sécurité.
(4) Le président de l'Organe de recours peut décider de permettre au membre du service de renseignement de garder secrètes certaines données pendant son audition.
(5) Si le service de renseignement ou de police concerné le demande, l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant.[215]
(6) Si l'information concernée provient d'un service de renseignement étranger, c'est le service de renseignement belge qui décide si elle peut être communiquée. Il s'agit d'un aspect de l'application de la 'règle du tiers service'.

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

	2014	2015	2016	2017	2018
Consultation du dossier par le requérant et/ou l'avocat	84	84	87	105	69
Audition du requérant (assisté ou non d'un avocat)[216]	115	107	127	158	111

214 Voir *supra* à propos de l'art. 5 § 3 L.Org.recours. À noter que dans la plupart des cas, il n'a été fait que partiellement droit à la demande de soustraction d'informations (parfois en raison d'une motivation inadéquate au vu des exceptions légales).
215 Voir *supra* à propos de l'art. 5 § 3 L.Org.recours.
216 Dans certains dossiers, le requérant (assisté ou non de son avocat) est auditionné à plusieurs reprises.

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

	2014	2015	2016	2017	2018
Habilitations de sécurité (art. 12 et s. L.C&HS)					
Recours irrecevable	0	4	0	3	0
Recours sans objet	3	3	7	0	4
Recours non fondé	12	19	18	13	12
Recours fondé (avec octroi partiel ou complet)	14	24	24	24	12
Devoir d'enquête complémentaire par l'autorité	0	0	2	0	1
Délai supplémentaire pour l'autorité	12	1	2	1	1
Donne acte de retrait de recours	0	1	0	0	3
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)					
Recours irrecevable	0	0	0	1	0
Recours sans objet	0	0	0	1	0
Recours non fondé	2	4	1	0	1
Recours fondé (avec octroi)	0	2	1	1	0
Attestations de sécurité pour lieux ou événements (art. 22*bis*, al.2 L.C&HS)					
Recours irrecevable	0	0	0	1	2
Recours sans objet	0	0	0	1	0
Recours non fondé	6	8	2	12	2
Recours fondé (avec octroi)	8	10	4	7	3
Donne acte de retrait de recours	0	2	0	1	2
Attestations de sécurité pour le secteur nucléaire (art. 8*bis* § 2 L.C&HS)					
Recours irrecevable	–	–	1	1	0
Recours sans objet	–	–	1	0	1
Recours non fondé	–	–	0	1	1
Recours fondé (avec octroi)	–	–	7	5	6
Donne acte de retrait de recours	–	–	–	–	2

	2014	2015	2016	2017	2018
Avis de sécurité (art. 22*quinquies* L.C&HS)					
Organe de recours non compétent	4	0	0	20[217]	12[218]
Recours irrecevable	4	6	15	10	3
Recours sans objet	4	0	0	1	3
Confirmation de l'avis négatif	53	28	42	49	46
Transformation en avis positif	41	23	46	41	27
Donne acte de retrait de recours	0	0	0	1	0
Recours contre des actes normatifs d'une autorité administrative (art. 12 L.Org.recours)	0	0	0	0	0
TOTAL	**163**	**135**	**173**	**195**	**144**

217 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 étaient dépourvus de base juridique parce que l'autorité qui demandait l'avis n'était pas celle qui voulait l'utiliser pour prendre une décision. 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.

218 À la suite des décisions de l'Organe de recours mentionnées dans la note de bas de page précédente, l'autorité a modifié sa méthode de travail dans le cadre de la délivrance d'un avis pour des personnes travaillant pour les institutions européennes. En l'absence de réponse à la critique qu'il avait émise, l'Organe de recours a dû une nouvelle fois se déclarer incompétent dans dix dossiers de ce genre.

CHAPITRE XI
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

XI.1. COMPOSITION DU COMITÉ PERMANENT R

En 2018, la composition du Comité a subi une profonde modification. En effet, le président Guy Rapaille[219] (F), avocat général près la cour d'appel de Liège, a passé le relais à Serge Lipszyc, premier substitut de l'auditeur du travail près l'auditorat du travail de Liège (F), qui a prêté serment le 25 septembre 2018.[220]

Le conseiller Gérald Vande Walle (F) a atteint l'âge de la retraite le 31 décembre 2017 et a été remplacé, début 2018, par Laurent Van Doren, précédemment commissaire divisionnaire de police.[221] Le conseiller Pieter-Alexander De Brock (N) était toujours en fonction.[222]

Le Service d'Enquêtes, composé de cinq commissaires auditeurs, dont le directeur Frank Franceus (N), est resté inchangé.

Le cadre administratif du Comité permanent R, placé sous la direction du greffier Wouter De Ridder (N) est lui aussi resté inchangé et comptait 18 collaborateurs. Toutefois, un Data Protection Officer (DPO) a été désigné pour effectuer tous les traitements de données du Comité qui ne relèvent pas de la 'sécurité nationale' (par exemple, les traitements effectués dans le cadre de la gestion du personnel et de la logistique).

---

219 Conformément à l'avis de la Conférence des Présidents du 10 octobre 2018, Guy Rapaille s'est vu octroyer le titre de président honoraire du Comité permanent R (*C.R.I.*, Chambre 2017-2018, PLEN 251).

220 Le 22 novembre 2018, Vanessa Samain et Didier Maréchal ont été désignés respectivement comme premier et second président suppléant.

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

222 Le 26 septembre 2018, la Chambre des représentants a décidé de publier un appel à candidats pour le mandat de membre néerlandophone et pour les mandats de premier et second membre suppléant néerlandophone. (*C.R.I.*, Chambre 2017-2018, PLEN 245) En effet, le mandat du conseiller De Brock prenait fin le 7 mai 2019. À la date d'approbation du présent rapport d'activités, aucune décision n'a encore été prise.

XI.2. RÉUNIONS AVEC LA COMMISSION DE SUIVI

Dans le courant de l'année 2018, quatre réunions ont eu lieu avec la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de Contrôle des services de renseignement et de sécurité.[223] Les treize membres avec voix délibérative étaient : Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Peter De Roover (N-VA), Laurette Onkelinx (PS), André Frédéric (PS), David Clarinval (MR), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld), Hans Bonte (sp.a), Stefaan Van Hecke (Ecolo-Groen) et Georges Dallemagne (cdH). Le Président de la Chambre Siegfried Bracke (N-VA) a assuré la présidence des réunions de la Commission.

Plusieurs enquêtes de contrôle communes du Comité permanent R et du Comité permanent P ont été discutées à huis clos lors des réunions de la Commission. En outre, du temps a 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 avec l'Organe de contrôle de l'information policière (C.O.C.) – concernant les banques de données (art. 44/6 LPD). Enfin, l'aperçu complet de toutes les recommandations de ces dix dernières années qui n'ont pas encore été concrétisées, transmis par le Comité, a lui aussi fait l'objet de discussions.

En novembre 2018, le *Rapport d'activités 2017* du Comité permanent R a été discuté, et la Commission a pris connaissance de la note prospective 2018-2020 du Comité. La Commission a pris *'acte du rapport d'activités 2017 du Comité R et souscrit à ses recommandations*'.[224]

XI.3. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

Les articles 52 à 55 L.Contrôle déterminent les cas où le Comité permanent R et le Comité permanent P doivent organiser des réunions communes et la manière

223 En juillet 2018, la Commission de suivi a également organisé un échange de vues avec le ministre de la Défense et le Chef du SGRS, en présence de l'ancien président du Comité, sur l'enquête de contrôle relative au fonctionnement de la Direction Counterintelligence.

224 *Doc. parl.*, Chambre 2018-19, 54-3375/001 (Rapport d'activités 2017 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).

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 2018, il a été question de deux enquêtes de contrôle communes : l'enquête initiée précédemment sur les services d'appui de l'OCAM (cf. I.6.3) et l'enquête ouverte en mai 2018 sur la *'position d'information de l'OCAM avant l'attentat commis à Liège'* (cf. I.4).

Par ailleurs, toute une série de points ont été mis à l'ordre du jour : l'adaptation (éventuelle) du statut administratif, la rédaction d'une charte déontologique, la discussion sur l' 'Audit des institutions à dotation', la nouvelle législation relative à la protection de données et, dans ce même cadre, la désignation d'un Data Protection Officer (DPO) commun, etc. Autre point à l'agenda : la préparation des célébrations du 25ème anniversaire des deux Comités.

Huit réunions communes ont été organisées en 2018, sans compter les fréquents contacts informels sur le terrain.

XI.4. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

L'article 57 alinéa 1er L.Contrôle stipule que les crédits de fonctionnement doivent être inscrits au budget des dotations. Le budget est traditionnellement 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.[225] Jusqu'en 2017, la quotité que représentait cette dotation était insuffisante pour financer les dépenses réelles du Comité, ce qui avait pour conséquence une perte structurelle.

Consciente de la situation, la Chambre des représentants a décidé d'adapter la dotation dans un souci d'équilibre et dans un souci de garantir l'exécution des missions légales supplémentaires attribuées au Comité.

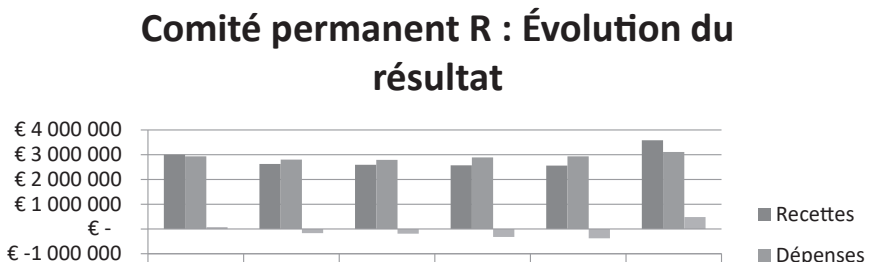
Le 'budget 2018' du Comité permanent R a été fixé à 3,759 millions d'euros, soit une augmentation de 3,4 % par rapport à 2017. Les sources de financement attribuées par la Chambre des représentants[226] sont les suivantes : 95,26 % au titre du budget de dotation et 4,74 % de boni de 2016.

L'exécution du budget 2018 a produit un boni comptable de 475.494 d'euros, ce qui représente la différence entre le budget approuvé et les dépenses constatées.

---

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

226 *Doc. parl.*, Chambre 2017-2018, 54-2843/001, 24-29.



	2013	2014	2015	2016	2017	2018
Recettes	€ 3 005	€ 2 626	€ 2 597	€ 2 570	€ 2 565	€ 3 582
Dépenses	€ 2 935	€ 2 799	€ 2 792	€ 2 889	€ 2 937	€ 3 107
Résultat	€ 70 38	€ -173	€ -194	€ -318	€ -372	€ 475

Ce boni n'empêche pas que la recherche de synergies entre les différentes institutions à dotation demeure une priorité. Le développement de ces synergies n'a eu qu'un impact financier très limité en raison de complications structurelles. Par exemple, les différences de statuts expliquent l'absence de mobilité du personnel des diverses institutions. Ces synergies permettent cependant d'améliorer la collaboration entre les institutions, ce qui favorise la qualité du travail fourni.

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

À la demande de la Commission de la Comptabilité de la Chambre des représentants, la Cour des comptes a initié, en décembre 2017, une enquête sur les institutions à dotation, conjointement avec Ernst & Young. Le Comité permanent R était donc concerné.

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

Afin de pouvoir mener à bien ces missions, les institutions ont dû mettre à disposition de nombreux documents et quantité d'informations. Elles ont également dû répondre à toute une série de questions ponctuelles (décembre 2017). S'appuyant sur les informations reçues, les équipes d'enquête de la Cour des Comptes et de Ernst & Young ont eu des entretiens avec plusieurs personnes clés du Comité (janvier-février 2018). Fin février, le projet de rapport a été soumis pour commentaires lors d'une *exit meeting*.

Cet audit a mobilisé les énergies au Comité permanent R, venant s'ajouter à une charge de travail croissante (*supra*).

Le rapport d'audit[227] a été transmis fin mars 2018 et a été discuté le 12 juin 2018 au sein de la Commission de la Comptabilité.

XI.6. FORMATION

Vu l'intérêt pour l'organisation, le Comité permanent R encourage ses membres et ses collaborateurs à suivre des formations générales (informatique, management…) ou propres au secteur, ou encore à participer à des conférences.[228] Concernant cette dernière catégorie, un ou plusieurs membre(s) du Comité permanent R ou membre(s) de son personnel a/ont assisté aux journées d'étude mentionnées ci-dessous.

DATE	TITRE	ORGANISATION	LIEU
15 février 2018	Naar een herbekijking van de Belgische veiligheidsarchitectuur : de vaststellingen en aanbevelingen van de parlementaire onderzoekscommissie 'Terroristische aanslagen'	KU Leuven	Leuven
20-22 février 2018	Roundtable discussion 'on the outline of the guidelines for intelligence oversight'	Democratic Centre for Armed Forces (DCAF)	Skopje
15 mars 2018	Cybercriminalité & cyberterrorisme	UC Liège	Liège
6 avril 2018	Le renseignement et son contrôle	Conseil d'État, France	Paris
4 mai 2018	High Level Round Table on Public Security	European Corporate Security Association (ECSA) et SAS Institute	Leuven
30 mai 2018	Info session – Implementation of the EU directive 2016/1148	European Corporate Security Association (ECSA) en Center for Cybersecuruty Belgium (CCB)	Bruxelles

227 *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.

