Quis custodiet ipsos custodes?

Activiteitenverslag 2022
Rapport d'activités 2022

Vast Comité I
Comité Permanent R

Vast Comité van Toezicht op
de inlichtingen- en veiligheidsdiensten

Comité Permanent de Contrôle des
services de renseignement et de sécurité

ACTIVITEITENVERSLAG 2022
RAPPORT D'ACTIVITÉS 2022

Quis custodiet ipsos custodes ?

Quis custodiet ipsos custodes? is een publicatiereeks die een bijdrage wil leveren tot het bevorderen van een geïnformeerde discussie over de werking, de bevoegdheden en de controle op de inlichtingen- en veiligheidsdiensten en op het inlichtingenwerk. In deze reeks worden o.m. wetenschappelijke studies, de activiteitenverslagen van het Vast Comité I en verslagboeken van colloquia opgenomen.

Redactie

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Leuvenseweg 48 bus 4, 1000 Brussel (02 286 29 88).

Reeds verschenen in deze reeks

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Vast Comité I, *Activiteitenverslag 2006,* 2007, 147 p.
3) Vast Comité I, *Activiteitenverslag 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, 2010, 220 p.
5) Vast Comité I, *Activiteitenverslag 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Vast Comité I, *Activiteitenverslag 2009,* 2010, 127 p.
8) Vast Comité I, *Activiteitenverslag 2010,* 2011, 119 p.
9) Vast Comité I, Activiteitenverslag 2011, 2012, 134 p.
10) W. Van Laethem en J. Vanderborght (eds), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, 2013, 565 p.
11) Vast Comité I, *Activiteitenverslag 2012*, 2013, 115 p.
12) Vast Comité I, *Activiteitenverslag 2013*, 2014, 210 p.
13) Vast Comité I, *Activiteitenverslag 2014*, 2015, 135 p.
14) Vast Comité I, *Activiteitenverslag 2015*, 2016, 132 p.
15) Vast Comité I, *Activiteitenverslag 2016*, 2017, 230 p.
16) Vast Comité I, *Activiteitenverslag 2017*, 2018, 152 p.
17) Vast Comité I, *Activiteitenverslag 2018*, 2019, 166 p.
18) J. Vanderborght (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, 2019, 151 p.
19) Vast Comité I, *Activiteitenverslag 2019*, 2020, 148 p.
20) Vast Comité I, *Activiteitenverslag 2020*, 2021, 189 p.
21) Vast Comité I, *Activiteitenverslag 2021*, 2022, 241 p.
21) Vast Comité I, *Activiteitenverslag 2022*, 2023, 168 p.

ACTIVITEITENVERSLAG 2022

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de
inlichtingen- en veiligheidsdiensten

Voorliggend *Activiteitenverslag 2022* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de plenaire vergadering van 23 mei 2023.

(*getekend.*)
Serge Lipszyc, voorzitter
Thibaut Vandamme, raadsheer
Linda Schweiger, raadsvrouw
Bjorn Verschaeve, dienstdoend griffier

Activiteitenverslag 2022
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

INHOUD

LIJST MET AFKORTINGEN

ADIV	Algemene Dienst Inlichting en Veiligheid
AG	Administrateur-generaal (VSSE)
ANG	Algemene Nationale Gegevensbank
AVG	Algemene Verordening Gegevensbescherming
BELPIU	*Belgian Passenger Information Unit*
BIM	Bijzondere inlichtingenmethoden
BIM-Commissie	Bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door inlichtingen- en veiligheidsdiensten
BIM-Wet	Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten
BINII	*Belgian Intelligence Network Information Infrastructure*
BS	Belgisch Staatsblad
BTA	Bevoegde Toezichthoudende Autoriteit
CCB	Centrum voor Cybersecurity Belgium
CCIV	Coördinatiecomité Inlichtingen en Veiligheid
CelEx	Cel Extremisme (FOD Justitie)
CI	*Counterintelligence*
COC	Controleorgaan voor politionele informatie
CRAB	Compte Rendu Analytique – Beknopt Verslag
CRIV	Compte Rendu Intégral – Integraal Verslag
DG EPI	Directoraat-generaal Penitentiaire Inrichtingen
DISCC	*Defense Intelligence and Security Coordination Centre* (ADIV)
DJSOC/Terro	Directie van de bestrijding van de zware en georganiseerde criminaliteit (afdeling terrorisme) van de Federale gerechtelijke politie
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
DVZ	Dienst Vreemdelingenzaken
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
FIRM	Federale Instituut voor de bescherming en de bevordering van de rechten van de mens
FOD	Federale overheidsdienst
FTF	*Foreign terrorist fighters*

GBA	Gegevensbeschermingsautoriteit
GBA-Wet	Wet van 3 december 2017 tot oprichting van de gegevens-beschermingsautoriteit
GBW	Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoons-gegevens (Gegevensbeschermingswet)
GGB	Gemeenschappelijke gegevensbanken
GGB HP	Gemeenschappelijke gegevensbank 'Haatpropagandisten'
GGB TF	Gemeenschappelijke gegevensbank '*Terrorist Fighters*'
HTF	*Homegrown terrorist fighters*
Hand.	Handelingen
HP	Haatpropagandisten
HUMINT	*Human intelligence*
HvJEU	Hof van Justitie van de Europese Unie
ICT	Informatie- en communicatietechnologie
IOWG	*Intelligence Oversight Working Group*
IRT	*Incident/intervention Respons Team* (VSSE)
JDC	*Joint Decision Centre*
JIC	*Joint Intelligence Centre*
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

LCMB	Lokale Comités voor Maritieme Beveiliging
LIVC-R	Lokale integrale veiligheidscel - radicalisme
LTF	*Local task force*
M.B.	Ministerieel besluit
MOD	Minister van Defensie
MoU	*Memorandum of Understanding*
MPLUS	Gewone methoden plus
NA	*Note aux autorités*
NAMB	Nationale Autoriteit voor Maritieme Beveiliging
NAVO	Noord-Atlantische Verdragsorganisatie
NSIP	Nationaal Strategisch Inlichtingenplan
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open sources intelligence*
Parl. St.	Parlementaire Stukken van Kamer en Senaat
PIO	*Prison Information Officer*
PGE	Potentieel gewelddadige extremisten
Plan R	Actieplan Radicalisme
Platform CT	Gemeenschappelijk contraterrorisme-platform
PNR-Wet	Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens
PROTEUS	Gegevensbank OCAD
RFC	*Requests for collect*
RFI	*Request for information*
RVV	Raad voor Vreemdelingenbetwistingen
SIGINT	*Signals intelligence*
SocSw.	Sociaal Strafwetboek
SOP	*Standard Operating Procedures*
Strategie TER	Strategische nota Extremisme en Terrorisme
TA	Toezichthoudende autoriteiten
TF	*Terrorist fighters*
TV	Terrorisme-veroordeelden
Vast Comité I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten
Vr. en Antw.	Schriftelijke vragen en antwoorden (Kamer of Senaat)
VSSE	Veiligheid van de Staat
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veilig-heidsattesten 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
WOB	Wet van 11 april 1994 betreffende de openbaarheid van bestuur
WPA	Wet van 5 augustus 1992 op het politieambt
W.Toezicht	Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse

VOORWOORD

Hoewel dit geen nieuwe vaststelling is, roept een terugblik op het jaar 2022 ons op de kwetsbaarheid van onze wereld ter discussie te stellen.

De inval in Oekraïne op 24 februari 2022 heeft, na de COVID-periode, een wereldwijde crisis versterkt die ons heeft getroffen op een manier die sinds de Tweede Wereldoorlog waarschijnlijk niet meer is voorgekomen. Deze crisis heeft een maatschappelijke onzekerheid uitgelokt die zich niet alleen heeft gemanifesteerd in aanzienlijke sociaal-economische moeilijkheden, maar vooral in een terugkeer van zeer duistere reflexen van angst en afwijzing van anderen.

In de versnelling van geopolitieke, economische en sociale bewegingen die zij met zich meebrengt, lijkt onze communicatiemaatschappij duidelijk te worstelen met voor de mensheid verwoestende verschijnselen, zoals radicalisme, extremisme en samenzwering, die in de sociale media ongekende versterkers van desinformatie vinden die soms niet onder controle te houden zijn.[1]

De bedreigingen en veiligheidsproblemen die zij opleveren voor de democratische ontwikkeling van onze samenleving stellen onze regeringen en hun inlichtingen- en veiligheidsdiensten dan ook radicaal ter discussie. In ieder geval moeten de middelen en de werking van deze essentiële instellingen worden aangepast.

Ter illustratie: de 'Qatargate' heeft het Europese en Belgische landernau opgeschud door ons te herinneren aan de realiteit en de gevaren van mogelijke buitenlandse inmenging in onze instellingen. Deze 'episode' heeft geleid en zal zeker blijven leiden tot een aanpassing van de preventieve maatregelen en reacties op deze dreiging.

De opening van het proces tegen de aanslagen in Brussel en Zaventem herinnert ons aan de toegenomen noodzaak om de burgers en de staat te beschermen tegen radicalisme, extremisme en terrorisme.

Het Vast Comité I kan de recente investeringsplannen in personele middelen, infrastructuur, instrumenten en operationele methoden voor onze twee inlichtingendiensten alleen maar toejuichen. Er is ook een duidelijke bereidheid van de autoriteiten en de verantwoordelijken van de diensten om hun samenwerking en partnerschappen op nuttige wijze te versterken ten behoeve van de nationale veiligheid. De analyse van de uitvoering van de aanbevelingen van de Parlementaire Commissie Terrorisme biedt een overzicht van het reeds verrichte werk en de nog

---

1 C. DUMBRAVA, *Les principaux risques des medias sociaux pour la démocratie. Risques liés à la surveillance, à la personnalisation, à la désinformation, à la moderation et au microciblage,* Service de recherche du Parlement européen, décembre 2021, Bruxelles.
https://www.europarl.europa.eu/thinktank/fr/document/EPRS_IDA(2021)698845

af te leggen weg, bijna zes jaar na de indiening van het rapport over de veiligheidsarchitectuur op 15 juni 2017.[2]

In dit verband beval het Vast Comité I "*een breder maatschappelijk (parlementair) debat aan over het in de Inlichtingenwet van 1998 voorziene takenpakket van de twee inlichtingendiensten en de hieraan gekoppelde prioriteitenstelling. Dit vergt een 'strategisch' onderbouwde discussie over de beschikbaarstelling van voldoende capaciteiten en middelen om elke dienst in staat te stellen alle bedreigingen van de (inter)nationale veiligheid naar behoren op te sporen, te bewaken en te beheersen. De inlichtingen- en veiligheidsdiensten moeten het voorwerp van parlementaire aandacht uitmaken, en dit niet alleen op het moment dat er zich individuele problemen voordoen*".

Deze aanbeveling roept, zoals vele andere, ook het probleem op van een goed begrip van het werk van het Comité door het Parlement. Zij zijn er als vogels in de mijn, niet om CO op te sporen, maar om gevaren, problemen en bedreigingen voor de burger en de staat te detecteren.

Anderzijds ziet het Vast Comité I er, met name in zijn hoedanigheid van gegevensbeschermingsautoriteit, op toe dat de inlichtingen- en veiligheidsdiensten hun rol bij de bescherming van de rechten en vrijheden van het individu ten volle op zich nemen en waarborgen. Dit is de evenwichtige prijs die voor onze democratie moet worden betaald.

Vanuit dit oogpunt blijft het Vast Comité I erop toezien dat de diensten informatie op een daadwerkelijk legale en proportionele manier verzamelen en verwerken. Ter herinnering: in 1998 beperkte de wetgever de bevoegdheid van het Comité tot uitsluitend de twee inlichtingendiensten, maar recente ontwikkelingen in de opdrachten van diverse andere diensten geven aanleiding tot toenemende bezorgdheid over de ontwikkeling van inlichtingenactiviteiten zonder passende wettelijke controle. Zo moet de oprichting van een "Cybercommando" binnen de ADIV in 2022 weliswaar worden toegejuicht, maar het feit dat deze eenheid wordt beschouwd als een nieuw onderdeel van de Defensiedienst doet vragen rijzen over het vermogen om de inlichtingenactiviteiten van deze dienst in de toekomst te controleren.

Dit debat over de ontwikkeling van inlichtingenactiviteiten buiten de grenzen van de diensten die vallen onder de wetten betreffende het Vast Comité I van 18 juli 1991 en de inlichtingen- en veiligheidsdiensten van 30 november 1998 stelt de huidige bevoegdheden en capaciteiten van het Vast Comité I ter discussie.

---

2 VAST COMITÉ I, Toezichtonderzoek naar de opvolging van de in de parlementaire onderzoekscommissie Terroristische Aanslagen geformuleerde aanbevelingen met betrekking tot de inlichtingen- en veiligheidsdiensten, oktober 2022.
https://www.comiteri.be/images/pdf/enquetes/Eindrapport_FR.pdf

Wij hopen dat de instellingen zullen evolueren, dat zij hun capaciteit zullen versterken om het hoofd te bieden aan de uitdagingen van inmenging, spionage, terrorisme, al die bedreigingen die de werking van onze democratische instellingen verzwakken. Het Comité blijft evenveel aandacht besteden aan de fundamentele rechten en vrijheden van het individu als aan de nationale veiligheid.

Ik hoop dat het lezen van dit verslag zal bijdragen tot een beter begrip van ons werk en uw belangstelling voor onze activiteiten zal stimuleren!

Serge Lipszyc,
Voorzitter van het Vast Comité van toezicht
Inlichtingen- en veiligheidsdiensten

19 mei 2023

HOOFDSTUK I.
DE TOEZICHTONDERZOEKEN

PREAMBULE

Diverse instanties of personen kunnen het Comité 'vatten' met een toezichtonderzoek: de Begeleidingscommissie, de voogdijministers, elke (rechts)persoon die klacht of aangifte wenst te doen…

In totaal ontving het Comité in 2022 68 klachten of aangiften.[1] Na een kort vooronderzoek en de verificatie van een aantal objectieve gegevens, wees het Comité 31 klachten of aangiften af omdat ze kennelijk niet gegrond waren[2] (art. 34 Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse (W.Toezicht)) of omdat het Comité onbevoegd was om de opgeworpen vraag te behandelen. In dat laatste geval werden de klagers doorverwezen naar de bevoegde instanties (bijv. het Openbaar Ministerie of het Vast Comité P). Drie van de 37 klachten konden worden afgerond in 2022, elf klachten waren begin 2023 nog in behandeling. In 2022 werden 27 van de 37 klachten gehercategoriseerd als *Data Protection Authority* (DPA)-klacht.[3]

Het Comité kan ook zelf het voortouw nemen op een toezichtonderzoek te openen: vier van de negen in 2022 gefinaliseerde onderzoeken werden ambtshalve opgestart (I.1, I.3, I.5 en I.9). Er werden vijf onderzoeken uitgevoerd op verzoek van de parlementaire Begeleidingscommissie (I.2, I.4., I.6, I.7 en I.8). Het Comité zette tevens zijn werkzaamheden voort in het kader van acht in 2022 of eerder opgestarte onderzoeken. Een korte omschrijving van deze nog lopende en/of opgestarte onderzoeken, volgt in I.10. De naar aanleiding van de toezichtonderzoeken geformuleerde aanbevelingen werden gebundeld in Hoofdstuk XI.

---

1 Eerst wordt de ontvankelijkheid bestudeerd en vervolgens gecategoriseerd ('gewone' klacht, DPA-klacht, BIM-klacht…). 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).

2 Het Comité is bestemmeling van nogal wat klachten en aangiften van mensen met waanbeelden.

3 Zie hierover 'IV.2. De behandeling van individuele verzoeken'.

I.1. DE OPVOLGING VAN WEGENS TERRORISME VEROORDEELDE GEDETINEERDEN

Zowel de Veiligheid van de Staat[4] (VSSE) als de politieke overheden[5] maken zich zorgen over terroristische recidive. Wetenschappelijke studies strekken er echter toe de omvang van dit gevaar te nuanceren en stellen dat het percentage recidive wat betreft terrorisme eerder laag is.[6] Aangezien slechts één geval van recidive al zware gevolgen kan hebben, is het evenwel gerechtvaardigd dat de inlichtingendiensten er de nodige aandacht aan besteden.

In België werden tussen 2015 en 2021 meer dan 470 personen veroordeeld wegens feiten van terrorisme.[7] In januari 2022 telde men in de Belgische gevangenissen, op een totaal van ca. 10.700 gedetineerden[8], 136 gedetineerden in verband met terrorisme of gedetineerden die werden geïdentificeerd als zijnde geradicaliseerd.

Vanuit deze achtergrond opende het Vast Comité I in april 2019 een toezichtonderzoek teneinde de informatiepositie van de inlichtingendiensten te evalueren, alsook de middelen die worden ingezet in het kader van de opvolging van (ex-)terro- en geradicaliseerde gedetineerden.[9] Het onderzoeksverslag werd in juni 2022 besproken in de Begeleidingscommissie.

I.1.1. RECHTSKADER EN STRATEGISCH KADER

Naast de Inlichtingenwet die de algemene bevoegdheid van de inlichtingendiensten vastlegt (artt. 7 en 8 wat betreft de VSSE en artt. 10 en 11 wat betreft de ADIV), wordt de opvolging door de VSSE en de ADIV van (ex-)terro- en geradicaliseerde gedetineerden meer bepaald aangestuurd door verschillende strategische

---

4 VSSE, *Activiteitenverslag 2017-2018*, 2018, p. 17; VSSE, *Rapport annuel 2020*, 2021, p. 27.

5 Parlementair onderzoek terroristische aanslagen, *Parl. St.*, Kamer 2016-7, 54-1752/9, pp. 99-100.

6 T. RENARD, CTC Sentinel, 'Overblown: Exploring the gap between the Fear of Terrorist Recidivism and the Evidence', Vol. 13, nr. 4, april 2020. Het lage percentage recidive bij terroristen wordt bevestigd in een document van het *Radicalisation Awareness Network* (RAN), een overlegplatform dat wordt ondersteund door de Europese Commissie; dit netwerk raamt dit percentage tussen 5 en 8% in Europa, maar moedigt aan tot bijkomend onderzoek naar deze problematiek, aangezien het meent over onvoldoende zowel kwantitatieve als kwalitatieve gegevens te beschikken (RAN, *La récidive chez les délinquants extrémistes violents et terroristes*, Slotdocument, 24 februari 2021).

7 *Parl. St.* Kamer 2021-2, 55-148.

8 Belga, "Combien y-a-t-il de détenus dans les prisons belges ?", *Le Vif*, 27 december 2021.

9 De uitdrukking '(ex-)terro- en geradicaliseerde gedetineerden' verwijst naar de a) personen die worden verdacht of beschuldigd van feiten die als terroristische feiten worden gekwalificeerd, onder aanhoudingsbevel zijn geplaatst of het voorwerp zijn van een regeling van voorlopige hechtenis onder elektronisch toezicht, ofwel voorwaardelijk in vrijheid zijn gesteld; b) personen die zijn veroordeeld wegens terroristische feiten en een strafinstelling verlaten als gevolg van definitieve invrijheidstelling of krachtens eender welke andere regeling; c) en, tot slot, gedetineerden (terro of gemeen recht) die tijdens en na hun opsluiting worden geïdentificeerd als zijnde geradicaliseerd.

documenten. Sommige van deze documenten organiseren de opvolging *vóór* en *na* de opsluiting, terwijl andere betrekking hebben op de werking van de inlichtingendiensten en hun partners *tijdens* de opsluiting. Het resultaat van dit alles is dat er een complex strategisch kader bestaat verspreid over verschillende actoren en bevoegdheidsniveaus.

I.1.1.1. De Strategie TER

In september 2021 volgde de strategische nota Extremisme en Terrorisme (Strategie TER genoemd) het Actieplan Radicalisme (Plan R) op. Hierin worden de uitwisselingen tussen de nationale partners georganiseerd met het oog op het vroegtijdig opsporen van terroristische en extremistische bedreigingen.[10] In dit kader werden meerdere overlegplatformen opgericht.

Voor de opvolging van de (ex-)terro- en/of geradicaliseerde gedetineerden *tijdens* hun opsluiting, vinden de uitwisselingen tussen de partners voornamelijk plaats in het kader van de vergaderingen van de werkgroep Gevangenissen (WG Gevangenissen). Deze werkgroep werd in 2015 opgesplitst in een strategische en een operationele WG Gevangenissen. De strategische WG bestaat sindsdien uit vertegenwoordigers van de VSSE, het OCAD, de Centrale eenheid antiterrorisme van de Centrale directie van de bestrijding van de zware en georganiseerde criminaliteit van de federale Politie (DJSOC/Terro), het directoraat-generaal Penitentiaire Inrichtingen (DG EPI), het Nationaal Crisiscentrum, de FOD Buitenlandse Zaken, de Dienst Vreemdelingenzaken en de administratie van de Justitiehuizen. Deze diensten komen elke trimester samen in het kader van een strategisch overleg en de organisatie van de opvolging van deze gedetineerden.

Naast de strategische WG, maken de vergaderingen van de operationele WG het voor de partners mogelijk om de gedetineerden te identificeren die moeten worden opgevolgd en om informatie uit te wisselen over individuele dossiers. Sinds 2021 neemt de ADIV niet langer deel aan de (strategische noch operationele) vergaderingen van de WG Gevangenissen.

De opvolging *ná* de vrijlating wordt vervolgens georganiseerd binnen de *local taskforces* (LTF, *infra*). Opgericht binnen de gerechtelijke arrondissementen, waken de strategische *local taskforces* (LTF's) "*over de afstemming tussen de lokale operationele LTF's*"[11] terwijl de operationele LTF's als doel hebben het organiseren van de

[10] OCAD, "Nieuwe strategie tegen terrorisme en extremisme vervangt actieplan radicalisme", 8 september 2021, http://ocad.belgium.be.

[11] OCAD, *Strategie TER,*, 2021, p. 10.

opvolging van individuele dossiers en de verwerking en uitwisseling van informatie tussen de partners.[12]

I.1.1.2. Het protocolakkoord VSSE – DG EPI

In het kader van het voormalige Plan R werd er in 2006 een protocolakkoord ondertekend tussen de VSSE en het DG EPI.[13] Dit protocol had als doel de informatie-uitwisseling tussen beide administraties te organiseren en te bevorderen.

In dit kader neemt het DG EPI zelf het initiatief om de informatie te verstrekken die het penitentiair personeel verzamelt met betrekking tot terro-gedetineerden of gedetineerden die in verband kunnen worden gebracht met radicalisme.[14] Van haar kant stuurt de VSSE de nuttige informatie waarover ze beschikt met betrekking tot die gedetineerden door.

Het protocolakkoord voorziet voor de VSSE ook in een rechtstreekse toegang tot de gegevensbank 'SIDIS Suite' van het DG EPI. Deze gegevensbank bevat de informatie betreffende de gedetineerden, zoals de identificatiegegevens, de gerechtelijke gegevens of ook gegevens in verband met bezoekers.

Ten tijde van het onderzoek werd een nieuw protocolakkoord, dat sinds 2016 wordt besproken, ingewacht.[15] Dit nieuwe protocol wil rekening houden met de evolutie van de praktijken en uitwisselingen tussen de VSSE en het DG EPI.