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

DATE	TITRE	ORGANISATION	LIEU
29 juin 2018	International collaboration regarding intelligence services and intelligence studies	Belgian Intelligence Studies Centre (BISC)	Bruxelles
24 septembre 2018	'SIGINT intelligence, surveillance, ethics and control' en 'Round table intelligence, surveillance and technology'	Université de Bordeaux	Paris
16 octobre 2018	Crypto War	KU Leuven	Bruxelles
12-19 octobre 2018	Sweepstakes	SHAPE	Lisbonne
22 novembre 2018	10 ans de contrôle parlementaire du renseignement	Parlement, France	Paris
26 novembre 2018	Le futur de la Défense belge	Egmont, Institut Royal des Relations Internationales	Bruxelles
29-30 novembre 2018	International Intelligence Oversight Forum (IIOF 2018)	UN-High Commissioner for Human Rights	Malte
29 novembre 2018	20 ans de la loi organique des services de renseignement et de sécurité	SGRS/VSSE	Bruxelles
6-7 décembre 2018	European Conference for Intelligence Oversight Bodies	Commission nationale de contrôle des techniques de renseignement (CNCTR) et le Comité permanent R	Paris

CHAPITRE XII
RECOMMANDATIONS

À la lumière des enquêtes de contrôle, des contrôles et des inspections clôturés en 2018, le Comité permanent R – parfois avec le Comité permanent P ou l'Organe de contrôle de l'information policière – formule les recommandations reprises ci-après. Elles portent plus particulièrement sur la protection des droits que la Constitution et la loi confèrent aux personnes (XII.1), sur la coordination et l'efficacité des services de renseignement, de l'OCAM et des services d'appui (XII.2) et, enfin, sur l'optimalisation des possibilités d'enquête du Comité permanent R (XII.3).

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

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

L'article 44/4 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 destruction, selon les modalités à fixer par le Roi.*' Le Comité permanent R insiste pour qu'un arrêté royal soit pris en ce sens dans les meilleurs délais.

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

XII.2.1. DIVERSES RECOMMANDATIONS ÉMISES À L'ÉGARD DU SGRS DANS LE CADRE DE L'ENQUÊTE DE CONTRÔLE SUR LA DIRECTION COUNTERINTELLIGENCE

L'enquête relative au fonctionnement de la Direction Counterintelligence (CI) du SGRS donnait un aperçu de la gravité, de la complexité et de la diversité des manquements au sein de ce service.[229] Le Comité était convaincu de l'intérêt, pour la Direction CI, d'avoir une organisation et une gestion qui répondent aux standards d'un service public efficace et efficient. Par conséquent, le Comité a formulé une série de recommandations. En ce qui concerne le délai d'exécution, différents degrés de priorité ont été donnés, allant de 'très haut' (à réaliser pour fin 2018), à 'moyen' (à réaliser pour fin décembre 2019), en passant par 'haut' (à réaliser pour fin juin 2019).

XII.2.1.1. Recommandations assorties d'une très haute priorité

Concernant la mission, la vision et le cycle de planification

- Définir, dans un document formel, la mission et la vision de CI, y compris le rôle et la mission de CI en matière de contre-terrorisme, endossées par tous les intéressés et conformes aux lignes politiques ainsi qu'à la vision et à la mission du SGRS dans son ensemble ;
- Établir une analyse et un plan sur le genre de renseignements (opérationnels *versus* stratégiques) que CI doit produire pour rencontrer les besoins des utilisateurs, en mettant l'accent sur l'analyse proactive et stratégique ;
- Tant en interne (au sein du SGRS, de la Direction CI et aussi vis-à-vis de la Direction I(ntelligence)) qu'à l'extérieur (en collaboration avec la VSSE, le Parquet, l'OCAM, etc.), le SGRS et la Direction CI doivent élaborer une position claire (définie dans des SLA et des protocoles) sur ce qu'on peut et doit attendre du service, et ce compte tenu des moyens disponibles. Une fois que cette position (vision, ambition, stratégie) aura été élaborée, il faudra s'y tenir pour que le service soit perçu comme un partenaire qui compte dans l'anti-terrorisme belge ;

[229] Voir 'Chapitre I.1. Le fonctionnement de la Direction Counterintelligence (CI) du SGRS'.

- Établir et approuver formellement une planification synchronisée à tous les niveaux de CI, en ce compris l'élaboration d'*intelligence requirements* (IR) et d'*information collection plans* (ICP) ;
- Définir, dans une directive interne, la méthodologie, les instruments et les processus utilisés pour la direction et la planification, ainsi que la méthode de suivi et d'évaluation.

Concernant l'organisation, l'affectation des moyens ainsi que la mesure et la répartition de la charge de travail

- Établir un plan concret des besoins et des moyens requis pour l'accomplissement des missions et des tâches, et planifier la manière dont celles-ci seront remplies et orientées ;
- Élaborer un organigramme consolidé définissant les fonctions, l'affectation, les rôles et les lignes de communication ;
- Disposer d'instruments de mesure pour le recueil de données quantitatives au niveau de la charge de travail et de l'*output*, et rassembler les résultats des mesures qui en découlent pour permettre une répartition équilibrée de la charge de travail.

Concernant l'organisation et la collaboration entre l'analyse et la collecte

- Élaborer un plan formel définissant les capacités de collecte et d'analyse requises, et ce pour chaque matière. Il doit être garanti que les capacités sont et restent disponibles. Si nécessaire, envisager une réorganisation de la fonction d'analyse comme pilier indépendant au sein de CI ;
- Élaborer et mettre à disposition des 'conceptions' (*designs*) qui doivent guider la collaboration entre la collecte et l'analyse (*intelligence requirements* et *information collection plans* intégrés).

Concernant la gestion des informations

- Établir un planning et développer un système pour résorber d'urgence le retard dans l'*input* d'informations dans la base de données et pour garantir que les informations entrantes soient introduites dans un délai raisonnable ;
- Effectuer une analyse des besoins à CI, y compris dans les postes de province, et ce afin de déterminer qui a besoin de quels systèmes (accès à des banques de données internes et externes, logiciels, etc.), et la concrétiser ;
- Organiser un cycle d'actualisation pour améliorer la connaissance et l'utilisation des outils IT employés ;
- Établir des méthodes et des procédures internes qui permettront d'éviter les '*broken links*' et qui permettront la constitution de fichiers personnels et la constitution de zones de stockage ;

- Définir des directives internes pour donner corps à la collaboration entre CI et la division J-6 (responsable des systémes de communication et d'information), afin que celle-ci puisse mieux répondre aux besoins de CI ;
- Désigner une fonction-relais ICT qui dispose du temps nécessaire et des connaissances requises.

Concernant les infrastructures

- Améliorer d'urgence les conditions matérielles dans le bâtiment qui abrite la Direction CI ;
- Éliminer les risques pour la sécurité en matière d'*Operations Security* (OpSec) qui découlent d'un manque d'infrastructures matérielles.

XII.2.1.2. Recommandations assorties d'une haute priorité

Concernant la gestion des processus et les *Standing Operating Procedures*

- Élaborer des descriptions de processus et des procédures formelles décrivant les différents aspects du fonctionnement du service, et conserver un recueil actualisé de *Standard Operating Procedures* (SOP). Ce recueil doit être distribué au personnel et expliqué de manière active ;
- Désigner, au sein de CI, un responsable qui supervise la gestion du processus.

Concernant le contrôle interne et la gestion des risques

- Développer et mettre en œuvre, au sein de CI (mais aussi du SGRS), un système de contrôle interne, qui monitore les processus et détecte/corrige toute dérogation aux normes préalablement définies ;
- Développer et mettre en œuvre un système de gestion des risques, dans lequel les risques (opérationnels) sont répertoriés, et prévoir des mesures pour y faire face.

Concernant l'appui et la logistique, dans et en dehors de CI

- Mesurer les besoins en termes d'appui logistique au sein de CI et établir un plan de réalisation ;
- Documenter la collaboration entre CI et les sections d'état-major, afin que celles-ci puissent mieux répondre aux besoins de CI, et désigner des responsables au sein de CI qui serviront de relais (personnel, sécurité, formation, etc.). En tenant compte des exigences de discrétion, il convient, à cet égard, de prévoir que les sections d'état-major reçoivent un accès à toutes les données nécessaires à l'accomplissement de leurs tâches ;
- Chaque plan en matière de systèmes de défense (à l'exception de l'ICT, mais aussi, entre autres, de la gestion des achats) qui s'applique au SGRS et à CI,

doit contenir une étude sur les implications pour le SGRS et CI et sur la manière d'éviter les conséquences indésirables.

Concernant la communication et le feedback

- Élaborer, au sein de CI, des directives de communication claires et formelles (quoi, comment, qui, quand, etc.). La culture de la transmission orale des informations et des instructions serait ainsi abandonnée. Attribuer explicitement la mission et la responsabilité de la communication interne à un membre du personnel dirigeant de CI ;
- Développer et appliquer des systèmes pour le feedback interne et externe à l'intention des membres du personnel concernés.

Concernant la gestion du personnel et des carrières, la formation et l'entraînement

- Répertorier les risques découlant de la croissance rapide du personnel de collecte et déterminer les mesures à prendre. L'objectif est de pas mettre en péril l'équilibre entre la collecte et l'analyse ;
- Développer une filière 'Renseignements' pour les militaires qui veulent travailler dans le service de renseignement, afin qu'ils arrivent parfaitement formés sur le terrain et qu'ils puissent véritablement développer une carrière militaire dans le domaine du renseignement ;
- Définir les besoins en termes de formation et établir un plan de formation dans les domaines où le personnel de CI manque de connaissances (juridiques, opérationnelles) actualisées, et prévoir une formation continue pour y remédier. Idem en ce qui concerne les connaissances de techniques de management pour les (aspirants) dirigeants.

Concernant la culture et le *tradecraft*

- Développer une approche pour concilier les différentes identités et contrer le sentiment 'nous-eux'. L'objectif est *in fine* de développer une véritable 'culture du SGRS', qui serait le fondement de la compréhension et du respect du rôle et de la position de chacun ;
- Consigner une procédure formelle pour traiter des cas délicats au sein de CI, où des personnes et/ou des militaires externes et/ou internes au service pourraient être impliqué(e)s, et ce en tenant compte de la confidentialité requise. Définir clairement les responsabilités, qui doit intervenir et quand, et à qui il faut faire rapport ;
- Organiser une concertation entre les différentes directions du SGRS afin d'aboutir à un consensus sur les principes en matière de *tradecraft* (y compris OpSec), en respectant les positions et rôles respectifs de chaque direction.

Cette concertation devrait aboutir à l'élaboration d'un document/manuel conjoint sur la conception commune de *tradecraft* ;
– Actualiser les règles de *tradecraft* et d'OpSec, en particulier à l'arrivée de nouveaux membres du personnel qui ne sont pas issus du monde du renseignement.

XII.2.1.3. Recommandations assorties d'une priorité moyenne

Concernant les détachements provinciaux

– Examiner les besoins des détachements provinciaux et les domaines dans lesquels ils peuvent constituer une valeur ajoutée. Définir la description des tâches et les moyens requis afin de garantir, pour chaque poste, un effectif minimal et une continuité (influence des congés, maladies, missions, réunions) ;
– Définir et veiller à l'application de règles pour une gestion efficace des détachements provinciaux et pour garantir la transmission requise des informations et des instructions ;
– Examiner les besoins en technologies de l'information et de la communication dans les postes provinciaux (entre autres, les banques de données et les outils ICT).

Concernant les statuts et l'évaluation individuelle

– Étudier et établir un plan pour supprimer les inégalités (notamment pécuniaires) entre les membres du personnel employés sous des statuts différents ;
– Répertorier les problèmes liés aux différents statuts (recrutement, évaluation, sanctions, etc.), même si ceux-ci ne peuvent pas être traités dans l'immédiat.

XII.2.2. LA DÉSIGNATION D'UN *STATION COMMANDER* EN ZONE D'OPÉRATION

Le Comité recommande la désignation d'un '*Station Commander*' lors de tout déploiement militaire en zone d'opération. Il y serait responsable de la coordination de l'ensemble des activités du SGRS pour toutes les directions, et ce en application du principe d'unité de commandement.

XII.2.3. L'ÉVALUATION DE L'IMPLANTATION GÉOGRAPHIQUE DES UNITÉS MILITAIRES

Le Comité permanent R recommande la réalisation d'une évaluation de l'implantation géographique optimale des unités militaires dans le cadre d'un

engagement en opération, compte tenu de l'évolution rapide de la situation sécuritaire et des missions assignées aux unités belges.

XII.2.4. PAS DE CLOISONNEMENT STRICT AU SEIN DU SGRS

À l'exception du cas spécifique où le personnel du SGRS est lui-même soumis à une enquête de sécurité ou de renseignement, le Comité permanent R n'est pas en faveur d'un cloisonnement strict entre les directions du SGRS. À cet égard, il doit être évident que toute personne en possession d'informations classifiées et sensibles est tenue au secret sous peine de sanctions. En revanche, les informations classifiées et sensibles qui concernent le personnel de la Défense ou qui portent sur une menace doivent être partagées au sein du SGRS.

XII.2.5. DIVERSES RECOMMANDATIONS EN VUE D'AMÉLIORER L'EFFICACITÉ DU FONCTIONNEMENT DES SERVICES ET DE LEUR COLLABORATION

L'enquête de contrôle sur l'attentat de Liège n'a révélé aucun manquement dans le chef des services de police, de renseignement et de sécurité. Eu égard aux recommandations de la Commission d'enquête 'Attentats terroristes' de la Chambre des représentants[230], les Comités permanents R et P ont formulé les recommandations reprises ci-après en vue d'améliorer le fonctionnement des services et leur collaboration.

XII.2.5.1. La DG EPI comme service d'appui de l'OCAM

Les ministres compétents devraient prendre l'initiative de désigner la DG EPI comme service d'appui de l'OCAM au vu de l'importance de la position de ce service dans le cadre de la détection et du suivi de la radicalisation des détenus.[231]

---

230 *Doc. parl.*, Chambre, 2017-18, 54-1752/9, titre 2 (Quatrième rapport intermédiaire sur le volet 'Radicalisme' du 23 octobre 2017, chapitre III, point 4, voir en particulier les numéros 151-152 relatifs à l'élaboration d'une formation des agents pénitentiaires, y compris le constat d'indicateurs de radicalisme et la création de 'référents radicalisme' au sein de chaque organisme afin de recueillir et d'analyser les informations extraites de l'observation des détenus, ainsi que les numéros 159-161 concernant l'échange d'informations entre la prison et d'autres services).

231 Cette recommandation a trouvé sa concrétisation dans l'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).

En outre, les conditions requises doivent être réunies pour permettre à la DG EPI de remplir ce rôle au mieux, notamment en prévoyant des moyens pour assurer une collecte et une analyse de qualité en milieu carcéral ou en élaborant des procédures.

XII.2.5.2. Une terminologie univoque dans le cadre normatif

Les instances compétentes doivent examiner les différents textes normatifs qui sont d'application (lois, arrêtés, circulaires, notes de service, etc.) afin de vérifier si la terminologie employée (signes de radicalisation, radicalisé (non) violent, prosélytisme, etc.) est définie de manière explicite, claire et identique, et le cas échéant, d'effectuer les adaptations requises. L'échange de données et une collaboration de qualité supposent que tous les services concernés emploient la même terminologie et l'appréhendent de la même manière.

XII.2.5.3. Fichiers relatifs aux détenus radicalisés

Les services, réunis dans le Groupe de travail Prisons du Plan Radicalisme, devaient soumettre aux ministres compétents, pour fin 2018, une proposition portant sur quelles données relatives aux détenus devraient être reprises (ou, le cas échéant, supprimées), dans quelles conditions et dans quels fichiers/quelles listes et sur les données qu'ils pourraient partager. À cet égard, il convient de :

- Déterminer quelles procédures d'échange de données et de création de banques de données nécessitent une formalisation plus poussée, et formuler des propositions à cet effet ;
- S'accorder sur une définition des tâches en termes d'échange d'informations sur ces personnes, d'analyse et d'accessibilité pour les différents services ; déterminer quelles informations introduire, le cas échéant, dans la banque de données commune (moyennant une adaptation du cadre réglementaire concerné) et les procédures à respecter ;
- Procéder à une estimation des moyens nécessaires pour concrétiser ce qui précède.

Ces différents points ne peuvent compromettre les différentes finalités de tous les services concernés en vue de renforcer la position d'information de chacun de ces services (finalité de renseignement, maintien de l'ordre, lutte contre la criminalité, analyse de la menace, gestion des détenus et déradicalisation).

XII.2.6. RECOMMANDATIONS RELATIVES AUX BANQUES DE DONNÉES COMMUNES[232]

XII.2.6.1. La désignation d'un conseiller en sécurité[233]

La non-désignation d'un conseiller en sécurité ou d'un délégué à la protection des données (DPO) demeure une lacune importante, surtout qu'il s'agit du point de contact du C.O.C. et du Comité permanent R. Les ministres de l'Intérieur et de la Justice qui sont responsables de traitement justifient cette situation en excipant que la LFP serait revue prochainement suite à l'adaptation du cadre juridique relatif à la protection de la vie privée. Le C.O.C. et le Comité permanent R effectuent de leur côté un contrôle sur la base de la réglementation en vigueur (et non future). Par ailleurs, ils ont constaté que l'absence d'un conseiller en sécurité pose des difficultés sur le plan pratique (fin de non-recevoir lors d'un contrôle de loggings demandé par un service, périodes d'indisponibilités soudaines et inexpliquées de la banque de données, absence d'approche coordonnée en matière d'incidents de sécurité, etc.). Le C.O.C. et le Comité permanent R maintiennent donc leur recommandation de procéder aux désignations requises.[234]

XII.2.6.2. Un outil informatique pour le suivi des délais de conservation

Le C.O.C. et le Comité permanent R recommandent une nouvelle fois le développement d'un outil informatique qui permettrait de suivre les délais de conservation des données visés à l'article 44/11/3*bis* § 5 de la LFP.

XII.2.6.3. Obligation d'information en cas d'incident de sécurité

Le C.O.C. et le Comité permanent R souhaitent être tenus étroitement informés en cas d'incident de sécurité susceptible d'affecter la confidentialité de la banque de données commune.

XII.2.6.4. La nécessité de sécuriser la transmission

À la suite d'une mission de contrôle, le C.O.C. et le Comité permanent R n'ont pas eu la confirmation formelle que l'évaluation visée à l'article 44/11/3*quater* LFP est systématiquement et préalablement effectuée en ce qui concerne la transmission (d'extraits) de la carte d'information à des instances tierces (c'est-à-dire des services non visés à l'art. 44/11/3*ter* LFP). En outre, ils ont rappelé leur recommandation antérieurement formulée à propos de la nécessaire sécurisation de la transmission.

---

232 Les premières recommandations avaient déjà été formulées antérieurement (www.comiteri.be).
233 Voir à ce propos COMITÉ PERMANENT R, *Rapport d'activités 2017*, 105-106.
234 Entre-temps, un DPO a été désigné par les deux ministres.

XII.2.6.5. Contrôle spontané des loggings

À l'exception d'un service audité, la recommandation d'exécuter spontanément un contrôle des loggings n'a pas été suivie. Certains services ont déclaré avoir pris des initiatives à ce propos ou qu'ils ne tarderaient pas à en prendre. La recommandation formulée précédemment reste donc d'actualité.

XII.2.6.6. Recommandations relatives aux listes de noms destinées à des tiers

L'adaptation du cadre juridique en ce qui concerne l'extraction et la transmission de listes à des tiers a conduit le C.O.C. et le Comité permanent R à formuler plusieurs recommandations :

- Les comparaisons automatisées présupposent des tests approfondis, et toutes les décisions doivent être prises après une intervention et une validation humaines ;
- Il appartient au service de base assurant la communication d'une liste d'informer adéquatement le tiers destinataire de la liste (quant à la finalité de la liste au regard de la mission légale du destinataire, quant à l'utilisation de la liste exclusivement dans le cadre de cette finalité, quant à la conservation limitée de la liste, quant aux mesures de sécurité et de confidentialité requises, etc.), par exemple par la conclusion d'un protocole d'accord avec le service destinataire ;
- Des précautions doivent être prises pour que l'utilisation de ces listes par les tiers répondent à des conditions de sécurité (confidentialité, intégrité, etc.) équivalentes à celles prévues dans la réglementation portant sur les banques de données communes ;
- La réglementation sur les banques de données communes n'attribuant pas au C.O.C. ni au Comité permanent R la compétence de contrôler l'utilisation des listes par les tiers, le C.O.C. et le Comité permanent R recommandent aux responsables de traitement d'évaluer si le cadre juridique est suffisant à cet égard, c'est-à-dire au regard de la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel

XII.2.6.7. Opérationnalisation des interrogations et accès directs

À la mi-2018, un nombre significatif de services partenaires et de Maisons de Justice ne disposaient toujours pas d'un accès à l'environnement en production de la banque de données commune et, en conséquence, ne l'utilisaient pas. Le C.O.C. et le Comité permanent R ont logiquement recommandé de remédier à cette situation en attirant l'attention des acteurs concernés sur le fait qu'il leur appartient de prendre leurs responsabilités.

En outre, le droit d'interrogation directe de la Direction générale du Centre de crise doit être concrétisé. Enfin, le C.O.C. et le Comité permanent R ont

considéré que le cadre réglementaire devait, le cas échéant, être adapté à la pratique de laquelle il ressort que certains services centraux de la DG EPI alimentent la banque de données, et pas les établissements pénitentiaires eux-mêmes, comme le prévoit pourtant l'AR (F)TF.

XII.2.6.8. Gestion des habilitations de sécurité requises

Le C.O.C. et le Comité permanent R ont recommandé de lancer rapidement les procédures (assez longues) de demandes d'habilitations de sécurité. À l'inverse, il faut systématiquement signaler toute perte du *need to know* d'un membre du personnel, de manière à éviter le maintien d'autorisations d'accès non nécessaires ou la continuation d'enquête de sécurité devenues entre-temps inutiles.

XII.2.6.9. Actualisation des procédures de validation

Les procédures de validation communiquées par certains services, soit antérieurement, soit à l'occasion du contrôle effectué en 2018, ne portaient que sur les FTF et devaient être mises à jour en ce qui concerne les HTF et les PH. En outre, la *Vlaamse Agentschap Jongerenwelzijn* devait mettre en place un système de validation interne[235] (l'article 8 de l'AR TF).

XII.2.7. CAPACITÉ DE TRADUCTION SUPPLÉMENTAIRE DANS LE CADRE DES MISSIONS SIGINT[236]

Afin d'atteindre ses objectifs et d'être en mesure d'accomplir ses missions légales, le SGRS doit pouvoir disposer de moyens humains et techniques suffisants en matière de SIGINT. À cet égard, pallier le manque de personnel chargé des traductions constitue une priorité.

235 Voir 'Chapitre VI. Le contrôle des banques de données communes'.

236 Voir 'Chapitre III. Le contrôle des interceptions à l'étranger, des prises d'images et des intrusions dans des systèmes informatiques'.

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

XII.3.1. L'ENREGISTREMENT ET LA MISE À DISPOSITION DES DONNÉES RELATIVES AUX MÉTHODES ORDINAIRES

Contrairement à la mise en œuvre des méthodes particulières, le Comité ne dispose pas des chiffres relatifs à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires visées à l'article 16/2 L.R&S. Dans son précédent rapport d'activités, le Comité recommandait aux services que ces données soient elles aussi consignées et tenues à disposition.[237] Étant donné que ce n'est pas encore le cas, le Comité réitère cette recommandation.

[237] COMITÉ PERMANENT R, *Rapport d'activités 2017*, 43.

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 2018 AU 31 DÉCEMBRE 2018)

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. – Coordination officieuse en langue allemande, *M.B.* 4 avril 2018

Loi du 21 mars 2018 modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *M.B.* 16 avril 2018

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

Loi du 19 juillet 2018 modifiant des dispositions diverses relatives aux services de police et relatif aux institutions romaines, *M.B.* 21 août 2018

Loi du 19 juillet 2018 modifiant diverses dispositions relatives au statut des militaires du cadre de réserve des Forces armées, *M.B.* 31 août 2018

Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, *M.B.* 5 septembre 2018

Loi du 15 juillet 2018 portant des dispositions diverses Intérieur, *M.B.* 25 septembre 2018

Loi du 13 septembre 2018 portant modification 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, *M.B.* 5 octobre 2018

A.R. 19 décembre 2017 portant répartition partielle, pour ce qui concerne la lutte contre le terrorisme et le radicalisme, du crédit provisionnel inscrit au programme 03-41-1 du budget général des dépenses pour l'année budgétaire 2017 et destiné à couvrir les dépenses concernant le renforcement des mesures prises ainsi qui des initiatives nouvelles en matière de lutte contre le terrorisme et le radicalisme, *M.B.* 10 janvier 2018

A.R. 13 décembre 2017 portant répartition partielle, pour ce qui concerne la lutte contre le terrorisme et le radicalisme, du crédit provisionnel inscrit au programme 03-41-1 du budget général des dépenses pour l'année budgétaire 2017 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.* 15 janvier 2018

A.R. 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité – traduction allemande, *M.B.* 9 mai 2018

A.R. 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.* 30 mai 2018

A.R. 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 1erbis "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, *M.B.* 30 mai 2018

A.R. 28 mai 2018 portant modification de l'arrêté royal du 10 février 2008 définissant la manière de signaler l'existence d'une surveillance par caméra, *M.B.* 1er juin 2018

A.R. 8 mai 2018 modifiant l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *M.B.* 1er juin 2018

A.R. 8 mai 2018 portant déterminant la liste des données et informations qui peuvent être consultées dans le cadre de l'exécution d'une vérification de sécurité, *M.B.* 1er juin 2018

A.R. 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

A.R. 29 mai 2018 modifiant l'arrêté royal du 23 janvier 2007 relatif au personnel de l'Organe de coordination pour l'analyse de la menace, *M.B.* 11 juin 2018

A.R. 18 juin 2018 portant désignation du président de la chambre de recours des services extérieurs de la Sûreté de l'État, *M.B.* 27 juillet 2018

A.R. 22 juillet 2018 relatif à la formation de base des membres du personnel du cadre d'agents de sécurisation de police et du cadre d'assistants de sécurisation de police et fixant l'entrée en vigueur des articles 1, 9 à 13, 15 à 24, 33 à 38 et 41 à 49 de la loi du 12 novembre 2017 relative aux assistants et agents de sécurisation de police et portant modification de certaines dispositions concernant la police, *M.B.* 16 août 2018

A.R. 30 juillet 2018 portant répartition partielle, pour ce qui concerne des dédommagements et des frais de justice, du crédit provisionnel inscrit au programme 06-90-1 du budget général des dépenses pour l'année budgétaire 2018 et destiné à couvrir des frais de justice et dédommagements, arriérés de primes de développement des compétences, cybersécurité, investissements en Défense et autres dépenses diverses, *M.B.* 21 août 2018

A.R. 2 septembre 2018 fixant les modalités de la notification ainsi que les informations transmises à l'Institut, conformément à l'article 33, § 2, alinéa 4, et § 3, alinéa 5, de la loi du 13 juin 2005 relative aux communications électroniques, *M.B.* 7 septembre 2018

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, *M.B.* 12 septembre 2018

A.M. 10 juillet 2018 modifiant, en ce qui concerne la Sûreté de l'État, l'arrêté ministériel du 11 juin 2018 relatif aux délégations de pouvoir du Ministre de la Justice à certaines autorités en matière de passation et d'exécution des marchés publics de travaux, de fournitures et de services et en matière de subventions et de dépenses diverses, *M.B.* 19 juillet 2018

A.M. 3 juillet 2018 déterminant les armes et munitions faisant partie de l'équipement réglementaire des membres du personnel des forces armées et fixant les dispositions particulières relatives à l'acquisition, à la détention, à la garde, au port, à l'utilisation et à la cession de ces armes et munitions, *M.B.* 5 septembre 2018