I.1.1.3. Het Actieplan aanpak radicalisering in gevangenissen

In 2015 werd een actieplan aanpak radicalisering in gevangenissen verspreid. Het document is opgebouwd rond tien actiepunten en heeft een dubbel doel: "*vermijden dat gedetineerden radicaliseren tijdens hun verblijf in de gevangenis*" en "*het uitwerken van een gespecialiseerde omkadering van geradicaliseerde personen tijdens hun detentie*".[16]

---

12 Binnen de operationele LTF's, die worden voorgezeten door de directeur-coördinator van het gerechtelijk arrondissement (DirCo), zijn de lokale politiezone(s), de gerechtelijke federale politie (GFP), het OCAD, de inlichtingendiensten, DJSOC/Terro, de Dienst Vreemdelingenzaken, Fedasil alsook het lokale parket vertegenwoordigd. Van hun kant bestaan de strategische LTF's uit de DirCo, de procureur des Konings en de provinciegouverneur.

13 Zie VAST COMITE I, *Activiteitenverslag* 2016, pp. 57-62 ('De VSSE en het samenwerkingsprotocol met de strafinrichtingen'). Zie ook VAST COMITE I, *Activiteitenverslag 2018*, pp. 27-28. ('De evaluatie van het protocol DG EPI/VSSE').

14 Bijvoorbeeld de situatie in de gevangenis, vrijlatingen, het verlaten van de gevangenis, externe contacten (bezoekers, briefwisseling, telefoons) en contacten binnen de gevangenis, gedrag, incidenten (vechtpartijen, bij controles aangetroffen voorwerpen, zelfmoordpoging, enz.), rekeningen in de gevangeniskantine, lectuur, culturele activiteiten of eender welk ander element op vraag van de VSSE.

15 In het activiteitenverslag 2021-2022 van de VSSE, werd door de Administrateur-generaal a.i. de ondertekening van het nieuwe protocol met DG EPI aangekondigd (VSSE, *Intelligence Report 2021-2022*, 2023, *www.vsse.be*, p. 4).

16 FOD Justitie, *Actieplan aanpak radicalisering in gevangenissen*, 11 maart 2015, p. 3.

In het kader van de uitvoering van dit actieplan, werd er binnen het DG EPI een Cel Extremisme (CelEx) opgericht. Een van de opdrachten van de CelEx bestaat erin informatie te verzamelen vanuit de gevangenissen en aanbevelingen te formuleren betreffende het gevangenisregime dat moet worden toegepast voor gedetineerden die worden geïdentificeerd als zijnde geradicaliseerd. In de schoot van de CelEx zijn er coördinatoren die ook als aanspreekpunt fungeren met de penitentiaire inrichtingen en de partnerdiensten.

Bepaalde actiepunten hebben rechtstreeks betrekking op de inlichtingendiensten en in het bijzonder op de Cel *Counter extremism Gevangenis – Prison* (CEGP) van de VSSE. Zo roept het actieplan op tot "*een sterkere informatiepositie door een meer gerichte informatiegaring en analyse*".

In 2018 werden besprekingen aangevat tussen de partners (DG EPI, DJSOC/Terro, OCAD, VSSE) en de minister van Justitie om dit plan te actualiseren. In dit kader ging het inzonderheid om de aanwijzing van een *(Prison) Information Officer* (PIO)[17] onder het leidinggevend personeel van elke gevangenis. De PIO, die een medewerker is van het DG EPI en houder van een veiligheidsmachtiging, zou de opdracht krijgen om in de gevangenis informatie te verzamelen en te verwerken en de operationele activiteiten van de VSSE te vergemakkelijken. Het DG EPI legde echter de nadruk op de terughoudendheid van het penitentiair personeel ten aanzien van deze functie van informatieverzameling, nochtans cruciaal volgens de VSSE.

In december 2021 kondigde de minister van Justitie aan dat er meer dan twintig veiligheidscoördinatoren voor de gevangenissen zouden worden aangeworven als aanspreekpunt voor de VSSE.[18] In het kader van een proefproject van het DG EPI zullen deze veiligheidscoördinatoren de opdrachten vervullen waarin is voorzien voor de PIO. Aangezien het gaat om leden van de directieteams van de gevangenissen, zullen deze echter ook managementtaken op zich nemen. Op dit punt verschilt de functie van die van de PIO zoals bedacht door de VSSE.

I.1.2. EEN CENTRAAL INSTRUMENT VOOR DE OPVOLGING VAN (EX-)TERRO- OF GERADICALISEERDE GEDETINEERDEN: DE GEMEENSCHAPPELIJKE GEGEVENSBANK *TERRORIST FIGHTERS*

Sinds 2016 wordt de informatie-uitwisseling over terrorisme en extremisme tussen de veiligheidsdiensten vereenvoudigd door de gemeenschappelijke gegevensbank

17 In het kader van het Actieplan Radicalisering in de gevangenissen van 2015 was er al sprake van lokale coördinatoren voor de gevangenissen.

18 *Parl. St.* Kamer 2021-2, CRIV 55 PLEN 144, p. 16.

Terrorist Fighters (GGB TF).[19] Voor elke ingeschreven entiteit bevatten de GGB een inlichtingenfiche met niet-geclassificeerde gegevens waarover de diensten beschikken alsook een dreigingsevaluatie door het OCAD.

De GGB TF wordt gebruikt voor de opvolging van (ex-)terro- en geradicaliseerde gedetineerden. Deze specifieke opvolging leidde bovendien tot de toevoeging van twee nieuwe categorieën in 2019, i.e. 'terrorismeveroordeelden' (TV) en 'potentieel gewelddadige extremisten' (PGE).[20] [21] Volgens de VSSE vertegenwoordigen deze nieuwe categorieën een meerwaarde, aangezien ze objectieve criteria aanbrengen en zorgen voor meer duidelijkheid in de opvolging van de betrokken entiteiten.

Het OCAD stelt de nieuwe categorie TV[22] voor als een '*laatste vangnet*'.[23] Die categorie heeft immers betrekking op "*diegenen die voor terrorisme veroordeeld werden, maar die nadien niet meer onmiddellijk in de aandacht van de veiligheidsdiensten, toch de nodige opvolging te geven (met name om zeker te zijn dat ze bij vrijlating zouden opgevolgd worden door de LTF/LIVC [lokale integrale veiligheidscel]*".[24]

---

19 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, *B.S.*, 22 september 2016 ; KB van 23 april 2018 tot wijziging van het KB van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank '*Foreign Terrorist Fighters*' en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank '*Foreign Terrorist Fighters*' naar de gemeenschappelijke gegevensbank '*Terrorist Fighters*', *B.S.*, 30 mei 2018. Parallel daarmee hebben de ministers van Binnenlandse Zaken en Justitie de *Joint Information Box* in 2018 omgevormd tot een gemeenschappelijke gegevensbank Haatpropagandisten (GGB HP).

20 KB van 20 december 2019 tot wijziging van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters en van het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de wet op het politieambt, *B.S.,* 27 januari 2020.

21 Zie VAST COMITÉ I en COC, Advies betreffende een ontwerp van Koninklijk besluit tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank *Terrorist Fighters*, 1 augustus 2019, 001/VCI-COC/2019..

22 In de gegevensbank heeft de categorie van terrorismeveroordeelden betrekking op individuen die, op cumulatieve wijze:
- een aanknopingspunt hebben in België;
- werden veroordeeld of ten aanzien van wie er gerechtelijke beslissingen tot internering zijn uitgesproken of, wanneer het om minderjarigen gaat, die het voorwerp zijn geweest van een beschermingsmaatregel wegens het plegen van terroristische misdrijven, zoals beschreven in Boek II, Titel I ter van het Strafwetboek, in België of wegens feiten die als zodanig worden gekwalificeerd of wegens een gelijkwaardig misdrijf in het buitenland;
- en voor wie het OCAD het dreigingsniveau beoordeelt als gemiddeld (niveau 2), ernstig (niveau 3) of zeer ernstig (niveau 4).

KB van 20 december 2019 tot wijziging van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters en van het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de wet op het politieambt, *B.S.,* 27 januari 2020.

23 OCAD, "Extrémisme de droite et Covid-19", *Insight*, nr. 10, p. 44.

24 Nota VSSE.

De categorie PGE[25] werd voor het OCAD toegevoegd om de gedetineerden geïdentificeerd als geradicaliseerd maar die niet aan de noodzakelijke voorwaarden voldeden om als FTF, HTF of haatpropagandist te worden ingeschreven, toch door de veiligheidsdiensten nauwlettend in de gaten dienen te worden gehouden – bijvoorbeeld op basis van hun gedrag tijdens hun opsluiting.

Onderstaande tabel bevat een overzicht in cijfers van de evolutie van de in de categorieën PGE en TV opgenomen entiteiten.[26]

	Mei 2019	**Mei 2020**	**Oktober 2021**	**Januari 2022**
TV	N.v.t.	16 (2,4%)	29 (4,1%)	30 (4,2%)
PGE	N.v.t.	13 (2%)	77 (11%)	106 (14,8%)
Totaal GGB TF & HP	696	672	712	713

Tussen mei 2020 en januari 2022 is het aantal in de GGB opgenomen TV's bijna verdubbeld. Van de 30 entiteiten die in januari 2022 werden ingeschreven als TV, waren er zeven nog gedetineerd.

In januari 2022 waren 23 van de 106 PGE's opgesloten in België en waren 33 ex-gedetineerden opgenomen in deze categorie. Drie jaar na de creatie ervan is de categorie PGE goed voor bijna 15% van alle entiteiten in de GGB, zonder dat dit echter als bijzonder wordt beschouwd door de VSSE.[27]

---

25 De categorie 'potentieel gewelddadige extremisten' bevat individuen die op cumulatieve wijze aan onderstaande voorwaarden voldoen:
- ze hebben extremistische opvattingen die het gebruik van geweld of dwang als actiemethoden in België kunnen legitimeren;
- er zijn betrouwbare aanwijzingen dat ze de intentie hebben om geweld te gebruiken, en dit in verband met hun extremistische opvattingen;
- ze voldoen aan één van de volgende voorwaarden die beschouwd worden als risicofactoren voor het gebruik van geweld:
  - ze hebben systematisch sociale contacten binnen extremistische milieus;
  - ze hebben een psychische problematiek, vastgesteld door een gekwalificeerde deskundige;
  - ze pleegden daden of hebben antecedenten die beschouwd kunnen worden als ofwel a) een misdaad of wanbedrijf die de fysieke of psychische integriteit van derden aantast of bedreigt; b) onderrichtingen of een opleiding voor de vervaardiging of het gebruik van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, dan wel voor andere specifieke methoden en technieken nuttig voor het plegen van terroristische misdrijven, c) bewuste handelingen die als materiële steun voor een terroristische/extremistische organisatie of netwerk gelden; d) feiten die door hun aard wijzen op een verontrustend veiligheidsbewustzijn in hoofde van betrokkene.

26 Terwijl entiteiten in meerdere categorieën kunnen worden opgenomen, is dat niet het geval voor TV die geen dubbel statuut kunnen hebben.

27 In januari 2022 ging het echter om de op twee na grootste categorie wat betreft het aantal ingeschreven entiteiten, enkel voorafgegaan door de FTF van categorie 1 (in Syrië/Irak) en de FTF van categorie 3 (*returnees*).