A.M. 16 octobre 2018 portant organisation interne, délégations de pouvoir et autorisations de signature au sein de la Sûreté de l'État en matière de passation et d'exécution de marchés publics et en matière de dépenses diverses, *M.B.* 24 octobre 2018

Sélection comparative d'attachés relations internationales (m/f/x) (niveau A1), francophones, pour l'administration de la Sûreté de l'État, *M.B.* 10 janvier 2018

Sélection comparative d'attachés relations internationales (m/f/x) (niveau A1), néerlandophones, pour l'administration de la Sûreté de l'État, *M.B.* 10 janvier 2018

Sélection comparative d'experts relations internationales (m/f/x) (niveau B), francophones, pour l'administration de la Sûreté de l'État, *M.B.* 10 janvier 2018

Sélection comparative d'experts relations internationales (m/f/x) (niveau B), néerlandophones, pour l'administration de la Sûreté de l'État, *M.B.* 10 janvier 2018

Appel aux candidats pour les mandats de président et de premier et second présidents suppléants du Comité permanent de contrôle des services de renseignements (Comité R), *M.B.* 25 janvier 2018

Sélections comparatives francophones d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État (SPF Justice) : assistants analystes (m/f/x) – experts en formation (m/f/x) – experts en sécurité (m/f/x) – conseiller en prévention (m/f/x), *M.B.* 31 janvier 2018

Sélections comparatives néerlandophones d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État (SPF Justice) : assistants analystes (m/f/x) – experts en formation (m/f/x) – experts en sécurité (m/f/x) – conseiller en prévention (m/f/x), *M.B.* 31 janvier 2018

Appel aux candidats pour les mandats de président et de premier et second président suppléant du Comité permanent de contrôle des services de renseignements (Comité R) – Erratum, *M.B.* 1er février 2018

Sélection comparative des gestionnaires de réseaux/pare-feux informatiques (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État (SPF Justice), *M.B.* 2 février 2018

Résultat de la sélection comparative de responsables de service budget et comptabilité (m/f/x) (niveau A3), francophones, pour la Sûreté de l'État), *M.B.* 5 février 2018

Sélection comparative de Consultants ICT pour l'OCAM (m/f/x) (niveau B), néerlandophones, pour le SPF Intérieur, *M.B.* 5 février 2018

Appel aux candidats pour les mandats de premier et de second membre suppléant (F) du Comité permanent de contrôle des services de renseignements (Comité R), *M.B.* 6 février 2018

Deuxième appel aux candidats pour les mandats de premier et de second membre suppléant (F) du Comité permanent de contrôle des services de renseignements (Comité R), *M.B.* 26 mars 2018

Circulaire ministérielle du 29 mars 2018 relative aux contrôles de sécurité lors des évènements, *BS* 5 avril 2018

Résultat de la sélection comparative de gestionnaires de réseaux/pare-feux informatiques (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, *M.B.* 16 avril 2018

Sélection comparative de Gestionnaires de système (m/f/x) (niveau B), francophones, pour la Sûreté de l'État. – Numéro de sélection : AFG17252, *M.B.* 27 avril 2018

Résultat de la sélection comparative d'experts relations internationales (m/f/x) (niveau B), francophones, pour l'administration de la Sûreté de l'État, *M.B.* 30 avril 2018

Circulaire du 22 mai 2018 du ministre de la Sécurité et de l'Intérieur et du ministre de la Justice relative à l'échange d'informations et au suivi des terrorist fighters et des propagandistes de haine (Diffusion restreinte AR 24 mars 2000)

Résultat de la sélection comparative d'attachés relations internationales (m/f/x) (niveau A), francophones, pour la Sûreté de l'État, *M.B.* 22 mai 2018

Recrutement, par détachement, et constitution d'une réserve de recrutement de commissaires-auditeurs francophones (m/f), dotés de connaissances particulières en ICT/Data, pour le Service d'Enquêtes du Comité permanent R, *M.B.* 30 mai 2018

Résultat de la sélection comparative d'attachés relations internationales (m/f/x) (niveau A1), néerlandophones, pour la Sûreté de l'État, *M.B.* 4 juin 2018

Résultat de la sélection comparative néerlandophone d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État : Conseillers en prévention (m/f/x), *M.B.* 20 juin 2018

Résultat de la sélection comparative francophone d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État : Conseillers en prévention (m/f/x), *M.B.* 20 juin 2018

Résultat de la sélection comparative néerlandophone d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État : Assistants analystes (m/f/x), *M.B.* 21 juin 2018

Résultat de la sélection comparative francophone d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État : Assistants analystes (m/f/x), *M.B.* 21 juin 2018

Résultat de la sélection comparative francophone d'accession au niveau B (épreuve particulière), pour la Sûreté de l'État : Experts en sécurité (m/f/x), *M.B.* 27 juin 2018

Résultat de la sélection comparative néerlandophone d'accession au niveau B (épreuve particulière), pour la Sûreté de l'État : Experts en sécurité (m/f/x), *M.B.* 27 juin 2018

Résultat de la sélection comparative de Gestionnaires de système (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, *M.B.* 18 juillet 2018

Nouvel appel aux candidats pour le mandat de second membre suppléant (F) du Comité permanent de contrôle des services de renseignements (Comité R), *M.B.* 19 juillet 2018

Sélection comparative de Gestionnaires de carrière (m/f/x) (niveau A1), néerlandophones, pour la Sûreté de l'État, *M.B.* 7 septembre 2018

Sélection comparative d'experts en budget (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, *M.B.* 7 septembre 2018

Sélection comparative de chefs de service logistique (m/f/x) (niveau A3), néerlandophones, pour la Sûreté de l'État, *M.B.* 14 septembre 2018

Sélection comparative de chefs de service logistique (m/f/x) (niveau A3), francophones, pour la Sûreté de l'État, *M.B.* 14 septembre 2018

Appel aux candidats pour le mandat de membre néerlandophone et les mandats de premier et de second membre suppléant (N) du Comité permanent de contrôle des services de renseignements (Comité R), *M.B.* 27 septembre 2018

Protocole d'accord du 13 novembre 2018 relatif à la collaboration entre l'Unité d'information des passagers et le SGRS dans le cadre de la loi relative au traitement des données des passagers (Diffusion restreinte, art. 20 AR 24 mars 2000)

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 2018 AU 31 DÉCEMBRE 2018)

Sénat

Conférence des présidents des Parlements de l'Union européenne, Tallinn, 23-24 avril 2018 – rapport, *Doc. parl.*, Sénat, 2017-2018, nº 6-432/1

Chambre des représentants

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du président et des premier et second présidents suppléants – appel aux candidats, *C.R.I.*, Chambre, 2017-2018, 11 janvier 2018, PLEN 210, p. 52

Projet de loi portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *Doc. parl.*, Chambre, 2017-2018, nos 54-2767/3 à 2767/6 et *C.R.I.*, Chambre, 2017-2018, 18 janvier 2018, PLEN 211, p. 51

Projet de loi modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière, *Doc. parl.*, Chambre, 2017-2018, nos 54-2855/1 à 54-2855/7 et *C.R.I.*, Chambre, 2017-2018, 8 mars 2018, PLEN 217, p. 62

Projet de loi modifiant le Code consulaire, *Doc. parl.*, Chambre, 2017-2018, nos 54-2989/1 à 54-2989/5

Comité permanent de contrôle des services de renseignements et de sécurité – Nomination du président – Candidature introduite, *C.R.I.*, Chambre, 2017-2018,
15 mars 2018, PLEN 219, p. 64

Comité permanent de contrôle des services de renseignements et de sécurité – Nomination du président, *C.R.I.*, Chambre, 2017-2018, 19 avril 2018, PLEN 223, p. 58

Ajustements des budgets des recettes et des dépenses pour l'année budgétaire 2018 – exposé général, *Doc. parl.*, Chambre, 2017-2018, nº 54-3035

Projet de loi modifiant des dispositions diverses relatives aux services de police et relatif aux institutions romaines, *Doc. parl.*, Chambre, 2017-2018, nº 54-3089/1

Projet de loi portant modification de la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, attestations et avis de sécurité, *Doc. parl.*, Chambre, 2017-2018, nos 54-3107/1 à 54-3107/8, *C.R.I.*, Chambre, 2017-2018, 18 juillet 2018, PLEN 242, p. 1 et *C.R.I.*, Chambre, 2017-2018, 19 juillet 2018, PLEN 243, p. 47

Comité permanent de contrôle des services de renseignements et de sécurité – Nomination d'un premier et d'un second membre suppléant (F) – Troisième appel aux candidats, *C.R.I.*, Chambre, 2017-2018, 3 mai 2018, PLEN 227, p. 40

Comité permanent de contrôle des services de renseignements et de sécurité – Nomination d'un premier et d'un second membre suppléant (F) – Candidatures introduites, *C.R.I.*, Chambre, 2017-2018, 28 juin 2018, PLEN 236, p. 77

Projet de loi portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de protêt, *Doc. parl.*, Chambre, 2017-2018, nº 54-3114/1

Projet de loi modifiant la loi du 16 mai 2001 portant statut des militaires du cadre de réserve des Forces armées, *Doc. parl.*, Chambre, 2017-2018, nº 54-3125/1

Projet de loi portant des dispositions diverses Intérieur, *Doc. parl.*, Chambre, 2017-2018, nos 54-3127/1 à 54-3127/3

Proposition de loi modifiant la loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité, *Doc. parl.*, Chambre, 2017-2018, nº 54-3166/1

Proposition de résolution relative à la lutte contre l'antisémitisme, *Doc. parl.*, Chambre, 2017-2018, nº 54-3194/1

L'utilisation de drones dans le secteur de la sécurité et de la défense, *Doc. parl.*, Chambre, 2017-2018, nº 54-3224/1

Échange de vues avec M. Marc De Mesmaeker, commissaire général de la police fédérale, *C.R.I.*, Chambre, 2017-2018, 16 juillet 2018, COM 950, p. 1

Projet de loi portant des dispositions diverses concernant le Registre national et les registres de population, *Doc. parl.*, Chambre, 2017-2018, nº 54-3256/1

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du second membre suppléant francophone – candidature introduite, *C.R.I.*, Chambre, 2017-2018, 20 septembre 2018, PLEN 244, p. 45

Comité P – nomination du président et des premier et second présidents suppléants – candidatures introduites, *C.R.I.*, Chambre, 2017-2018, 26 septembre 2018, PLEN 245, p. 28

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du membre néerlandophone et des premier et second membres suppléants – appel aux candidats, *C.R.I.*, Chambre, 2017-2018, 26 septembre 2018, PLEN 245, p. 28

Projet de loi contenant le budget des Voies et Moyens de l'année budgétaire 2019, *Doc. parl.*, Chambre, 2018-2019, nº 54-3293/1

Proposition de résolution concernant l'évolution et la modernisation du cadre de réserve des forces armées, *Doc. parl.*, Chambre, 2018-2019, nº 54-2683/5

Comité permanent de contrôle des services de police – Nomination du président, *C.R.I.*, Chambre, 2018-2019, 14 novembre 2018, PLEN 254, p. 52

Projet de loi contenant le Budget général des dépenses pour l'année budgétaire 2019, *Doc. parl.*, Chambre, 2018-2019, nos 54-3294/1, 54-3294/18, 54-3294/28, 54-3294/29, 54-3294/33 en 54-3294/39

Justification du budget général des dépenses pour l'année budgétaire 2019, *Doc. parl.*, Chambre, 2018-2019, nos 54-3295/2, 54-3295/3, 54-3295/6, 54-3295/7, 54-3295/8, 54-3295/9, 54-3295/10, 54-3295/16 et 54-3295/17

Note de politique générale, *Doc. parl.*, Chambre, 2018-2019, nos 54-3296/3, 54-3296/5, 54-3296/6, 54-3296/15 et 54-3296/28

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, no 54-3340/1

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 renseignements et de sécurité, Médiateurs fédéraux, Autorité de protection des données, Commissions de nomination pour le notariat, Organe de contrôle de l'information policière, Commission MRD, Commission fédérale de déontologie, *Doc. parl.*, Chambre, 2018-2019, nos 54-3418/1 à 54-3418/5 et *C.R.I.,* Chambre, 2018-2019, 20 décembre 2018, PLEN 264, p. 67

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 2018 AU 31 DÉCEMBRE 2018)

Sénat

Question écrite de M. Taelman au ministre de la Justice sur la 'cybercriminalité – entreprises – mesures' (Sénat, 2014-2015, 4 décembre 2014, Q. no 6-277)

Question écrite de J.-J. De Gucht au ministre de la Justice sur le 'réseau d'aide à des terroristes condamnés – appels à la libération de détenus – contrôle – Sûreté de l'État' (Sénat, 2017-2018, 14 avril 2017, Q. no 6-1379)

Question écrite de J.-J. De Gucht au ministre de la Justice sur le 'réseau d'aide à des terroristes condamnés – appels à la libération de détenus – contrôle – Sûreté de l'État' (Sénat, 2017-2018, 14 avril 2017, Q. no 6-1383)

Question écrite de J.-J. De Gucht au ministre de la Justice sur la 'Sûreté de l'État (VSSE) – services partenaires étrangers – demande d'identification téléphonique – délai de réponse – terrorisme' (Sénat, 2017-2018, 29 novembre 2017, Q. no 6-1671)

Question écrite de J.-J. De Gucht au ministre de la Défense sur le 'Comité permanent R – caractère prédictif du service de renseignement – nécessité d'un feed-back' (Sénat, 2017-2018, 29 novembre 2017, Q. no 6-1673)

Question écrite de J.-J. De Gucht au ministre de la Défense sur le 'Service Général du Renseignement et de la Sécurité (SGRS) – Comité permanent R – position d'information – gestion des données' (Sénat, 2017-2018, 29 novembre 2017, Q. nº 6-1674)

Question écrite de J.-J. De Gucht au ministre de la Justice 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, 2017-2018, 8 décembre 2017, Q. nº 6- 1681)

Question écrite de J.-J. De Gucht au ministre de la Justice 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, 2017-2018, 8 décembre 2017, Q. nº 6- 1687)

Question écrite de J.-J. De Gucht au ministre de la Justice 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, 2017-2018, 8 décembre 2017, Q. nº 6- 1690)

Question écrite de J.-J. De Gucht au ministre de la Justice sur le 'Potentiel scientifique et économique (PSE) – Protection – Relations entre la Sûreté de l'État, les centres de recherche et le secteur privé' (Sénat, 2017-2018, 8 décembre 2017, Q. nº 6- 1693)

Question écrite de J.-J. De Gucht au ministre de la Justice sur la '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, 2017-2018, 29 décembre 2017, Q. nº 6-1737)

Question écrite de P. Van Rompuy au ministre des Affaires sociales sur la 'Sûreté de l'État – cybersécurité – infrastructure réseau de la Chine – sécurité du réseau de téléphonie belge' (Sénat, 2017-2018, 28 juin 2018, Q. nº 6- 1922)

Chambre des représentants

Question de V. Yüksel au ministre de l'Intérieur sur 'l'Internet Referral Unit de la police fédérale' (*C.R.I.*, Chambre, 2017-2018, 10 janvier 2018, COM 795, p. 14, Q. nº 22854)

Question de K. Gabriëls au ministre de l'Intérieur sur le 'niveau 3 de la menace' (*Q.R.*, Chambre, 2017-2018, 10 janvier 2018, nº 141, p. 308, Q. nº 2351)

Question de G. Dallemagne au ministre des Affaires étrangères sur la 'lutte contre le terrorisme – organisation d'une mission en Arabie saoudite' (*Q.R.*, Chambre, 2017-2018, 10 janvier 2018, nº 141, p. 397, Q. nº 1203)

Question de F. Dewinter au ministre de la Justice sur 'Ibrahim El Bakraoui' (*Q.R.*, Chambre, 2017-2018, 10 janvier 2018, nº 141, p. 427, Q. nº 1196)

Question de F. Dewinter au ministre de la Justice sur 'les demandeurs d'asile suspectés de terrorisme ou de complicité terroriste' (*Q.R.*, Chambre, 2017-2018, 10 janvier 2018, nº 141, p. 454, Q. nº 2079)

Question de Ph. Pivin au ministre de la Justice sur les 'faits de radicalisation dans les établissements scolaires' (*Q.R.*, Chambre, 2017-2018, 10 janvier 2018, nº 141, p. 461, Q. nº 2158)

Question de Ph. Pivin au ministre de l'Intérieur, sur 'le retrait du permis de séjour de l'imam de la Grande Mosquée' (*C.R.I.*, Chambre, 2017-2018, 17 janvier 2018, COM 797, p. 2, Q. nº 22314)

Questions jointes de K. Jadin et V. Yüksel au ministre de la Défense sur 'Ies effets de l'opération Vigilant Guardian' (*C.R.I.*, Chambre, 2017-2018, 17 janvier 2018, COM 798, p. 10, Q. nos 22747 et 23031)

Question de K. Metsu au ministre de la Justice sur 'les services de renseignements au sein des prisons' (*C.R.I.*, Chambre, 2017-2018, 17 janvier 2018, COM 799, p. 25, Q. no 22976)

Question de K. Metsu au ministre de la Justice sur 'le multilinguisme des gardiens de prison' (*C.R.I.*, Chambre, 2017-2018, 17 janvier 2018, COM 799, p. 26, Q. no 22977)

Question de K. Metsu au ministre de la Justice sur 'les profils à risque dans nos prisons' (*C.R.I.*, Chambre, 2017-2018, 17 janvier 2018, COM 799, p. 24, Q. no 22978)

Question de C. Van Cauter au ministre de la Justice sur 'le suivi des personnes condamnées pour des infractions terroristes' (*C.R.I.*, Chambre, 2017-2018, 17 janvier 2018, COM 799, p. 21, Q. no 23015)

Question de F. Dewinter au ministre de l'Intérieur sur 'les demandeurs d'asile suspectés de terrorisme ou de complicité terroriste' (*Q.R.*, Chambre, 2017-2018, 17 janvier 2018, no 142, p. 175, Q. no 2456)

Question de K. Gabriëls au ministre de l'Intérieur sur 'l'arrestation du prédicateur de haine Chadlioui' (*Q.R.*, Chambre, 2017-2018, 17 janvier 2018, no 142, p. 192, Q. no 2611)

Question de K. Gabriëls au ministre de l'Intérieur sur 'l'attentat terroriste à Bruxelles-Central le 20 juin 2017' (*Q.R.*, Chambre, 2017-2018, 17 janvier 2018, no 142, p. 196, Q. no 2625)

Question de B. Vermeulen au ministre de l'Intérieur sur 'les réseaux locaux, régionaux et fédéraux de caméras ANPR' (*Q.R.*, Chambre, 2017-2018, 17 janvier 2018, no 142, p. 230, Q. no 2712)

Questions jointes de Ph. Pivin et G. Dallemagne au ministre de l'Intérieur sur 'les négociations relatives à la Grande Mosquée de Bruxelles' (*C.R.I.,* Chambre, 2017-2018, 18 janvier 2018, PLEN 211, 10, Q. nos 2545 et 2546)

Question de T. Vandenput au ministre des Affaires étrangères sur 'la rencontre avec le ministre saoudien des Affaires étrangères' (*C.R.I.,* Chambre, 2017-2018, 18 janvier 2018, PLEN 211, 16, Q. no 2551)

Question de V. Wouters au Premier ministre sur 'le contrôle parlementaire : les réponses apportées aux questions par les ministres du gouvernement Michel' (*C.R.I.,* Chambre, 2017-2018, 18 janvier 2018, PLEN 211, 23, Q. no 2555)

Question de Ph. Pivin au ministre de la Justice sur le 'service de renseignements – uniformisation des techniques de fichage' (*Q.R.*, Chambre, 2017-2018, 29 janvier 2018, no 143, p. 281, Q. no 891)

Question de W. Janssen au ministre de la Justice sur le 'SPF Justice – un parc automobile plus respectueux de l'environnement' (*Q.R.*, Chambre, 2017-2018, 29 janvier 2018, no 143, p. 321, Q. no 2202)

Question de S. Crusnière au ministre de la Justice sur le 'Brabant wallon – état des effectifs au sein des parquets' (*Q.R.*, Chambre, 2017-2018, 29 janvier 2018, no 143, p. 333, Q. no 2233)

Question de B. Hellings au ministre de la Justice sur 'la mort de Dag Hammarskjöld. – enquête de l'ONU' (*Q.R.*, Chambre, 2017-2018, 29 janvier 2018, no 143, p. 338, Q. no 2262)

Question de G. Dallemagne au ministre des Affaires étrangères sur 'la situation des Belges arrêtés en Iraq et en Syrie' (*C.R.I.,* Chambre, 2017-2018, 1er février 2018, PLEN 213, 43, Q. nº 2601)

Question de G. Calomne au ministre de la Justice sur 'la brochure de la Sûreté de l'État sur le salafisme' (*C.R.I.,* Chambre, 2017-2018, 1er février 2018, PLEN 213, p. 40, Q. nº 2602)

Question de V. Yüksel au ministre de la Défense sur 'la situation des Belges arrêtés en Iraq et en Syrie' (*C.R.I.,* Chambre, 2017-2018, 1er février 2018, PLEN 213, 45, Q. nº 2605)

Question de A. Top au ministre de la Défense 'la collaboration avec la milice kurde YPG en Syrie' (*C.R.I.*, Chambre, 2017-2018, 7 février 2018, COM 815, p. 6, Q. nº 23489)

Question de É. Thiébaut au ministre de l'Intérieur sur 'la fusillade raciste en Italie et la surveillance de l'extrême droite' (*C.R.I.*, Chambre, 2017-2018, 7 février 2018, COM 817, p. 17, Q. nº 23553)

Question de G. Calomne au ministre de l'Intérieur sur 'le dark web' (*Q.R.*, Chambre, 2017-2018, 9 février 2018, nº 144, p. 113, Q. nº 2435)

Question de K. Degroote au ministre de l'Intérieur sur 'l'évolution du nombre excédentaire d'officiers' (*Q.R.*, Chambre, 2017-2018, 16 février 2018, nº 145, p. 162, Q. nº 2808)

Question de K. Jadin au ministre de l'Intérieur sur les 'espions dans nos prisons' (*Q.R.*, Chambre, 2017-2018, 16 février 2018, nº 145, p. 188, Q. nº 2870)

Question de K. Jadin au ministre de l'Intérieur sur 'la restructuration du monde du renseignement' (*Q.R.*, Chambre, 2017-2018, 16 février 2018, nº 145, p. 191, Q. nº 2893)

Question de G. Calomne au ministre de l'Intérieur sur 'le screening du radicalisme auprès des réfugiés' (*Q.R.*, Chambre, 2017-2018, 16 février 2018, nº 145, p. 293, Q. nº 1296)

Question de B. Hellings au ministre de la Défense sur 'le suivi des *foreign terrorist fighters* belges encore présents en Irak et en Syrie' (*C.R.I.*, Chambre, 2017-2018, 28 février 2018, COM 828, p. 15, Q. nº 23834)

Question d'A. Frédéric au ministre de la Justice sur 'la Sûreté de l'État et les sectes' (*C.R.I.*, Chambre, 2017-2018, 28 février 2018, COM 829, p. 4, Q. nº 23753)

Question de S. Van Hecke au ministre de la Justice sur 'la réforme de l'avis de sécurité émis sur les maisons de cultes dans le cadre d'une demande d'agrément' (*C.R.I.*, Chambre, 2017-2018, 28 février 2018, COM 829, p. 18, Q. nº 23807)

Question de G. Dallemagne au ministre de la Justice sur 'l'information concernant Oussama Atar' (*C.R.I.*, Chambre, 2017-2018, 28 février 2018, COM 829, p. 22, Q. nº 23941)

Questions jointes de H. Bonte et P. Dewael au ministre de la Justice sur 'la base de données sur les terroristes' (*C.R.I.,* Chambre, 2017-2018, 1er mars 2018, PLEN 216, 11, Q. nos 2660 et 2661)

Questions jointes de M. Van Hees, B. Hellings, R. Hedebouw, O. Maingain, M. De Coninck, W. De Vriendt et J. Fernandez Fernandez au ministre de l'Intérieur sur 'la vérification de l'article 3 de la Convention européenne des droits de l'homme' (*C.R.I.,* Chambre, 2017-2018, 6 mars 2018, COM832, 8, Q. nos 23134, 23135, 23438, 23475, 23482, 23740, 23814, 24062, 24063, 24070 et 24082)

Questions jointes de B. Vermeulen et S. Lahaye-Battheu au ministre de l'Intérieur sur 'la migration de transit' (*C.R.I.,* Chambre, 2017-2018, 7 mars 2018, COM835, 6, Q. nos 24051 et 24163)

Question de B. Hellings au ministre des Affaires étrangères sur 'le suivi des Foreign Terrorist Fighters belges encore présents en Irak et en Syrie' (*C.R.I.,* Chambre, 2017-2018, 7 mars 2018, COM838, 31, Q. nº 23836)

Question de V. Yüksel au ministre de la Défense sur 'la participation et la contribution de l'armée belge aux opérations contre l'EI' (*C.R.I.,* Chambre, 2017-2018, 8 mars 2018, PLEN 217, 23, Q. nº 2689)

Question de F. Dewinter au ministre de la Justice sur 'le screening des candidats à l'asile pour déceler des liens avec des groupes terroristes ou radicaux et potentiellement violents' (*Q.R.*, Chambre, 2017-2018, 29 mars 2018, nº 150, p. 210, Q. nº 2409)

Question de K. Jadin au ministre de la Justice sur 'les services secrets kazakhs en Belgique' (*Q.R.*, Chambre, 2017-2018, 29 mars 2018, nº 150, p. 223, Q. nº 2475)

Question de B. Pas au ministre de l'Intérieur sur 'les transactions financières en lien avec le terrorisme' (*Q.R.*, Chambre, 2017-2018, 4 avril 2018, nº 151, p. 152, Q. nº 1883)

Question de Ph. Pivin au ministre de la Justice sur la 'transmission des informations entre services de renseignement européens' (*Q.R.*, Chambre, 2017-2018, 4 avril 2018, nº 151, p. 213, Q. nº 2286)

Question de P. Buysrogge au ministre de la Justice sur la 'VSSE – investissements dans l'infrastructure' (*Q.R.*, Chambre, 2017-2018, 4 avril 2018, nº 151, p. 230, Q. nº 2470)

Question de B. Vermeulen au ministre de la Défense sur les 'faux profils sur les réseaux sociaux, cyberespionnage contre des collaborateurs de l'État' (*Q.R.*, Chambre, 2017-2018, 4 avril 2018, nº 151, p. 317, Q. nº 1445)

Question de K. Jadin au ministre de la Défense sur 'la restructuration du monde du renseignement' (*Q.R.*, Chambre, 2017-2018, 4 avril 2018, nº 151, p. 320, Q. nº 1442)

Question de P. Luykx au ministre des Affaires étrangères sur 'la sécurisation des représentations belges à risque' (*Q.R.*, Chambre, 2017-2018, 20 avril 2018, nº 153, p. 238, Q. nº 1339)

Question de K. Metsu au ministre de la Justice sur le 'retour des épouses de jihadistes parties en Syrie' (*Q.R.*, Chambre, 2017-2018, 9 mai 2018, nº 155, p. 330, Q. nº 2303)

Question de B. Vermeulen au ministre de la Justice sur les 'faux profils sur les réseaux sociaux – cyberespionnage contre des collaborateurs de l'État' (*Q.R.*, Chambre, 2017-2018, 9 mai 2018, nº 155, p. 335, Q. nº 2354)