I.1.3. DE OPERATIONELE OPVOLGING DOOR DE INLICHTINGENDIENSTEN TIJDENS DE OPSLUITING

Het werk van de inlichtingendiensten ten aanzien van (ex-)terro- en geradicaliseerde gedetineerden vindt plaats op twee ogenblikken: tijdens de opsluiting en na de vrijlating. Tijdens de opsluiting heeft de opvolging een dubbel doel: enerzijds de radicalisering van (mede)gedetineerden vermijden, en anderzijds de opvolging na hun vrijlating voor te bereiden, om elke (poging tot) recidive van terroristische misdrijven te verhinderen.

I.1.3.1. De ADIV: een theoretische bevoegdheid

Wat betreft de opvolging van terro- en geradicaliseerde gedetineerden, beperkt de bevoegdheid van de ADIV zich tot voormalige en actieve militairen, reservisten en kandidaat-militairen evenals civiele leden van Defensie. In de praktijk volgt de ADIV oud-leden van Defensie, veroordeeld voor terrorisme, niet actief op. Omdat een strafrechtelijke veroordeling voor een terroristisch misdrijf onverenigbaar is met een tewerkstelling bij Defensie, volgt de ADIV inderdaad dergelijke personen enkel op wanneer ze een band vertonen met een *actief* personeelslid van Defensie. In januari 2022 stelde de ADIV dat ze geen enkel onderzoek of operatie voerde naar TV's ingeschreven in de GGB.

I.1.3.2. De VSSE: opvolging van geval tot geval

Binnen de VSSE is de Cel *Counter extremism Gevangenis – Prison* (CEGP) belast met het verzamelen en verwerken van de informatie betreffende de gedetineerden. Op basis van deze informatie stelt de CEGP analysenota's op met betrekking tot het fenomeen van radicalisme en terrorisme in de gevangenissen alsook, voor elke in de GGB opgenomen gedetineerde, een nota met het oog op zijn vrijlating.

Verzamelen van informatie in de gevangenissen door de VSSE

Gelet op de beschikbare middelen, streeft de VSSE er in de gevangenissen hoofdzakelijk naar om een beter beeld te krijgen van het fenomeen van radicalisering, en dit in nauwe samenwerking met de gefedereerde entiteiten. De VSSE gaf echter toe dat de relaties met sommige actoren die bevoegd zijn in het domein van 'deradicalisering' moeilijk verlopen. De VSSE merkt een gebrek aan vertrouwen op vanwege deze actoren en verklaart dat ze van hen niet de minste *feedback* krijgt over hun contacten met gedetineerden. Anderzijds is er volgens de VSSE wel sprake van een goede samenwerking met de Justitiehuizen.

Het verzamelen van informatie tijdens de opsluiting door de VSSE is er dus in de eerste plaats op gericht een beeld te krijgen van de situatie in de gevangenis. Daartoe

maakt de dienst gebruik van verschillende gegevensverzamelingsmethoden zoals voorzien in de W.I&V (artt. 14 tot 19).[28]

Bij de obstakels die ze identificeert voor een doeltreffende opvolging van terro- en geradicaliseerde gedetineerden, legt de VSSE de nadruk op de zware belasting die het verzamelen en analyseren van informatie door de CEGP vertegenwoordigen. Bovendien wijst ze op de nood aan stelselmatige samenwerking met de penitentiaire inrichtingen.

De VSSE spreekt echter haar waardering uit voor de zeer goede samenwerking met de CelEx, DJSOC/Terro en het OCAD. Inzonderheid binnen de WG Gevangenissen lijkt de informatie op voldoende wijze te circuleren.

Informatie verzamelen via de samenwerking met het directoraat-generaal Penitentiaire Inrichtingen

Het DG EPI is een essentiële partner van de VSSE. Zijn software SIDIS Suite, die toegankelijk is voor de CEGP, centraliseert de gegevens van de gedetineerden (persoonsgegevens, vingerafdrukken, gevangenisparcours en -regime, bezoekers, verloven…). Voor gedetineerden die voorkomen in de GGB wordt de gegevensinvoer betreffende elke externe beweging (verlof, voorwaardelijke vrijlating, vrijlating op het einde van de straf enz.) automatisch doorgegeven via een *push*-bericht naar de verschillende partners van het DG EPI, onder wie ook de VSSE.

Binnen het DG EPI wisselt de CelEx dagelijks informatie uit in verband met radicalisering en extremisme met de lokale en de centrale diensten van de penitentiaire administratie alsook met al zijn externe partners.[29] Meer bepaald met de CEGP bestaat het doel van de informatie-uitwisseling erin de door de CelEx opgestelde evaluatiefiches van gedetineerden te delen; deze fiches bevatten bijvoorbeeld informatie over hun dagelijks gedrag, eventuele incidenten, interne contacten, bezoeken, het gevangenisverleden en financiële bewegingen. De fiches bevatten ook de neerslag van waarnemingen door het gevangenispersoneel (wat de gedetineerden lezen, gespreksonderwerpen, houding, ideologie…).

In het kader van zijn opdrachten heeft de CelEx zijn eigen gegevensbank samengesteld met gegevens van gedetineerden die banden hebben met terrorisme en radicalisering. Deze was gedurende lange tijd richtinggevend voor het werk van de partners binnen de WG Gevangenissen en bepaalde welke dossiers bij voorrang dienden te worden gevolgd. In 2018, na de aanval door Benjamin Herman in Luik

---

28 Art. 14 tot 19 W.I&V.

29 Om de twee maanden stelt de CelEx dus observatieverslagen op met betrekking tot de gedetineerden die het voorwerp zijn van opvolging door deze dienst. Een synthese van deze tweemaandelijkse verslagen wordt ter informatie verzonden naar de partners (OCAD, DJSOC/Terro en VSSE) en ingevoerd in de GGB. Bovendien krijgen de partners kennis van elke nieuwe opsluiting van personen die worden verdacht van of werden veroordeeld wegens feiten in verband met terrorisme alsook in geval van vermoedens van radicalisering van een gedetineerde. Op verzoek van de gevangenisdirecties kan de CelEx ook niet-bindende adviezen formuleren over de opsluitingsvoorwaarden van de gedetineerden en over de voorwaarden voor uitvoering van de straf.

en gelet op het bestaan van een grote hoeveelheid lijsten en gegevensbanken eigen aan elke dienst, heeft de minister van Justitie echter gevraagd om de CelEx-lijst op te nemen in de gemeenschappelijke gegevensbanken, zelfs al had dit tot gevolg dat er gedetineerden werden geschrapt die niet beantwoordden aan de definities van de categorieën in de GGB HP en TF. In het verleden gaf het grote aantal lijsten met telkens verschillende doeleinden, definities en dus ook cijfers immers aanleiding tot verwarring.[30] Sinds 2020 baseert de VSSE zich op de cijfers van de GGB en stelt ze dat het voortaan voor alle partners duidelijk is dat deze GGB het referentie-instrument is. Het Comité stelt echter vast dat elke dienst zijn eigen gegevensbank heeft behouden, ook al wordt die enkel intern gebruikt.

De individuele synthesefiches

Zes maanden voorafgaand aan de vrijlating, stelt de VSSE een individuele synthesefiche op voor elke gedetineerde die voorkomt in de GGB. Dergelijke fiches hebben als doel om, voorafgaand aan de effectieve vrijlating, de relevante elementen samen te brengen waarover de VSSE beschikt (bijv. de handelingen van de gedetineerde in de gevangenis, de beweging en de organisatie waarvan de gedetineerde deel uitmaakte of nog steeds deel uitmaakt, het netwerk van relaties in België en in het buitenland alsook de potentiële technische en organisatorische vaardigheden van de betrokkene).

Op basis van deze geclassificeerde nota stelt de CEGP een niet-geclassificeerde synthesefiche op die bestemd is voor de gemeenschappelijke gegevensbank.

De tool ThETIS als analyse-instrument

In het kader van de opvolging van terro- en geradicaliseerde gedetineerden, maakt de VSSE gebruik van de *tool* ThETIS (Target Evaluation Tool Indicator Based)[31] om het niveau van radicalisering van een individu en het risico *op* gebruik van geweld te evalueren. Gezien dit wordt gebruikt voor alle gedetineerden die aan het einde van hun straf komen, maakt ThETIS het voor de VSSE aldus mogelijk om de prioritaire doelen te definiëren.

30 Zo volgde de CelEx op 31 december 2018 212 gedetineerden (onder wie 112 terro-gedetineerden). Van haar kant raamde de VSSE het aantal terroristische of geradicaliseerde gedetineerden – op basis van een extrapolatie – op ongeveer 450, maar daarbij wees ze op het risico dat velen onder hen wellicht onterecht werden gevolgd.

31 Door de VSSE ontwikkeld op basis van *Violent Extremist Risk Assessment 2 Revised* (VERA-2R) van het *Nederlands Instituut voor Forensische Psychiatrie en Psychologie* (NIFP).

De verspreiding van informatie en inlichtingen

De informatie die de VSSE met eigen middelen en in het kader van de samenwerking met het DG EPI verzamelt, wordt vervolgens op verschillende manieren gedeeld met de externe partners.

Sinds 2015 stelt de CEGP een algemene, jaarlijkse nota op over de gedetineerden die voorkomen in de GGB[32] en die tijdens het komende jaar zullen of zouden kunnen vrijkomen. Deze nota wordt meermaals per jaar bijgewerkt en toegestuurd aan het DG EPI, de ADIV, het OCAD, de DVZ, de Federale Politie, het Federaal Parket en de respectieve kabinetten van de Eerste Minister, de minister van Justitie en de minister van Binnenlandse Zaken. De inhoud van de nota's wordt ook besproken in de WG Gevangenissen en in de LTF's. Deze nota wordt, op hun verzoek, ook gestuurd naar bepaalde buitenlandse partners.

Naast de algemene jaarlijkse nota's, stelt de VSSE ook een nota 'einde straf' op voor elke terro- of geradicaliseerde gedetineerde.[33] Deze 'nota aan de autoriteiten' (NA) vat het gevangenisparcours samen van de gedetineerden die aan het eind van hun straf komen, hun contacten en de observaties tijdens hun opsluiting. Ze bevat ook elementen over de waarschijnlijke evolutie van de gedetineerde zodra hij de gevangenis zal hebben verlaten.[34] Die NA's worden toegestuurd aan de partners van de VSSE (DG EPI, DJSOC/Terro, OCAD, Federaal Parket, ADIV) één maand vóór de vrijlating van de gedetineerden die in de GGB zijn opgenomen en worden vervolgens besproken binnen de LTF's of in het kader van de LIVC-R in functie van het profiel van de entiteiten.

Op basis van de lezing van verschillende nota's einde straf die de VSSE heeft toegestuurd, stelde het Comité vast dat het om een relevante oefening gaat. De nota's bieden immers een volledige kijk op het gevangenisparcours van de gedetineerde. Deze nota's voeden vervolgens de discussies en uitwisselingen in de schoot van de operationele WG Gevangenissen.

I.1.4. OPERATIONELE OPVOLGING DOOR DE INLICHTINGENDIENSTEN NA DE VRIJLATING OP HET EINDE VAN DE STRAF

Nadat een gedetineerde is vrijgekomen, bespreken de partners de nood aan opvolging door de inlichtingendiensten en/of de politiediensten met elkaar. Er is dus

---

32 Tot in 2018 hadden de algemene nota's betrekking op alle gedetineerden van de CelEx-lijst.

33 Tenzij de opmaak van een nota niet gerechtvaardigd blijkt op basis van nieuwe informatie die werd verzameld. In dit geval wordt de zaak besproken binnen de operationele WG.