Question de Ph. Pivin au ministre de la Défense sur la 'sécurisation de l'espace public – coordination Vigilant Guardian' (*Q.R.*, Chambre, 2017-2018, 9 mai 2018, nº 155, p. 452, Q. nº 1461)

Question de B. Vermeulen au ministre de l'Intérieur sur 'la mention d'une nationalité supplémentaire dans le Registre national' (*C.R.I.,* Chambre, 2017-2018, 25 avril 2018, COM880, p. 22, Q. nº 24867)

Question de S. Van Hecke au ministre de la Justice sur la 'réforme de l'avis de sécurité concernant les lieux de culte dans le cadre d'une demande d'agrément' (*Q.R.*, Chambre, 2017-2018, 17 mai 2018, nº 156, p. 237, Q. nº 2304)

Questions jointes de B. Helling, P. Vanvelthoven et G. Dallemagne au ministre des Finances sur 'la livraison – à 24 reprises par 3 entreprises belges – de produits

chimiques pouvant servir à la production d'armes chimiques en Syrie' (*C.R.I.,* Chambre, 2017-2018, 22 mai 2018, COM901, p. 14, Q. nos 25283, 25335 et 25344)

Questions jointes de D. Van der Maelen et B. Hellings au ministre des Affaires étrangères sur 'la désignation d'un haut fonctionnaire indépendant dans le cadre de l'enquête sur la mort de Dag Hammarskjöld' (*C.R.I.,* Chambre, 2017-2018, 23 mai 2018, COM904, p. 18, Q. nos 24839 et 25006)

Question de G. Dallemagne au ministre de l'Intérieur sur 'le signalement d'O. Atar à Interpol' (*C.R.I.,* Chambre, 2017-2018, 30 mai 2018, COM909, p. 1, Q. no 25257)

Questions jointes d'O. Maingain, B. Pas, C. Van Cauter, L. Onkelinx, S. Van Hecke, R. Hedebouw, H. Bonte, S. De Wit, Ph. Pivin, M. de Lamotte, R. Terwingen, V. Wouters, M. Gerkens et A. Carcaci au ministre de l'Intérieur sur 'l'attentat terroriste à Liège' (*C.R.I.,* Chambre, 2017-2018, 31 mai 2018, PLEN 231, p. 2, Q. nos 2884 à 2896 et 2904)

Questions jointes de W. De Vriendt, T. Vandenput, A. Top, S. Crusnière et P. Buysrogge au ministre de la Défense sur les activités du SGRS en Syrie' (*C.R.I.,* Chambre, 2017-2018, 31 mai 2018, COM919, p. 23, Q. nos 25692, 25696, 25716, 25725 et 26050)

Question de Ph. Pivin au ministre de l'Intérieur sur la 'base de données centrale terrorisme' (*Q.R.*, Chambre, 2017-2018, 6 juin 2018, no 158, p. 230, no 3088)

Question de Ph. Pivin au ministre de l'Intérieur sur la 'sécurisation de l'espace public – Coordination Vigilant Guardian' (*Q.R.*, Chambre, 2017-2018, 6 juin 2018, no 158, 232, no 3114)

Question de G. Calomne au ministre de la Justice sur 'les nouvelles méthodes particulières de recherche et d'investigation de la Sûreté de l'État' (*Q.R.*, Chambre, 2017-2018, 6 juin 2018, no 158, p. 338, no 2648)

Question de B. Vermeulen au ministre de la Défense sur 'les militaires et le personnel civil de la Défense possédant plusieurs nationalités' (*Q.R.*, Chambre, 2017-2018, 6 juin 2018, no 158, p. 399, no 1483)

Question de S. Lahaye-Battheu au ministre de l'Intérieur sur 'le cadre du personnel de la police locale et fédérale' (*Q.R.*, Chambre, 2017-2018, 12 juin 2018, no 159, p. 267, no 1144)

Question de B. Vermeulen au ministre de l'Intérieur 'faux profils sur les réseaux sociaux – cyberespionnage contre des collaborateurs de l'État' (*Q.R.*, Chambre, 2017-2018, 12 juin 2018, no 159, p. 284, no 2844)

Question de K. Degroote au ministre de l'Intérieur 'les causes des pénuries de personnel à la police' (*Q.R.*, Chambre, 2017-2018, 12 juin 2018, no 159, p. 287, no 2863)

Question de P. De Roover au ministre de la Justice sur 'le rapport de l'OCAM concernant la Grande Mosquée' (*C.R.I.,* Chambre, 2017-2018, 13 juin 2018, COM923, p. 1, Q. no 25751)

Question de B. Vermeulen au ministre de la Justice sur 'le financement de mosquées par des fonds issus du trafic de stupéfiants' (*C.R.I.,* Chambre, 2017-2018, 13 juin 2018, COM923, p. 2, Q. no 25728)

Question de J.-J. Flahaux au ministre des Affaires étrangères 'la conférence internationale sur le financement du terrorisme' (*Q.R.*, Chambre, 2017-2018, 18 juin 2018, no 160, p. 140, Q. no 1358)

Question de A. Frédéric au ministre de la Justice sur 'la composition de la tête de l'OCAM' (*C.R.I.,* Chambre, 2017-2018, 20 juin 2018, COM930, p. 1, Q. no 25752)

Questions jointes de C. Van Cauter et S. De Wit au ministre de la Justice sur 'la détention limitée d'un prisonnier radicalisé' (*C.R.I.,* Chambre, 2017-2018, 20 juin 2018, COM930, p. 3, Q. nos 26127 et 26228)

Questions jointes de C. Van Cauter et A. Lambrecht au ministre de la Justice sur 'l'arrestation d'un contact de Benjamin Herman' (*C.R.I.,* Chambre, 2017-2018, 20 juin 2018, COM930, p. 7, Q. nos 25944 et 26017)

Question de S. De Wit au ministre de la Justice sur 'le transfert d'informations vers la police et les bourgmestres lors des libérations temporaires ou conditionnelles de certains détenus' (*C.R.I.,* Chambre, 2017-2018, 20 juin 2018, COM930, p. 18, Q. no 26231)

Question de Ph. Goffin au ministre de la Justice sur 'les délais d'obtention des habilitations de sécurité par les directeurs de prison' (*C.R.I.,* Chambre, 2017-2018, 20 juin 2018, COM930, p. 21, Q. no 26164)

Question de B. Friart au ministre de l'Intérieur sur 'les effectifs de la police' (*Q.R.*, Chambre, 2017-2018, 22 juin 2018, no 161, p. 100, Q. no 2219)

Question de A. Top au ministre de l'Intérieur sur 'les corps de police du Grand Bruxelles' (*Q.R.*, Chambre, 2017-2018, 22 juin 2018, no 161, p. 107, Q. no 2720)

Question de B. Pas au ministre de l'Intérieur sur la 'Police fédérale et locale – évolution' (*Q.R.*, Chambre, 2017-2018, 22 juin 2018, no 161, p. 115, Q. no 2987)

Question de P. Luykx au ministre des Affaires étrangères sur la 'l'accréditation des diplomates en Belgique' (*Q.R.*, Chambre, 2017-2018, 22 juin 2018, no 161, p. 191, Q. no 1364)

Question de V. Yüksel au ministre de la Défense sur 'l'externalisation au ministère de la Défense' (*C.R.I.,* Chambre, 2017-2018, 27 juin 2018, COM936, p. 12, Q. no 26051)

Question de G. Dallemagne au Premier ministre sur 'le financement du terrorisme' (*Q.R.*, Chambre, 2017-2018, 29 juin 2018, no 162, p. 97, Q. no 320)

Question de K. Jadin au Premier ministre sur 'le financement du terrorisme' (*Q.R.*, Chambre, 2017-2018, 29 juin 2018, no 162, p. 102, Q. no 321)

Question de F. Schepmans au ministre de la Défense sur les 'cybersécurité-experts' (*Q.R.*, Chambre, 2017-2018, 29 juin 2018, no 162, p. 229, Q. no 1509)

Questions jointes de B. Vermeulen et Yüksel au ministre de l'Intérieur sur 'l'influence exercée sur le débat public au moyen des médias sociaux' (*C.R.I.,* Chambre, 2017-2018, 18 juillet 2018, COM954, p. 12, Q. nos 26354 en 26631)

Question de B. Lutgen au ministre de la Défense sur les 'attachés de défense à l'étranger' (*Q.R.*, Chambre, 2017-2018, 20 juillet 2018, no 164, p. 336, Q. no 1547)

Question de B. Hellings au ministre de l'Intérieur sur le 'CGRA. – règles en matière de gestion des médias sociaux' (*Q.R.*, Chambre, 2017-2018, 20 juillet 2018, no 164, p. 463, Q. no 1418)

Question de E. Burton au ministre de la Justice sur 'les détenus radicalisés ou qui risquent de se radicaliser' (*Q.R.*, Chambre, 2017-2018, 3 août 2018, no 165, p. 351, Q. no 2561)

Question de G. Calomne au ministre de la Justice sur 'les véhicules de services publics équipés de moteurs au diesel' (*Q.R.*, Chambre, 2017-2018, 3 août 2018, no 165, p. 386, Q. no 2777)

Question de J.-J. Flahaux au ministre de la Justice sur la 'lutte contre le terrorisme – coopération franco-belge' (Q.R., Chambre, 2017-2018, 3 août 2018, no 165, p. 392, Q. no 2789)

Question de G. Dallemagne au ministre de la Justice sur 'les projets financés avec la provision terrorisme' (Q.R., Chambre, 2017-2018, 3 août 2018, nº 165, p. 396, Q. nº 2793)

Question de N. Lijnen au ministre des Affaires étrangères sur 'l'implication de l'Iran dans un attentat déjoué' (*Q.R.*, Chambre, 2017-2018, 4 septembre 2018, nº 167, p. 272, Q. nº 1495)

Question de P. Luykx au ministre des Affaires étrangères sur 'la contribution des ambassades belges à l'identification des combattants revenant de Syrie' (*Q.R.*, Chambre, 2017-2018, 19 septembre 2018, nº 167, p. 211, Q. nº 231)

Questions jointes de J Chabot et G. Dallemagne au ministre de la Défense sur 'le Service Général du Renseignement et de la Sécurité (SGRS)' (*C.R.I.,* Chambre, 2017-2018, 19 septembre 2018, COM960, p. 16, Q. nºs 26671 et 26915)

Question de G. Dallemagne au ministre des Affaires étrangères sur 'la position de l'Arabie saoudite concernant la Grande Mosquée de Bruxelles' (*C.R.I.,* Chambre, 2017-2018, 20 septembre 2018, PLEN 244, p. 21, Q. nº 3070)

Question de W. De Vriendt au ministre des Affaires étrangères sur la 'présence militaire terrestre belge en Syrie' (*Q.R.*, Chambre, 2017-2018, 28 septembre 2018, nº 170, p. 107, Q. nº 1487)

Question de G. Calomne au ministre de la Justice sur la 'Sûreté de l'État – recrutements' (*Q.R.*, Chambre, 2017-2018, 28 septembre 2018, nº 170, p. 143, Q. nº 2613)

Question de L. Onkelinx au ministre de l'Intérieur sur 'les mesures prises à la police fédérale pour se prémunir contre d'éventuelles intrusions informatiques et cyberattaques' (*C.R.I.,* Chambre, 2017-2018, 3 octobre 2018, COM974, p. 1, Q. nº 26648)

Question de E. Burton au ministre de la Justice sur 'les compétences linguistiques des agents pénitentiaires responsables des sections Deradex' (*Q.R.*, Chambre, 2018-2019, 8 octobre 2018, nº 171, p. 372, Q. nº 2560)

Question de G. Calomne au ministre de la Justice sur 'le recrutement par les réseaux terroristes de personnes fragilisées' (*Q.R.*, Chambre, 2018-2019, 8 octobre 2018, Q. nº 171, p. 379, Q. nº 2752)

Question de B. Vermeulen au ministre de la Justice sur le 'financement étranger de partis politiques' (*Q.R.*, Chambre, 2018-2019, 8 octobre 2018, nº 171, p. 387, Q. nº 2799)

Question de B. Hellings au ministre de la Justice sur la 'conformité de la pratique du parquet de Bruxelles avec l'esprit du Code de la nationalité belge' (*Q.R.*, Chambre, 2018-2019, 16 octobre 2018, nº 172, p. 189, Q. nº 789)

Question de G. Dallemagne au ministre des Affaires étrangères sur 'l'attentat déjoué de Villepinte et l'absence de réaction de la Belgique' (*C.R.I.,* Chambre, 2018-2019, 17 octobre 2018, COM982, p. 19, Q. nº 27126)

Question de J. Chabot au ministre de la Défense sur 'le SGRS et les menaces de cyberattaques' (*C.R.I.,* Chambre, 2018-2019, 7 novembre 2018, COM992, p. 4, Q. nº 27147)

Question de Ph. Pivin au ministre de la Justice sur 'les conditions de libération des prisonniers radicalisés (*C.R.I.,* Chambre, 2018-2019, 7 novembre 2018, COM994, p. 8, Q. nº 27326)

Question H. Bonte au ministre de l'Intérieur sur 'l'Unification des zones de police bruxelloises – nécessité d'une initiative gouvernementale' (*Q.R.*, Chambre, 2018-2019, 9 novembre 2018, nº 177, p. 153, Q. nº 2290)

Question P. Dewael au ministre de l'Intérieur sur 'le financement des mosquées depuis les États du Golfe' (*Q.R.*, Chambre, 2018-2019, 9 novembre 2018, nº 177, p. 163, Q. nº 3212)

Question J.-J. Flahaux au ministre de l'Intérieur sur les 'personnes fichées en Belgique.' (*Q.R.*, Chambre, 2018-2019, 9 novembre 2018, nº 174, p. 177, Q. nº 3314)