34 Sinds 2018 stelt de VSSE dus de nota's op voor gedetineerden die vrijkomen nadat ze hun straf hebben uitgezeten, terwijl het OCAD de nota's opstelt voor gedetineerden die vroegtijdig, al dan niet onder voorwaarden, worden vrijgelaten. Deze taakverdeling, die in de eerste plaats pragmatisch is, is echter willekeurig.

geen automatische opvolging van de ex-terro-gedetineerden en/of geradicaliseerde gedetineerden door de inlichtingendiensten. Bovendien focussen deze diensten voornamelijk op gedetineerden die de gevangenis verlaten nadat ze hun straf volledig hebben uitgezeten. De (weinige) personen die onder voorwaarden worden vrijgelaten[35], worden immers opgevolgd door de politiediensten en de justitiehuizen.[36]

I.1.4.1. Het overleg met de partners binnen de local taskforces

In het kader van de Strategie TER zijn de *local taskforces,* door de dossiers te behandelen die afkomstig zijn van de LIVC-R of een van de partners, belast met de 'veiligheidsopvolging' teneinde de openbare veiligheid te garanderen.

Ook de bijzondere gevallen van ex-terro-gedetineerden of geradicaliseerde gedetineerden worden besproken in de LTF's. Tijdens de operationele vergaderingen stellen de diensten samen vast welke acties moeten worden ondernomen in het kader van de opvolging van de betrokken entiteiten op basis van de informatie die wordt ingevoerd in de GGB en de nota's 'einde straf' die de VSSE opstelt.[37]

Ondanks de verplichting om ten minste eenmaal per maand te vergaderen, komen de twintig provinciale LTF's gemiddeld tienmaal per jaar samen, wat neerkomt op een cijfer tussen zes en twaalf vergaderingen per jaar naargelang de betrokken LTF's.

I.1.4.2. De ADIV: een zeer beperkt actieterrein

De ADIV is enkel geïnteresseerd in gewezen gedetineerden die voorkomen in een terro-dossier wanneer het gaat over een *actief* lid van Defensie (hierbij inbegrepen de reservisten). De ADIV verantwoordt dit beperkt toepassingsveld door enerzijds te wijzen op zijn ondersteunende rol in deze materie en anderzijds op de beperkte middelen dewelke de dienst bijvoorbeeld verhinderen om een autonome vertegenwoordiger te voorzien die deelneemt aan de WG Gevangenissen.

---

35 Zie meer bepaald omzendbrief COL 10/2018 van het College van procureurs-generaal bij de hoven van beroep van 28 juni 2018 betreffende de voorwaarden die opgelegd kunnen worden aan personen die vervolgd of veroordeeld worden voor feiten van terrorisme of die gelinkt worden aan gewelddadig extremisme.

36 Meer bepaald op basis van artikel 20 van de Wet van 5 augustus 1992 op het politieambt (*B.S.*, 1 januari 1993) en de omzendbrief COL 11/2013 van de minister van Justitie, de minister van Binnenlandse Zaken en het college van procureurs-generaal bij de hoven van beroep van 7 juni 2013.

37 De partners kunnen bijvoorbeeld kiezen voor een "*zichtbare en aanklampende opvolging*" door de lokale politiekorpsen via gesprekken met de familie / de school / de werkgever of via het organiseren van maandelijkse huisbezoeken. Het dossier kan ook worden doorgestuurd naar de Dienst Vreemdelingenzaken met het oog op de verwijdering van het grondgebied of naar de bevoegde LIVC-R (zie Bijlage 2). In 2021 vestigde de VSSE echter de aandacht op de nagenoeg onbestaande feedback van de LIVC-R.

Deze theoretische opvolging maakt het voorwerp uit van geen enkele interne richtlijn. Evenmin zijn structurele middelen toebedeeld aan deze problematiek. Om deze reden verklaarde de ADIV in januari 2022 geen enkel dergelijk dossier op te volgen.

In het verleden betreurde de ADIV dat het niet op systematische wijze werd gewaarschuwd door de FOD Justitie, noch door de partners van de FOD Justitie, over de vrijlating van terro-gedetineerden die een link vertoonden met Defensie, iets wat ADIV slechts vernam ter gelegenheid van de operationele vergaderingen van de LTF's. De toegang tot de gegevensbank SIDIS Suite zou het mogelijk maken om "*dergelijk gebrek aan informatie aan te pakken*". Deze toegang was evenwel ten tijde van het onderzoek niet geregeld; er werd dienaangaande gewacht op een koninklijk besluit.[38]

I.1.4.3. De VSSE: opvolging volgens de evaluatie van de dreiging en de capaciteiten

Na de vrijlating op het einde van de straf blijft de VSSE sommige ex-terro- en/of geradicaliseerde gedetineerden opvolgen op basis van de evaluatie die intern wordt gemaakt en naargelang de beschikbare capaciteiten van de dienst.

De rol van de afdelingen Counter Extremism en Counter Terrorism en van de front offices van de VSSE

Zodra de gedetineerden vrijkomen, zijn het de afdelingen Counter Extremism (CE) en Counter Terrorism (CT) alsook de *front offices* van de VSSE[39] die het werk nodig voor het opvolgen van ex-gedetineerden onder elkaar verdelen.

De aanpak inzake de verzameling van informatie na de vrijlating maakt het voorwerp uit van een intern overleg en wordt gedefinieerd naargelang van de prioriteiten en beschikbaarheden.

Buitenlandse gedetineerden: samenwerking met de Dienst Vreemdelingenzaken

Voor buitenlandse gedetineerden die worden vrijgelaten en vervolgens naar een gesloten centrum worden overgebracht met het oog op hun verwijdering, werkt de VSSE nauw samen met de DVZ en de Cel Radicalisme.

---

38 De wet van 5 mei 2019 houdende diverse bepalingen inzake informatisering van Justitie, modernisering van het statuut van rechters in ondernemingszaken en inzake de notariële aktebank (*B.S.*, 19 juni 2019) kent een leesrecht met betrekking tot de SIDIS Suite toe aan verschillende diensten waaronder de VSSE, de ADIV en het OCAD. De draagwijdte en de nadere regels voor toepassing van dit leesrecht moeten echter worden vastgesteld in een koninklijk besluit.

39 Of gedelokaliseerde diensten van de centrale afdelingen.

De individuele fiches die de VSSE opmaakt met betrekking tot gedetineerden die veroordeeld zijn wegens feiten van terrorisme of geradicaliseerde gedetineerden die niet het recht hebben om op het Belgisch grondgebied te verblijven, worden naar de DVZ verzonden. Vervolgens kan de DVZ bijkomende informatie aan de VSSE verstrekken waarmee deze laatste haar nota 'einde straf' kan aanvullen. Bovendien maakt deze informatie de effectieve opvolging mogelijk van gedetineerden zonder verblijfsrecht na hun vrijlating alsook hun plaatsing in een gesloten centrum met het oog op hun verwijdering van het grondgebied.

Internationale samenwerking

Informatie-uitwisseling vindt ook plaats met de buitenlandse partners op basis van een evaluatie van de dreiging die de betrokkene vertegenwoordigt, voor zover hij/zij een rechtstreekse band heeft met het partnerland. Deze nood aan informatie-uitwisseling met de partners wordt van geval tot geval beoordeeld.

Meer in het bijzonder zendt de VSSE, op basis van de W.I&V en van richtlijnen van het College van procureurs-generaal, een kopie van de jaarlijkse algemene nota aan een buitenlandse partner, en dit op diens verzoek. Deze informatie-uitwisseling voldoet aan de bepalingen van het rechtskader zoals vastgesteld in de W.I&V (inzonderheid artikel 19). Het Comité stelde zich echter vragen over het specifieke karakter van deze informatie-uitwisseling met een specifieke partner en, vooral, over het gebruik van die informatie door de betrokken partner. Bovendien maakt het Comité zich zorgen over het delen van informatie betreffende gedetineerden die hun straf hebben uitgezeten en mogelijk niet (langer) het voorwerp zijn van opvolging door de Belgische inlichtingen- en veiligheidsdiensten. Een dergelijke benadering blijkt bovendien in tegenspraak te zijn met de benadering van geval tot geval die wordt geacht richting te geven aan de informatie-uitwisseling met buitenlandse partners.

I.1.5. BESLUITEN

Gelet op de maatschappelijke en politieke onrust die ermee gepaard gaat, wordt het gevaar van terroristische recidive ernstig genomen door de inlichtingendiensten. Terwijl de ADIV zijn acties beperkt tot een in de eerste plaats theoretische bevoegdheid, staat de VSSE in voor de opvolging van terro- en/of geradicaliseerde gedetineerden gedurende de hele uitvoering van de straf alsook na de vrijlating van de betrokkenen.

In het kader van de Strategie TER werkt de VSSE nauw samen met haar partners om deze opvolging te verzekeren. In dit stadium van de evaluatie kan het Vast Comité I niet anders dan vaststellen dat het systeem van opvolging naar behoren functioneert.

De VSSE, het OCAD en DJSOC/Terro waren voorstander van het aanwijzen van *prison information officers* binnen elke strafinrichting om er het fenomeen van terrorisme en extremisme op te volgen. De aanwerving van veiligheidscoördinatoren die de minister van Justitie in december 2021 heeft aangekondigd, leek een veelbelovend alternatief te zijn waarvan de concrete uitvoering moet worden opgevolgd.

In de loop van zijn onderzoek, kon het Comité de nauwe samenwerking tussen de VSSE en het DG EPI vaststellen dewelke het mogelijk maakt om de informatieverzameling op bevredigende wijze te organiseren. De overlegplatformen, meer bepaald de WG Gevangenissen en de LTF's, alsook de gemeenschappelijke gegevensbank TF, lijken bovendien een goede doorstroming van de informatie te garanderen. De grootste moeilijkheid in het kader van de opvolging van (ex-) terro- of geradicaliseerde gedetineerden lijkt veeleer te maken te hebben met het structurele gebrek aan middelen als gevolg waarvan de VSSE (en haar partners) zich gedwongen ziet (zien) om prioriteiten te bepalen wat betreft de op te volgen dossiers. De coördinatie tussen de diensten die wordt georganiseerd in het kader van de Strategie TER en haar verschillende overlegplatformen, laat echter toe om dit gebrek aan middelen te verhelpen.

I.2. OFFENSIEVE CAPACITEITEN VOOR DE INLICHTINGENDIENSTEN?

I.2.1. OORSPRONG EN AFBAKENING VAN DE ENQUÊTE

Midden 2020 vroeg de parlementaire Begeleidingscommissie aan het Vast Comité I om zich te buigen over de eventuele noodzakelijkheid om de Belgische inlichtingendiensten, in navolging van sommige buurlanden, met buitenlandse inlichtingencapaciteiten te voorzien, bijvoorbeeld met zogenaamde 'externe diensten'.[40]

Het Comité besliste om de rapportage van huidige enquête te beperken tot de VSSE. Wat betreft de ADIV, is de militaire inlichtingendienst immers reeds actief in het buitenland en zowel zijn wettelijke opdracht als de wijze waarop sommige van zijn bevoegdheden zijn omschreven, laten geen twijfel bestaan over zijn 'buitenland-capaciteit'. De ADIV is een dienst die, van nature uit en rekening houdend met de opdrachten die hem zijn toebedeeld, inlichtingen verzamelt in en over het

[40] Het onderzoeksverslag werd in oktober 2022 overgemaakt aan de Begeleidingscommissie.

buitenland. Het gaat dus over een dienst die per definitie actief is in het buitenland.[41]

Verschillende bewoordingen worden gebruikt om activiteiten van inlichtingendiensten buiten het nationaal territorium aan te duiden. Soms gebruikt men bijvoorbeeld de termen '*services extérieurs*', 'buitenlandse dienst', 'offensieve diensten'[42], maar ook 'inlichtingendiensten' (waarbij de interessesfeer zich veeleer toespitst op buitenlandse bedreiging terwijl binnenlandse bedreigingen veeleer toebehoren tot de interessesfeer van de zogenaamde 'veiligheidsdiensten', enz.). Het Vast Comité I opteerde voor het gebruik van de terminologie 'buitenlandse inlichtingencapaciteit' die verwijst naar:

> *Operationele activiteiten, clandestien of niet clandestien, ontplooid in het buitenland door de inlichtingendiensten (daarbij eveneens inbegrepen de collecteactiviteiten die worden uitgevoerd <u>vanaf</u> het Belgisch grondgebied maar die ook gevolgen hebben in het buitenland) met het oog op het verzamelen van informatie van zowel binnenlandse als buitenlandse bedreigingen.*

Ingevolge hun wettelijke opdrachten beperken de Belgische inlichtingendiensten zich niet tot het opvolgen van fenomenen binnen en buiten de nationale grenzen. Informatie over het buitenland behoort eveneens tot hun takenpakket. Aldus kan het nodig zijn om informatie te verzamelen over een nationale bedreiging in het buitenland.