Question V. Yüksel au ministre de la Justice sur 'les combattants syriens de retour en Belgique' (*Q.R.*, Chambre, 2018-2019, 9 novembre 2018, nº 174, p. 350, Q. nº 2009)

Question K. Degroote au ministre de l'Intérieur sur 'l'effectif de la police intégrée' (*Q.R.*, Chambre, 2018-2019, 22 novembre 2018, nº 175, p. 150, Q. nº 3490)

Question D. Van der Maelen au ministre des Affaires étrangères sur 'la reprise d'informations publiées par Sputnik News sur une chaîne de réseaux sociaux officielle du ministre belge des Affaires étrangères' (*Q.R.*, Chambre, 2018-2019, 22 novembre 2018, nº 175, p. 261, Q. nº 1536)

Question G. Dallemagne au ministre des Affaires étrangères sur 'les interférences russes en faveur de l'extrême-droite dans la campagne électorale en Italie' (*Q.R.*, Chambre, 2018-2019, 22 novembre 2018, nº 175, p. 273, Q. nº 1543)

Question de B. Vermeulen au Premier ministre sur 'le CCB' (*Q.R.*, Chambre, 2018-2019, 6 décembre 2018, nº 176, p. 133, Q. nº 345)

Question de B. Vermeulen au Premier ministre sur 'l'ingérence de puissances étrangères pendant les élections en Belgique' (*Q.R.*, Chambre, 2018-2019, 6 décembre 2018, nº 176, p. 140, Q. nº 348)

Question de K. Degroote au ministre de l'Intérieur sur 'la mobilité au sein de la police intégrée' (*Q.R.*, Chambre, 2018-2019, 6 décembre 2018, nº 176, p. 191, Q. nº 3487)

Question de H. Bonte au ministre de la Justice sur 'les Foreign terrorist fighters et le secteur des jeux de hasard' (*Q.R.*, Chambre, 2018-2019, 6 décembre 2018, nº 176, p. 243, Q. nº 2373)

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, 6 décembre 2018, nº 176, p. 245, Q. nº 2539)

Question H. Bonte au ministre de la Justice sur 'la libération d'un prédicateur de haine et la nécessité d'une mise à disposition' (*C.R.I.,* Chambre, 2018-2019, 13 décembre 2018, PLEN 262, p. 17, Q. nº 3306)

Questions jointes de V. Matz, Ph. Pivin et S. De Crom au ministre de l'Intérieur sur 'les grèves de policiers' (*C.R.I.,* Chambre, 2018-2019, 13 décembre 2018, PLEN 262, p. 12, Q. nºs 3301 à 3303)

Question de A. Lambrecht au ministre de la Justice sur 'les détenus radicalisés' (*Q.R.*, Chambre, 2018-2019, 21 décembre 2018, nº 177, p. 67, Q. nº 2474)

Question de P. De Roover au ministre de la Justice sur les 'institutions religieuses – flux de financement étrangers' (*Q.R.*, Chambre, 2018-2019, 21 décembre 2018, nº 177, p. 77, Q. nº 2723)

ANNEXE D.
RENFORCEMENT DU CONTRÔLE DES ÉCHANGES INTERNATIONAUX DE DONNÉES ENTRE LES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

Co-rédigé par:

Belgian Standing Intelligence Agencies Review Committee
(Comité permanent de contrôle des services de renseignement et de sécurité / Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten)
www.comiteri.be

Danish Intelligence Oversight Board
(Tilsynet med Efterretningstjenesterne)
www.tet.dk

Review Committee on the Intelligence and Security Services - The Netherlands
(Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten)
www.ctivd.nl

EOS Committee - The Norwegian Parliamentary Intelligence Oversight Committee
(EOS-utvalget)
www.eos-utvalget.no

Independent Oversight Authority for Intelligence Activities (OA-IA)
(Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND/ Autorité de surveillance indépendante des activités de renseignement AS-Rens)
www.ab-nd.admin.ch

1. CONTENU

Cinq organes de contrôle européens des services de renseignement ont initié une nouvelle forme de coopération. Dans la présente déclaration, nous :

- Décrirons notre projet, qui a amené chacun de nous à réaliser une enquête sur l'utilisation, par nos services nationaux respectifs, des informations concernant les *foreign terrorist fighters* et à partager ses méthodes, ses meilleures pratiques et ses expériences.
- Aborderons les défis auxquels nous sommes confrontés dans le cadre du contrôle effectué sur les échanges internationaux de données, y compris le risque de lacunes en matière de contrôle dans le contexte de la coopération entre les services de renseignement au niveau international.
- Identifierons des voies de progrès pour un renforcement de la coopération en matière de contrôle, par exemple en limitant le secret entre les organes de contrôle, et ce afin de permettre l'échange de certaines informations. L'objectif étant d'améliorer notre contrôle sur les échanges internationaux de données.

2. INTRODUCTION

Les récents attentats terroristes, comme ceux qui ont touché Paris, Bruxelles et Londres, ont été perpétrés par des personnes téléguidées, encouragées ou inspirées par l'EIIL, Al-Qaeda ou des groupes terroristes similaires. Identifier et analyser la menace que constituent les *returnees* et les *homegrown terrorist fighters* est une mission importante des services de renseignement et de sécurité dans toute l'Europe.

Au cours de ces dernières années, la menace du terrorisme djihadiste s'est répandue et a gagné en complexité. Analyser cette menace requiert une coopération internationale entre les services de renseignement et de sécurité, tant au niveau bilatéral que multilatéral. Une telle coopération existe en Europe et avec d'autres pays. L'intensification de cette coopération va de pair avec l'accroissement des échanges de données à caractère personnel. Échanger des données avec des services étrangers fait partie des activités quotidiennes des services de renseignement et de sécurité. Les données peuvent être échangées de différentes manières, que ce soit oralement ou par écrit.

Les organes de contrôle ont naturellement suivi le développement de la coopération internationale entre les services de renseignement et de sécurité. Nos mandats de contrôle respectifs étant strictement nationaux, nous nous sommes intéressés au risque de lacunes dans le contrôle. Idéalement, les systèmes nationaux de contrôle devraient être complémentaires. Ainsi, lorsqu'un organe de contrôle atteint les limites de son mandat national, l'autre est compétent pour exercer un contrôle efficace. Cependant, la législation nationale en matière d'échanges d'informations et le contrôle de ces échanges peuvent ne pas satisfaire à ces exigences. En outre, la coopération internationale entre les services de renseignement pourrait se développer de telle manière que le contrôle national ne pourrait plus être exercé comme il se doit. Il pourrait alors en résulter un "déficit de responsabilité" ou une "lacune dans le contrôle".

À la lumière de ce qui précède, les cinq organes de contrôle belge, danois, néerlandais, norvégien et suisse ont décidé de lancer un projet visant à échanger leurs expériences et leurs méthodes. Chacun de ces organes de contrôle a mené une enquête au niveau national sur les échanges internationaux de données relatifs aux *foreign terrorist fighters* entre les services de renseignement et de sécurité soumis à leur contrôle.

Nous avons mené nos enquêtes respectives plus au moins au même moment, à partir de notre contexte national et dans le cadre de notre mandat national. Nous nous sommes régulièrement réunis pour comparer nos méthodes d'enquête, interpréter les cadres juridiques, discuter des problèmes juridiques et pratiques et collationner nos constatations et nos conclusions. Aucune information classifiée n'a été échangée.

3. PRATIQUES EN VIGUEUR EN MATIÈRE DE CONTRÔLE DES ÉCHANGES DE DONNÉES

Les organes de contrôle participants contrôlent les échanges de données entre les services de renseignement et de sécurité de différentes manières. Nous pouvons :
- Évaluer les relations ou les mécanismes entre les services de renseignement et de sécurité ;
- Évaluer la légitimité et la qualité d'échanges de données spécifiques avec des services étrangers ;
- Revoir le système d'échange de données dans son ensemble, y compris les garde-fous ;
- Être impliqués dans des procédures relatives aux recours et plaintes individuels.

Les mandats des organes de contrôle sont certes différents, mais nous disposons tous d'une large gamme d'instruments nous permettant de contrôler les échanges internationaux de données.

Évaluation du lien de coopération

Les organes de contrôle peuvent évaluer si le lien de coopération entre leur service national et les services partenaires d'autres pays répond à certains critères. La législation organique des services de renseignement et de sécurité peut définir des critères spécifiques de coopération. Généralement, les critères incluent la nécessité de coopérer, le respect des droits de la personne, l'existence d'une législation sur la protection des données et/ou la fiabilité. Il conviendrait de placer la barre très haut pour ce qui relève de la coopération avec des services qui ne respectent pas les critères. Les organes de contrôle belge, néerlandais, norvégien et suisse évaluent les considérations émises à cet égard par leurs services nationaux.

Les liens de coopération entre les services peuvent s'appuyer sur des accords, par exemple des lettres d'intentions ou *memorandums of understanding*. De tels accords ne sont généralement pas contraignants sur le plan juridique mais offrent un cadre pratique pour les échanges de données par les services. L'existence de certains de ces accords est même classifiée. D'autres accords sont rendus publics par les gouvernements ou les services. Ils

peuvent néanmoins tracer les contours des liens de coopération en abordant la question de l'objectif visé par la coopération, les attentes en termes de fonctionnement de la coopération, les restrictions liées à la divulgation à des tiers ou les aspects procéduraux de la coopération. Les organes de contrôle des cinq pays peuvent contrôler si ces accords respectent les lois et les réglementations nationales ou faire rapport à ce sujet.

Évaluation de la légitimité d'échanges de données spécifiques

Les organes de contrôle peuvent évaluer si les échanges individuels de données répondent aux exigences légales imposées par les lois et réglementations nationales.

Les législations nationales de nos pays partagent certaines caractéristiques, plus particulièrement les principes de nécessité et de proportionnalité. Ces principes partagés trouvent leur source dans les cadres légaux internationaux tels que la Convention européenne des droits de l'homme. Le principe de nécessité inclut le critère d'une finalité légale claire pour l'échange de données et une attente raisonnable en termes de résultat à atteindre via l'échange de données. En vertu du principe de proportionnalité, le service se doit de concilier la finalité de l'échange et la gravité de la violation des droits fondamentaux. La plupart des législations nationales renferment encore d'autres exigences, comme le caractère raisonnable, la justesse, l'efficacité et la fiabilité de l'échange d'informations.

La politique interne des services peut définir des règles additionnelles en matière d'échanges de données. Une telle politique peut, par exemple, spécifier quel type d'échange de données est autorisé, dans quelles circonstances, quel niveau d'autorisation est requis et quel usage peut être fait des données obtenues. En l'absence de loi nationale ou d'accords bilatéraux et multilatéraux, ou si ceux-ci passent sous silence un point précis, la politique interne peut offrir des garanties supplémentaires.

Évaluation de la qualité d'échanges de données spécifiques

La qualité peut se rapporter au contenu des données ou du format des données. S'agissant du contenu, la qualité signifie que les données sont correctes, suffisamment claires et précises dans leur libellé, confirmées par des données sous-jacentes, actualisées, et qu'elles comportent une indication de probabilité ou de fiabilité. S'agissant du format, les aspects 'qualité' ont trait à l'inclusion d'un niveau de classification, de la date de l'échange, de la désignation du ou des service(s) partenaire(s) destinataire(s) et des réserves quant à l'utilisation ultérieure des données. Les cinq organes de contrôle peuvent tous contrôler la qualité de l'échange de données à cet égard.

La qualité peut également avoir une signification différente. Elle peut se rapporter à l'efficacité ou à l'efficience : l'échange de données est-il pertinent ? A-t-il eu lieu en temps voulu ? L'objectif est-il atteint ? Ce genre de contrôle de qualité est moins courant dans le chef des organes de contrôle. Les organes de contrôle belge et suisse sont expressément autorisés à vérifier l'efficacité et l'efficience d'un échange de données.

Révision du système d'échange de données dans son ensemble

Les organes de contrôle peuvent adopter une approche plus large lorsqu'ils contrôlent la légitimité d'un échange de données. En contrôlant certains cadres de coopération multilatéraux, l'organe de contrôle néerlandais a spécialement examiné le système d'échange de données dans son ensemble et la protection des droits individuels au sein même du système. Si certains échanges de données spécifiques peuvent être légitimes, le système peut malgré tout ne pas offrir de garanties suffisantes permettant d'assurer la légitimité de l'échange de données à plus long terme. Ce genre de contrôle peut contribuer à éviter un échange illégal de données entre les services de renseignement et de sécurité.

Une approche similaire pourrait être adoptée lors du contrôle de la qualité de l'échange de données. Lorsque l'objectif visé par l'échange de données est de contrer le djihadisme, la qualité générale de l'échange de données pourrait être mesurée en examinant la quantité d'informations partagées qui ont mené aux poursuites et à la condamnation, voire à directement à la prévention une attaque. Mais mesurer l'utilité des données échangées de cette manière peut s'avérer compliqué. Ce genre de contrôle est souvent mis en œuvre après la survenance d'un acte terroriste. L'organe de contrôle évalue alors si les données pertinentes ont été suffisamment et correctement échangées avec des partenaires nationaux et internationaux. L'organe de contrôle belge a été impliqué dans ce genre de contrôle.

Implication dans des recours et plaintes individuels

De manière générale, les organes de contrôle des cinq pays peuvent recevoir des plaintes concernant les activités des services de renseignement et de sécurité. Les organes de contrôle peuvent généralement rendre des avis ou des recommandations juridiquement non contraignants aux services renseignement et de sécurité et/ou aux ministres qui endossent la responsabilité politique. Les services respectent habituellement de tels avis ou recommandations. Une nouvelle loi a été adoptée aux Pays-Bas en 2017, conférant à l'organe de contrôle le pouvoir de prendre des décisions contraignantes concernant les plaintes, y compris la possibilité d'ordonner la cessation de l'exercice d'une compétence ou encore la destruction ou le retrait des données traitées.