De inlichtingen kunnen openlijk in het buitenland worden verzameld (zoals bijvoorbeeld via het raadplegen van open bronnen) of op een clandestiene manier (wanneer, bijvoorbeeld, de ontplooide activiteiten niet ter kennis worden gebracht van de buitenlandse autoriteiten, en dus illegaal kunnen zijn in het land waarin deze activiteiten worden ontplooid).

De collecte kan ten slotte geheel of ten dele gebeuren vanaf het Belgisch grondgebied (bijvoorbeeld vanuit België informatie halen uit buitenlandse communicaties).

Er moet - tot slot - op worden gewezen dat de buitenlandse inlichtingencapaciteit, in het kader van het toezichtonderzoek, zich beperkt tot het verzamelen van

---

41 Zoals onder meer blijkt uit een aantal eerdere toezichtonderzoeken van het Comité, maakt de ADIV ook gebruik van die buitenlandse capaciteit. Zie bijvoorbeeld VAST COMITÉ I, Activiteitenverslag 2014 ('De rol van de ADIV bij het opvolgen van het conflict in Afghanistan'), pp. 11-12; Activiteitenverslag, 2018, pp.18-21 ('De activiteiten van de ADIV in een buitenlandse operatie zone'); Activiteitenverslag 2020, p.65 ((1.10. 'Incidenten in een buitenlandse operatiezone'). In dezelfde zin: de bevoegdheden van de ADIV en de intercepties in het buitenland, het nemen van beelden en de intrusies in informaticasystemen.

42 Het gebruik van de woorden 'offensieve diensten' kon evenmin worden weerhouden vermits die vaak worden geassocieerd met clandestiene operaties in het buitenland. Dergelijke acties gevoerd in het buitenland worden vaak gekoppeld aan propaganda, het leveren van wapens, het beschadigen van infrastructuur en zelfs het fysiek uitschakelen van bepaalde personen. Ook kan ze betrekking hebben op het actief ondersteunen of daadwerkelijk uitvoeren van staatsgrepen. De VSSE drong wat dit betreft sterk aan stellende dat het gebruik van de woorden 'offensieve diensten een onnodige verwarring zou kunnen veroorzaken bij haar buitenlandse partners.

informatie. Directe tussenkomst in het buitenland - bijvoorbeeld via verstoringsmaatregelen - werd hier niet onderzocht.

I.2.2. DE INLICHTINGENCAPACITEITEN VAN DE VSSE IN HET BUITENLAND: HET WETTELIJK KADER

Overeenkomstig de artikelen 7 en 8 van de Wet van 30 november 1998 (W.I&V) laat de inlichtingenbevoegdheid van de VSSE zich bepalen door te beschermen belangen in combinatie met te beheersen bedreigingen.[43] Hierdoor is de VSSE belast met het opsporen en onderzoeken van 'inlichtingen die betrekking hebben op elke activiteit' (art. 7, 1°) die één of meerdere van de wettelijke opgesomde belangen bedreigt of zou kunnen bedreigen.

Binnen dit kader moet de VSSE haar aandacht niet beperken tot dreigingen die zich voordoen binnen de landsgrenzen. Ook de dreigingen die hun oorsprong of beweegreden(en) buiten de landsgrenzen hebben, behoren tot de interessesfeer van de VSSE. Deze extra aandacht is hierbij zowel van belang voor de bescherming van de uitwendig alsook van de inwendig georiënteerde staatsbelangen.

Om die binnen-of buitenlandse dreiging effectief te kunnen opvolgen, moet de VSSE (net als de ADIV) haar werking niet beperken tot het Belgisch grondgebied. Het wettelijk kader laat toe, binnen de hierna vermelde beperkingen, dat de VSSE inlichtingen in het buitenland kan verzamelen en collecte-activiteiten kan ontplooien buiten het Belgisch grondgebied via vier procedures.

(1) Via de samenwerking en de uitwisseling van informatie met buitenlandse partnerdiensten

Artikel 20 § 1 W. I&V stelt, *in fine*, dat de VSSE en de ADIV "*er eveneens voor (zorgen) dat er samenwerking is met de buitenlandse inlichtingen- en veiligheidsdiensten*". Deze samenwerking kan bilateraal of multilateraal zijn.

Via uitwisseling met diensten kan de VSSE kennis nemen van inlichtingen betreffende buitenlandse fenomenen en kan ze deze behandelen. De informele samenwerking op internationaal niveau binnen de Club van Bern is wat dit betreft belangrijk. Dit procedé op het vlak van inlichtingengaring vereist geen enkele activiteit op het buitenlands grondgebied, behoudens occasionele werkvergaderingen.

Ook kunnen inlichtingenofficieren (LO's) naar het buitenland gestuurd worden. Vanzelfsprekend bevinden die zich dan fysiek in het buitenland, terwijl ze vaak (maar niet altijd) werken in de kantoren van de partnerdiensten. Zij begeven zich evenwel nooit alleen op het terrein om inlichtingen te verzamelen.

---

[43] De te beschermen 'belangen' zijn: (1) de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, (2) de uitwendige veiligheid van de Staat en de internationale betrekkingen, (3 het wetenschappelijk en economisch potentieel van het land. Oe te beheersen 'bedreigingen' zijn: (1) spionage, (2) inmenging, (3) extremisme, (4) terrorisme, (5) proliferatie, (6) schadelijke sektarische organisaties en (7) criminele organisaties.

(2) Via gewone inlichtingenmethoden

Om inlichtingen te verzamelen, kan de VSSE ook gebruik maken van gewone inlichtingenmethoden. De wet heeft immers de inzet van deze methoden - anders dan de bijzondere inlichtingenmethoden - op geen enkele wijze beperkt tot het Belgisch grondgebied.

Dit betekent uiteraard niet dat deze methoden vanuit het standpunt van dat derde land zouden toegelaten zijn, noch dat buitenlandse actoren verplicht zijn om in te gaan op wat voor Belgische actoren als een 'vordering' kan gezien worden (zoals de verplichting voor overheden, telecombedrijven of logiesverstrekkende instanties om desgevraagd informatie over te maken). Vanuit Belgisch-juridisch standpunt gezien, verzet echter niets er zich tegen dat de VSSE alle gewone methoden (openlijk of clandestien) zou inzetten van op het Belgisch grondgebied of zelfs in een derde land.

Het Vast Comité I identificeert, praktisch gezien, twee mogelijkheden waarbij de VSSE inlichtingen in het buitenland kan vergaren via gewone inlichtingenmethoden:

– de VSSE kan in het buitenland beroep doen op menselijke bronnen (art. 18 W.I&V) overeenkomstig de richtlijnen van de Nationale Veiligheidsoverheid (NVR) en zoals bepaald in het Nationaal Strategisch Inlichtingenplan (NSIP)[44];
– de VSSE kan in het buitenland een observatie uitvoeren zoals voorzien in artikel 16/1 § 1 W. I&V, namelijk een observatie zonder behulp van een technisch middel.

(3) Via bepaalde bijzondere inlichtingenmethoden

Naast de gewone inlichtingenmethoden bestaan ook bijzondere inlichtingenmethoden (BIM's).

In dit verband moet worden gewezen naar een opvallende wetswijziging op het vlak van het toepassen van BIM's. Oorspronkelijk waren de BIM's exclusief beperkt tot het "*grondgebied van het Rijk*". In 2017 werd artikel 18/1, 1° WI&V vervangen (Wet van 30 maart 2017, *B.S.* 28 april 2017) en werd bepaald dat BIM's vanaf nu door de VSSE "*op of vanaf het grondgebied van het Rijk*" kunnen worden ingezet.

Sinds 2017 kan de informatievergaring via een BIM plaatsgrijpen in het buitenland, maar moet ingezet worden vanaf België. Op die manier is het dus bijvoorbeeld mogelijk om zich toegang te verschaffen tot een mailadres gekoppeld aan een buitenlandse server, maar enkel wanneer de verrichtingen gebeuren in België. Een ander klassiek voorbeeld is de observatie van een voertuig via een baken.[45] Dit baken zal steeds in België op het voertuig moeten worden aangebracht maar de via dit baken verzamelde informatie kan verzameld worden buiten de nationale grenzen.

---

44 Het betreft meer bepaald een plan goedgekeurd door de Nationale Veiligheidsraad, gezamenlijk opgesteld door de VSSE en de ADIV. Dit plan bepaalt in hoofdzaak de wijze waarop bepaalde prioriteiten moeten worden opgevolgd door de beide inlichtingendiensten.

45 Een baken is een toestel waarmee verplaatsingen van een voertuig kunnen worden gevolgd.

(4) Met de medewerking van de ADIV

Aangezien de ADIV veel meer wettelijke, materiële en menselijke collectecapaciteiten heeft in het buitenland, kan het voor de VSSE interessant zijn om de medewerking van deze dienst te verzoeken.

De inlichtingenwet voorziet hier in een zeer specifieke mogelijkheid: "*Op verzoek van de Veiligheid van de Staat verleent de Algemene Dienst Inlichting en Veiligheid zijn medewerking aan de Veiligheid van de Staat bij het inwinnen van inlichtingen wanneer militairen betrokken zijn bij activiteiten bedoeld in artikel 7, 1° 1 en 3°/1*" (art. 9 W. I&V).

Een meer algemene mogelijkheid tot samenwerking dient zich aan wanneer de VSSE een dreiging opvolgt die ook onder de bevoegdheid van de ADIV valt. Aan deze Iaatste dienst zou dan kunnen gevraagd worden om zijn dispositieven aan te wenden en de bekomen informatie te delen met de VSSE. Deze vorm van medewerking heeft echter zijn grenzen. Het kan niet de bedoeling zijn dat de VSSE via de ADIV haar eigen wettelijke beperkingen omzeilt.

I.2.3. DE PRAKTIJK VAN DE VSSE WAT BETREFT HET VERZAMELEN VAN BUITENLANDSE INLICHTINGEN

Al is dit niet altijd de positie van de dienst is geweest[46], werd de ontwikkeling van een 'netwerk van VSSE-functionarissen in het buitenland' een uitgesproken ambitie van de dienst en opgenomen in haar '*Strategische visie VSSE 2019-2020*'.[47] Concreet nemen de activiteiten aangaande het verzamelen van informatie in het buitenland door de VSSE verschillende vormen aan.

I.2.3.1. De uitwisseling van gegevens met buitenlandse partners

Momenteel verkrijgt de VSSE een groot deel van haar buitenlandse inlichtingen via samenwerking en informatie-uitwisseling met buitenlandse partnerdiensten. Deze betrekkingen variëren van eenvoudige protocollaire contacten tot uitgebreide operationele samenwerking.[48] Van de ongeveer 120 buitenlandse diensten waarmee

---

46 In de eerste decennia na het stemmen van de Wet houdende regeling van de inlichtingen- veiligheidsdiensten van 30 november 1998 (W.I&V) had de VSSE een restrictieve visie op haar opdracht, die de dienst beperkt achtte tot het nationale grondgebied. Deze visie, aangehouden door de dienst zelf, berustte op een restrictieve interpretatie van de wet.

47 *Strategische visie 2019-2020 van de VSSE,* p. 7.

48 De wijze waarop de Belgische inlichtingendiensten samenwerken op bilateraal niveau met buitenlandse partnerdiensten, werd gedefinieerd in een richtlijn dewelke op 26 september 2016 werd goedgekeurd door de Nationale Veiligheidsraad. Het betreft de « Richtlijn aangaande de relaties van de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichtingen (ADIV) met buitenlandse inlichtingendiensten de Belgische inlichtingendiensten met buitenlandse inlichtingendiensten ». Deze Richtlijn voorziet in een tweejaarlijkse evaluatie van de samenwerking.

de VSSE bilaterale betrekkingen onderhoudt, hebben er zich ongeveer 70 verbindingsofficieren bij VSSE aangemeld.[49]

I.2.3.2. Het inzetten van eigen verbindingsofficieren

In haar nota van maart 2021 getiteld "*VSSE internationale relaties 2021-2024. Visie — Context — Doelstellingen*", geeft de VSSE aan dat zij haar eigen informatiepositie in het buitenland wil verbeteren en haar afhankelijkheid van informatie van externe partnerdiensten wil verminderen.

De VSSE zet daarin uiteen dat het inzetten van permanente vertegenwoordigers in het buitenland een oplossing kan bieden, en dat dit een aanvulling moet zijn op de informatie-uitwisseling met buitenlandse partnerdiensten. Volgens de VSSE kan de vertegenwoordiging, afhankelijk van de doelstellingen van haar diensten (en de vraag of zij operationeel of strategisch is), twee vormen aannemen:

- een vertegenwoordiging in landen met een aanzienlijke en directe operationele impact op de verschijnselen in België die voor de VSSE prioritair zijn en waarvoor het operationele rendement, door een permanente aanwezigheid, kan worden verhoogd;
- een diplomatieke vorm van vertegenwoordiging waarbij de permanente aanwezigheid duidelijk een meerwaarde kan betekenen bovenop de bestaande geïnstitutionaliseerde betrekkingen, en waarbij deze meerwaarde niet op een andere manier kan worden verkregen.

Zoals besproken in het Comité-onderzoek betreffende de opvolging van de aanbevelingen van de Onderzoekscommissie 'Aanslagen', heeft de VSSE momenteel weinig verbindingsofficieren.

De VSSE is voornemens het aantal verbindingsofficieren in de toekomst uit te breiden.

In de VSSE-strategienota over internationale betrekkingen voor de periode 2021 - 2024 staat dat de inzet van de LO's moet plaatsvinden in een context van complementariteit en synergie met nationale partners, in dit geval de ADIV en de Federale Politie.

I.2.3.3. Het beroep doen op het netwerk van verbindingsofficieren van de Federale Politie in het buitenland

De VSSE heeft verklaard gebruik te willen maken van het uitgebreide netwerk van verbindingsofficieren van de Federale Politie in het buitenland. In september 2020

[49] Nota van de VSSE genaamd '*Internationale relaties VSSE 2021-2024. Visie — Context — Doelstellingen*', dateren van 12 maart 2021.

is daartoe een samenwerkingsovereenkomst gesloten tussen de VSSE en de Federale Politie.

In het kader van het toezichtonderzoek naar de opvolging van de aanbevelingen van de Parlementaire Onderzoekscommissie 'Aanslagen', werd de VSSE verzocht haar samenwerking met de Federale Politie in dit verband te verduidelijken. Zij verklaarde: "*concreet komt de VSSE regelmatig samen met de verbindingsofficieren van de Federale Politie en wisselt zij via haar deskundigen informatie met hen uit. De VSSE neemt ook elk jaar deel aan de 'week van de verbindingsofficieren' die door de Federale Politie wordt georganiseerd*".[50]

Het protocolakkoord vermeldt dat de samenwerking tussen de Federale Politie en de VSSE jaarlijks zal worden geëvalueerd. De laatste evaluatie vond plaats begin april 2022 en bevestigde de tevredenheid van beide partijen.[51]

I.2.3.4. Wat betreft het ontwikkelen van HUMINT-activiteiten in het buitenland

Net zoals het Comité, beoordeelt de VSSE het gebruik van menselijke bronnen in het buitenland als wettelijk. De VSSE voegt toe dat een onderscheid moet worden gemaakt tussen (1) een reeds in België aangeworven bron die naar het buitenland reist of daar verblijft en (2) de benadering, aanwerving en behandeling van een bron in het buitenland.

I.2.4. CONCLUSIES EN AANBEVELINGEN

Het huidig rechtskader biedt de VSSE voldoende mogelijkheden om aan haar potentiële behoeften en ambities op het gebied van buitenlandse inlichtingen(-capaciteiten) te voldoen indien de omstandigheden dat vereisen. Terwijl de dienst in het verleden van oordeel was dat de W.I&V. haar dergelijke mogelijkheden niet bood, is de dienst vandaag, zoals het Comité, van mening dat in het buitenland, gewone en sommige bijzondere methoden kunnen worden gebruikt.

---

50 Brief van de VSSE van 3 augustus 2022 aan het Vast Comité I betreffende de aanbevelingen van de parlementaire onderzoekscommissie 'Aanslagen' - reacties van de VSSE.

51 *Ibidem.*

I.3. DE GEVOLGEN VAN BUITENLANDSE MONITORINGNETWERKEN VOOR DE BELGISCHE INLICHTINGENDIENSTEN: DE ZAAK CRYPTO AG, RUBICON EN MAXIMATOR

In oktober 2022 sloot het Vast Comité I een toezichtonderzoek inzake de gevolgen voor de Belgische inlichtingendiensten van buitenlandse monitoringnetwerken. Het onderzoek bestond uit twee delen:

- Het eerste luik betrof de afluisteroperatie 'RUBICON' en bij uitbreiding de coderingsapparatuur CRYPTO AG (I.3.1.)
- Een tweede luik behandelde de geheime alliantie SIGINT MAXIMATOR (I.3.2.).[52]

Het Comité wou daarbij onderzoeken of enerzijds de twee Belgische inlichtingendiensten op de hoogte waren van het bestaan hiervan vooraleer het bekend werd bij het grote publiek en, anderzijds, in hoevere beide inlichtingendiensen hierdoor waren getroffen.

I.3.1. CRYPTO AG - RUBICON

In de eerste helft van 2020 werden in de pers onthullingen gedaan over het zogenaamde 'RUBICON'-spionageprogramma. Uit bepaalde berichtgeving bleek dat bij het begin van de jaren '60 van de vorige eeuw de Amerikaanse inlichtingendiensten *Central Intelligence Agency* (CIA) en *National Security Agency* (NSA) en de Duitse inlichtingendienst *Bundesnachrichtendienst* (BND) belangen had in een Zwitserse onderneming, CRYPTO AG. Deze vervaardigde apparatuur voor gecrypteerde of versleutelde communicatie.

De Amerikaanse en Duitse inlichtingendiensten konden door hun zeggenschap binnen deze firma gedurende tientallen jaren berichten die via de CRYPTO-coderingsapparatuur werden verzonden, meelezen. Het betrof niet alleen communicatie tussen vijandige mogendheden, maar ook tussen bevriende en zelfs NAVO-landen. In 1993 besloot Duitsland zich terug te trekken uit het programma en liet ze CRYPTO AG in de handen van de CIA, dewelke, gedurende de 25 volgende jaren, alleen eigenaar was van het bedrijf.

Verschillende landen hadden, in meer of mindere mate, kennis van bepaalde aspecten van dit spionageprogramma. Dit was hoofdzakelijk het geval vanaf de jaren '80, moment waarop er voor het eerst vragen werden gesteld over de activiteiten van het bedrijf CRYPTO AG.[53] Het Vast Comité I wou, middels zijn

---

52 Deze toezichtonderzoeken werden geopend in 2020.

53 James Bamford, 1982, *The Puzzle Palace, A Report on America's Most Secret Agency*.

onderzoek, uitmaken of de Belgische inlichtingendiensten op de hoogte waren van deze operatie of er door werden getroffen.[54]

De VSSE verklaarde dat de dienst pas door de onthullingen in de pers op de hoogte was van de banden tussen het bedrijf CRYPTO AG en de Amerikaanse inlichtingendiensten CIA en NSA en de Duitse BND. Wat de ADIV betreft werd, van zodra de RUBICON-afluisterpraktijken in de pers waren verschenen, op 12 februari 2020 via Belga een persbericht verspreid waarin zij meedeelde dat zij op de hoogte was van de RUBICON-affaire en de mogelijke omvang van de afluisterpraktijken onderzocht. De ADIV bevestigde dit ook aan de krant De Tijd, waarin staat dat "*De ADIV doet er alles aan om zich tegen hen (bedoeld wordt: afluisterpraktijken) te wapenen en maakt vooral een erezaak van om het wettelijk kader op dit gebied te respecteren en anderzijds een morele code te hanteren ten opzichte van zijn partners/bondgenoten in een wereld waar, zonder naïef te zijn, vertrouwen vaak met voorzichtigheid gepaard gaat*". [55]

Het Vast Comité I bevroeg beide Belgische inlichtingendiensten omtrent een mogelijke interne compromittering als gevolg van de zaak RUBICON. Op basis van geclassificeerde informatie vanuit zowel de VSSE en de ADIV, stelde het Comité dat de compromittering van de door de diensten gebruikte apparaten "*miniem*" was en, wat betreft Defensie, "*uiterst miniem*".

I.3.2. MAXIMATOR

In de nasleep van het RUBICON-cryptageschandaal, publiceerde de Nederlandse universitair en expert in informaticabeveiliging, Prof. Bart JACOBS in april 2020 een wetenschappelijk artikel over het bestaan van een geheime SIGINT-alliantie tussen verschillende Europese landen, bekend onder de noemer 'MAXIMATOR'.[56]

Het artikel onthult dat een Europese SIGINT-samenwerking in 1976 heimelijk werd opgericht. Oorspronkelijk gebeurde dit met drie deelnemers: Denemarken, Zweden en Duitsland. Nederland vervoegde de alliantie in 1978, terwijl Frankrijk in 1985 zou zijn toegetreden en sinds 2006 de *lead* hebben genomen.[57, 58]

---

54 In het verleden heeft het Comité meerdere toezichtonderzoeken uitgevoerd naar andere afluister- en interceptieschandalen. Zie bijvorbeeld VAST COMITÉ I, *Activiteitenverslag 1999*, 24 – 51 ('Onderzoek over de manier waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, ECHELON genaamd, voor het onderscheppen van het telefoon- en faxverkeer in België'); *Activiteitenverslag 2006*, 42 – 51 ('De zaak Swift'); *Activiteitenverslag 2014*, 8-35 ('De Snowden-onthullingen en de informatiepositie van de Belgische inlichtingendiensten').

55 L. BOVE, *De Tijd*, 12 februari 2020 ('*België onderzoekt jarenlange spionage door CIA')*.

56 "Maximator: European signals intelligence cooperation, from a Dutch perspective", *Intelligence and National Security*, Routledge, Volume 35, Number 5, August 2020 p.659-668.

57 *www.electrospaces.net/2020/05/maximator-and-other-european-sigint-alliance*

58 J.J. QUIQUATER, Cruel paradoxe de la cryptographie belge, 20 mei 2020, *www.regional-it.be/detached/cruel-paradoxe-de- la-cryptographie-belge*

Het MAXIMATOR-netwerk zou sterk geleund hebben op de door de Duitse partner geleverde informatie die afkomstig was van het kraken van CRYPTO AG-communicatie.