Le secret, qui est indispensable aux services de renseignement et de sécurité pour mener leurs activités, limite en général le droit des personnes à accéder à leurs données à caractère personnel. Certains pays accordent aux personnes le droit de demander à l'organe de contrôle national de vérifier les données à caractère personnel que les services ont traitées à leur propos. Au Danemark, quiconque peut demander à l'organe de contrôle danois de vérifier si le service de sécurité traite illégalement des données à caractère personnel le concernant. Dans le cas du service de renseignement militaire, ce contrôle est limité aux personnes résidant au Danemark. Dans les deux cas, l'organe de contrôle danois peut ordonner l'effacement des données relatives au requérant.

En Belgique, l'organe de contrôle a l'obligation d'examiner toutes les plaintes qui ne sont manifestement pas non fondées. Le plaignant recevra les conclusions de l'enquête formulées en termes généraux. Le plaignant aura alors la possibilité d'utiliser ces conclusions devant le tribunal ou une autorité administrative. Dans certains cas spécifiques, l'organe de contrôle doit rendre un avis officiel à une cour pénale à la suite d'une plainte. Par ailleurs, le comité peut prendre des décisions contraignantes concernant deux autres objets de plaintes que sont l'utilisation de méthodes particulières et la protection des données.

En Norvège, les résidents peuvent introduire une plainte auprès de l'organe de recours si un citoyen ou une citoyenne suspecte qu'il/elle a fait l'objet d'une surveillance illégale. Cependant, l'organe de contrôle norvégien n'a pas le pouvoir d'ordonner l'effacement des données. En Suisse, le Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT) gère les demandes individuelles de traitement des données.

4. DÉFIS DU CONTRÔLE DES ÉCHANGES INTERNATIONAUX DE DONNÉES

En cours de projet, nous avons découvert que la coopération renforcée entre les services de renseignement et de sécurité et les échanges de données entre les services, en particulier au niveau multilatéral, peuvent poser des défis légaux et pratiques aux organes de contrôle.

Le contrôle ne traverse pas les frontières nationales

La législation nationale encourage souvent la coopération et les échanges d'informations entre les services de renseignement et de sécurité, tant au niveau bilatéral que multilatéral. Toutefois, elle ne prévoit généralement pas une base légale spécifique à l'intention des organes de contrôle pour coopérer ou échanger des informations sur des personnes. Aucun des cinq organes de recours collaborant dans le cadre de cette publication commune ne dispose d'une base légale explicite pour échanger des données avec un autre organe de contrôle, certainement pas lorsqu'il s'agit d'informations classifiées.

Les services de renseignement et de sécurité traversent les frontières, ce que ne peuvent pas faire les organes de contrôle. Le contrôle se limite aux mandats nationaux. Ceci reflète un aspect de l'échange de données : soit le contrôle se concentrera sur la communication de données et leur collecte préalable, soit il se concentrera sur la réception des données et leur utilisation. Les organes de contrôle nationaux ne seront pas en mesure, chacun de leur côté, d'avoir une vue d'ensemble sur l'échange de données à caractère personnel, sans parler du contrôle de la légalité ou du processus d'échange complet.

Une telle limite au contrôle national ne constitue pas nécessairement une lacune dans le contrôle. Lorsque le contrôle est exhaustif et efficace des deux côtés de la frontières, il n'y a pas de lacune dans les mandats des organes de contrôle. Cependant, quand il s'agit de la coopération entre les services de renseignement et de sécurité – principalement la

coopération multilatérale – la coopération des organes de contrôle n'est jamais aussi solide que son maillon le plus faible.

Le défi de la coopération au regard du secret

Les organes de contrôle sont limités aux règles nationales régissant le secret et ne peuvent ni partager ni discuter de la substance de leurs enquêtes au-delà de ce qui est considéré comme information publique. Dans la pratique, cela signifie que les organes de contrôle ont une vue très limitée sur un éventuel contrôle efficace des échanges de données ou sur d'éventuelles lacunes en matière de contrôle. Les organes de contrôle ne peuvent pas traverser les frontières, pas plus qu'ils ne peuvent partager avec d'autres organes de contrôle ce qui se passe à intérieur de leurs frontières.

Au fil de la progression du projet commun aux cinq organes de contrôle, nous avons eu à maintes reprises l'occasion de nous rendre compte que nous n'étions même pas en mesure de discuter de questions connues de nous tous, par exemple, le contenu des accords conclus entre les services soumis à notre contrôle. En outre, nous avons réalisé que ce qui relève de l'information publique dans un pays pourrait être considéré comme confidentiel dans un autre pays. Notre projet s'en est trouvé compliqué, limitant les possibilités de mener une discussion substantielle sur ce point.

Évaluation de la nécessité et de la proportionnalité

Comme mentionné ci-dessus, les organes de contrôle évaluent en permanence la nécessité d'un échange de données pour atteindre un objectif spécifique, et ce, dans le respect du principe de proportionnalité. Pour ce faire, les organes de contrôle doivent tenir compte du niveau de protection des droits individuels accordé par le service qui reçoit les données. Avec l'augmentation du volume des échanges de données et du nombre de services étrangers avec lesquels les données sont échangées, les organes de contrôle seront confrontés à une tâche de plus en plus ardue. Ces critères de nécessité et de proportionnalité peuvent devenir plus abstraits et perdre de la valeur si les données échangées perdent en spécificité ou si elles sont échangées au sein d'un groupe plus large de services de renseignement et de sécurité.

Différents régimes juridiques nationaux peuvent inclure différentes normes de légalité et de qualité en matière de collecte, de traitement, de conservation et d'échange des données. Le degré de protection des droits individuels offert par le service qui reçoit les données est un élément important dans l'évaluation de la proportionnalité d'un échange de données particulier. Ce degré de protection n'est pas toujours aisé à déterminer, étant donné que les services de renseignement et de sécurité peuvent ne pas être ouverts sur tous les aspects du cadre légal en vigueur et sur les normes qu'ils appliquent.

Dans le contexte d'échanges de données multilatéraux, des normes et des définitions communes pourraient contribuer à définir dans quelles circonstances l'échange de données est considéré comme nécessaire et proportionnel et quel niveau minimal de protection des droits doit être mis en place pour offrir une garantie suffisante de respect des droits individuels. Il y a un intérêt commun pour toutes les parties – les services de

renseignement et de sécurité et les organes de contrôle – à disposer de telles normes communes et d'une interprétation commune des garanties juridiques existantes. La légitimité des échanges multilatéraux dont il est question peut également s'en trouver accrue.

Distinction opérée par certains pays entre les citoyens et les étrangers

Certains cadres légaux nationaux offrent un niveau plus élevé de protection et un accès privilégié à des voies de recours individuels aux nationaux/résidents qu'aux étrangers/non-résidents. La distinction entre ces groupes peut limiter voire interdire l'accès à des recours individuels pour les étrangers ou non-résidents dont les données ont été échangées par les services de renseignement et de sécurité respectifs.

Une distinction similaire peut déterminer le mandat de l'organe de recours. Certains organes de recours ne sont mandatés que pour contrôler les échanges de données relatifs aux nationaux et résidents. La communication de données concernant d'autres personnes peut demeurer hors de leur portée. Si aucun autre organe de contrôle ne peut contrôler efficacement cette partie de l'échange de données, il en résulte une lacune dans le contrôle.

Moyens et méthodes d'échanges de données

Les services de renseignement et de sécurité échangent des données de différentes manières. Certains moyens et certaines méthodes d'échange de données sont autant de nouveaux défis pour les organes de contrôle. Entre autres exemples, citons l'échange informel de données, la manière de contrôler efficacement les données échangées lors de conférences et de réunions ou encore par téléphone. L'accroissement des échanges de données au niveau international peut contraindre les organes de contrôle à trouver des méthodes plus perfectionnées de contrôle. En effet, il ne leur est plus possible de contrôler chaque échange de données. En ce qui concerne la protection des données, les évolutions en matière d'échange de données au niveau multilatéral peuvent invoquer la responsabilité de chaque service participant, mais aussi des organes de contrôle. Pour offrir une garantie suffisante de respect des droits individuels, les services de renseignement et de sécurité pourraient être amenés à discuter des normes à appliquer et œuvrer à la définition d'un seuil minimal de protection commun à tous les services participants.

5. VERS UN CONTRÔLE PLUS PERFORMANT DES ÉCHANGES INTERNATIONAUX DE DONNÉES

Notre projet nous a montré que les efforts déployés par les services de renseignement et de sécurité pour trouver de nouveaux moyens d'échanger des données de manière efficace, en particulier au niveau multilatéral, et la forte augmentation du volume de données échangées, ont posé de nouveaux défis aux organes de contrôle. Sont autant concernés les limites des mandats nationaux des organes de contrôle, leur incapacité à discuter de manière appropriée des échanges internationaux de données avec d'autres

organes de contrôle, que leurs propres efforts visant à innover leurs procédures et leurs méthodes en vue de garantir un contrôle efficace.

La souveraineté et les intérêts nationaux régissent la coopération internationale entre les services de renseignement et de sécurité. Contrairement à d'autres domaines de coopération internationale, il faut s'attendre à ce que le contrôle des services de renseignement et de sécurité continue à être exercé par les organes de contrôle nationaux. Toutefois, les services de renseignement et de sécurité traversent les frontières, ce que ne peuvent pas faire les organes de contrôle.

Le contrôle donc reflète toujours une face de l'échange de données. En outre, les organes de contrôle sont pour la plupart dans l'incapacité de partager leur contrôle sur un échange de données particulier avec d'autres organes de contrôle. Les limites du contrôle national font courir le risque de l'apparition de lacunes dans le contrôle en matière d'échange international de données par les services de renseignement et de sécurité. La question reste de savoir comment répondre à un tel risque.

Les organes de contrôle peuvent se rapprocher en échangeant des connaissances, des expériences et des méthodes d'enquête, mais aussi en comparant leurs constatations, conclusions et recommandations. C'est précisément ce que ce projet commun nous a permis d'expérimenter. Nous avons appris de nos meilleures pratiques respectives, nous avons développé une meilleure compréhension de nos systèmes juridiques respectifs et nous avons instauré un certain climat de confiance. Afin de permettre aux organes de contrôle de suivre les développements de la coopération entre les services de renseignement et de sécurité, nous n'avons d'autre choix que d'intensifier notre coopération.

Une étape utile et nécessaire vers une coopération plus étroite est de limiter le secret lorsqu'il s'agit de partager des informations entre organes de contrôle. Ceux-ci devraient au moins pouvoir discuter des accords de coopération concrets qui ont été conclus tant au niveau bilatéral que multilatéral entre les services de renseignement et de sécurité soumis à leur contrôle. En toute logique, une étape supplémentaire pourrait être de partager des informations avec d'autres organes de contrôle qui ont déjà été partagées par les services de renseignement et de sécurité eux-mêmes. Une fois que les données ont été échangées, le contrôle peut être effectué dans la foulée. Nous ne suggérons pas que toutes les restrictions en matière de secret soient balayées d'un revers de main. Loin s'en faut. La coopération entre les organes de contrôle doit s'organiser dans les limites des normes établies par les législateurs nationaux.

Pouvoir discuter des accords de coopération internationaux et des échanges de données avec d'autres organes de contrôle implique certaines responsabilités. Offrir des garanties suffisantes de respect des droits individuels dans le cadre de la coopération internationale requiert que les services de renseignement et de sécurité discutent des normes qu'ils appliquent et œuvrent à la définition d'un seuil minimal de protection commun à tous les services participants. Cela requiert également que les organes de contrôle fassent respecter ce seuil minimal de protection des données et tentent de trouver un terrain d'entente dans l'interprétation des garanties juridiques existantes.

Compte tenu des évolutions technologiques et du renforcement de la coopération, les échanges de données entre les services de renseignement et de sécurité s'intensifient, avec comme corollaire une augmentation du nombre d'échanges individuels de données. Le volume considérable de données échangées peut devenir un défi en soi. Évaluer la légitimité et la qualité de chaque échange individuel peut devenir une tâche écrasante pour les organes de contrôle. En plus des vérifications ponctuelles, il devient de plus en plus important d'évaluer le système et le cadre des échanges de données, ainsi que l'existence et le fonctionnement des garde-fous en matière de respect des droits fondamentaux.

Dans un souci d'efficacité, les organes de contrôle devront élaborer de nouvelles méthodes. Éventuellement en recourant de plus en plus à l'autonomisation informatique et à des outils développés pour contrôler de grands volumes de données. Pour ce faire, les organes de contrôle ont besoin d'étendre leur expertise en technologies de l'information et leur connaissance des systèmes utilisés par les services. Une autre manière de faciliter un contrôle plus efficace serait de prendre en considération les besoins des organes de contrôle lorsque les services mettent de nouveaux systèmes en place et de renforcer les mécanismes de contrôle interne et externe.

Les organes de contrôle belge, danois, néerlandais, norvégien et Suisse continueront à échanger leurs méthodes et leurs meilleures pratiques. Ils continueront à discuter des défis internationaux auxquels ils sont confrontés et des meilleures approches pour les relever. Nous invitons les organes de contrôle d'autres pays à se joindre à nos efforts pour limiter le risque de lacunes dans le contrôle et pour améliorer le contrôle des échanges internationaux de données entre les services de renseignement et de sécurité.

Signé à Berne le 22 octobre 2018,

M. Serge Lipszyc, Président du Comité de contrôle des services de renseignement et de sécurité (Belgique)

M. Michael Kistrup, Président de l'Organe de contrôle des services de renseignement (Danemark)

M. Harm Brouwer, Président du Comité de contrôle des services de renseignement et de sécurité (Pays-Bas)

Mme Eldbj0rg L0wer, Présidente du Comité EOS – Le Comité de contrôle parlementaire des services de renseignement (Norvège)

M. Thomas Fritschi, Directeur de l'Autorité de surveillance indépendante des activités de renseignement (Suisse)