Niettegenstaande het bijzonder geheime karakter van het programma zouden na verloop van tijd een aantal andere Europese landen op de hoogte gewest zijn van het netwerk. Het bleef daarbij niet bij de loutere kennis van het bestaan van het samenwerkingsverband. Enkele landen zouden op eigen initiatief gevraagd hebben zelfs om deel te kunnen uitmaken van het MAXIMATOR-netwerk. De meesten werden geweigerd, vaak op basis van het feit dat ze over geen voldoende cryptoanalyse ervaring of expertise beschikten.

In zijn artikel vermeldt JACOBS dat België vanwege het gebrek aan SIGINT-capaciteiten, expliciet werd uitgesloten van het netwerk – wat het tot de opvallende uitzondering in Noord-West-Europa maakte. De auteur preciseerde: *"As a result, Belgium was not 'protected' by the Maximator members and bought (weakened) CRYPTO AG equipment, as also reported in the leaked BND and CIA documents, so that its (CRYPTO AG based) communication was readable by both western five-member SIGINT alliances (Five-eyes and Maximator)"*. [59]

Op vragen van het Comité hierover antwoordden de inlichtingendiensten dat ze niet op de hoogte waren van de MAXIMATOR-alliantie voordat het artikel van Prof. JACOBS verscheen.

Bij de afsluiting van zijn onderzoek achtte het Vast Comité I dat de kans groot dat België zelf het voorwerp heeft uitgemaakt van interceptie-activiteiten van het MAXIMATOR-netwerk.

I.4. OPVOLGING VAN HET TOEZICHTONDERZOEK 'PRISM'

In 2013 voerde het Vast Comité I een toezichtonderzoek naar de aandacht die de Belgische inlichtingendiensten al dan niet besteedden aan de mogelijke dreigingen voor het Belgische Wetenschappelijk en Economisch Potentieel (WEP) uitgaande van elektronische bewakingsprogramma's op communicatie- en informatiesystemen die op grote schaal door inlichtingendiensten worden ingezet.[60]

---

59 "Als gevolg hiervan werd België niet beschermd door de activiteiten van MAXIMATOR-leden en kocht het (afgezwakte en minder beveiligde) CRYPTO AG-apparatuur, wat ook blijkt uit de gelekte BND- en CIA-documenten. Op die manier werd haar communicatie die verliep over AG CRYPTO-toestellen afgeluisterd door zowel het FIVE EYES-verband (nvdr. een bondgenootschap tussen de inlichtingendiensten van Australië, Canada, Nieuw-Zeeland, het Verenigd Koninkrijk en de Verenigde Staten) als door het MAXIMATOR-samenwerkingsverband" (vrije vertaling).

60 VAST COMITÉ I, *Activiteitenverslag 2016*, pp. 52-56 ('De bescherming van het wetenschappelijk en economisch potentieel en de Snowden-onthullingen').

Op verzoek van de parlementaire Begeleidingscommissie, besloot het Vast Comité I om bepaalde implementeringen van de elf aanbevelingen uit het onderzoek van 2013 tegen het licht te houden, en na te gaan op welke wijze de aanbevelingen werden opgevolgd.[61] Deze aanbevelingen worden hieronder in vijf thema's gegroepeerd.

I.4.1. DE NOODZAKELIJKE OPVOLGING VAN NIEUWE TECHNOLOGISCHE MOGELIJKHEDEN OP VLAK VAN MASSALE DATACAPTATIE

In zijn initiële toezichtonderzoek verzocht het Comité beide inlichtingendiensten om aandacht te besteden aan de inherente risico's die nieuwe technologische mogelijkheden met zich mee kunnen brengen op vlak van massale datacaptatie en economische en wetenschappelijke spionage.

Aandacht voor dit fenomeen is wat VSSE en SGRS betreft noodzakelijk om hun informatiepositie te consolideren over de middelen en *modus operandi* van andere diensten. Dit niet alleen om de autoriteiten zo nodig te informeren of tegenmaatregelen te treffen, maar ook om hun eigen collecte-technieken te evalueren.

Het Vast Comité I merkte op een dergelijke fenomeenanalyse - bedoeld om de bedreiging die uitgaat van buitenlandse interceptiesystemen voor het Belgische WEP en de kritische infrastructuren in kaart te brengen - nog niet werd uitgevoerd.

Het Vast Comité I stelde vast dat beide diensten verklaren dat zij niet over de middelen beschikken om het fenomeen van massale datacaptatie naar behoren aan te pakken. Het Comité is echter van mening dat de diensten moeten blijven investeren in de bescherming tegen dergelijke massale datacaptatie-praktijken. Het Comité juicht dan ook de creatie van een het Belgische *Cyber Commando* van Defensie (onder de vleugels van ADIV) en officieel operationeel sinds oktober 2022, toe. Deze entiteit zal verantwoordelijk zijn voor de uitvoering van de strategie op het vlak van *cyber security*.

I.4.2. NAUWERE SAMENWERKING TUSSEN DE PARTNERS OP NATIONAAL NIVEAU

In 2013 hadden verschillende aanbevelingen van het Vast Comité I betrekking op de samenwerking tussen de Belgische diensten. Het Comité riep de twee inlichtingendiensten op hun samenwerking te intensiveren. Het betreurde met name dat de VSSE en de ADIV geen gebruik hadden gemaakt van de mechanismen voor

[61] Op verzoek in november 2019 van de parlementaire Begeleidingscommissie, opende het Vast Comité I een toezichtonderzoek in september 2020 en bezorgde de Begeleidingscommissie het toezichtrapport in oktober 2022.

informatie-uitwisseling waarin hun in 2004 ondertekende samenwerkingsprotocol voorziet - bijvoorbeeld de oprichting van platforms voor *ad-hoc* samenwerking. Sinds 2013 is er geen platform voor gegevensverzameling meer opgericht. Wel is er nu een coördinatieplatform gewijd aan de bescherming van het WEP, onder voorzitterschap van de VSSE.

Volgens het Vast Comité I moeten - op permanente basis - extra middelen worden uitgetrokken voor de bescherming van WEP. Het Comité was tevens van mening dat de bescherming van het WEP het voorwerp van opvolging kon uitmaken binnen een gemeenschappelijk platform van de twee inlichtingendiensten, vergelijkbaar met het CT-platform in de strijd tegen het terrorisme.

Daarnaast had een aanbeveling van het Vast Comité I aan het adres van de ADIV betrekking op de compartimentering en verspreiding van informatie binnen de dienst. In het licht van de bevindingen van een eerder onderzoek[62] en de antwoorden van de ADIV, betreurde het Vast Comité I dat op dit punt onvoldoende vooruitgang was geboekt, met name omdat er binnen de dienst niet één allesomvattend computersysteem bestaat.

Naast de samenwerking tussen de inlichtingendiensten, heeft het Comité ook aangedrongen op een bredere interdepartementale samenwerking op het gebied van cyberveiligheid, ICT-beveiliging en cyberinlichtingen. Het Vast Comité I stelde vast dat het Centrum voor Cyberveiligheid België (CCB) in oktober 2014 werd opgericht. Hoewel het CCB sinds december 2020 betrokken is bij de besprekingen van het WEP-coördinatieplatform, neemt het niet systematisch deel aan de vergaderingen van het Strategisch Comité en het Coördinatiecomité voor inlichtingen en veiligheid, noch aan die van de Nationale Veiligheidsraad. Het CCB is evenmin belast met het opsporen van cyberdreigingen en is evenmin rechtstreeks verantwoordelijk voor de bescherming van het WEP.

Naast de oprichting van de CCB zal de hervorming van de Nationale Veiligheidsoverheid (NVO) en het Defensie Cyber Commando het huidige inlichtingen- en veiligheidslandschap ingrijpend veranderen.

I.4.3. POLITIEKE RUGDEKKING

Op internationaal niveau heeft het Comité aanbevolen dat de ADIV en de VSSE "*iedere bedreiging ernstig te nemen, ook als deze afkomstig is van bevriende diensten of diensten van bevriende landen*". Het Comité beval tevens aan de voorwaarden voor samenwerking met buitenlandse partners vast te leggen in richtlijnen en te onderwerpen aan politieke controle. Een andere aanbeveling was specifiek gericht

62 VAST COMITÉ I, *Activiteitenverslag 2021,* pp. 38-51 ('Het opsporen en opvolgen van de radicalisering van een militair : de zaak-Jürgen Conings').

op bi- of multilaterale samenwerkingsovereenkomsten die door de politieke leiding moeten worden bekrachtigd.[63]

In dit verband dient de 'Richtlijn betreffende de samenwerking van de Belgische inlichtingendiensten met de buitenlandse inlichtingendiensten' van 26 september 2016 van de Nationale Veiligheidsraad (NVR) te worden vermeld. Het document beoogt de keuze van de internationale partners van de ADIV en de VSSE te objectiveren, teneinde de omvang en de aard van de samenwerking met deze partners te bepalen en deze samenwerking regelmatig te evalueren. De richtlijn geeft ook richtsnoeren voor het delen van persoonsgegevens met buitenlandse agentschappen. Uit de richtlijn blijkt echter niet duidelijk of de VSSE en de ADIV voorafgaande ministeriële (of andere) toestemming of machtiging nodig hebben. Volgens het Vast Comité I lijkt een dergelijke toestemming essentieel.[64]

Sinds het onderzoek van het Vast Comité I naar het Memorandum of Understanding tussen de ADIV en een Rwandese inlichtingendienst in 2020, zijn de diensten ook verplicht om elke twee jaar een gezamenlijke evaluatie van hun gemeenschappelijke strategische partners uit te voeren. In dat kader heeft het Vast Comité I ook aanbevolen dat bilaterale overeenkomsten tussen de diensten en hun strategische partners door de bevoegde minister worden goedgekeurd of gedekt.

Het Vast Comité I is van mening dat de dreiging die uitgaat van het gebruik van massadatacaptatiesystemen door een strategische partner moet worden meegenomen in de beoordeling van de inlichtingendienst van zijn relatie met een 'bevriende' partnerdienst.

Meer in het algemeen heeft het Comité in 2013 aanbevolen dat het Ministerieel Comité voor Inlichtingen en Veiligheid - nu de Nationale Veiligheidsraad - de inlichtingendiensten beleidsrichtlijnen geeft.

Voor zover het Vast Comité I heeft kunnen nagaan, heeft de Nationale Veiligheidsraad na het onderzoek van 2013 geen specifieke aandacht besteed aan het fenomeen van massale datacaptatie. Het vaststellen van het algemene inlichtingenbeleid en de daaruit voortvloeiende prioriteiten behoort volgens het Comité tot de verantwoordelijkheid van de NVR. Het Vast Comité I verwacht echter nog steeds dat de NVR zich actiever met dit onderwerp bezighoudt.

I.4.4. WETGEVENDE PRECISERINGEN

In 2013 verzocht het Comité om verschillende wetgevende preciseringen wat betreft de methoden voor de verzameling van gegevens. Het Comité beval vooreerst

---

63 Deze aanbeveling werd hernomen uit een toezichtonderzoek uit 2017. Zie VAST COMITÉ I, *Activiteitenverslag 2017*, 107 ('Politieke dekking voor samenwerkingsverbanden').

64 Zie in die zin : Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van inlichtingen- en veiligheidsdiensten met het oog op het invoeren van wegingsnotities voor de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten, *Parl. St.*, Kamer 2019-20, 55K956/001 (23 januari 2020).

aan om, gezien de technologische evoluties, het territoriaal toepassingsgebied voor wat betreft de inzet van bijzondere inlichtingenmethoden (BIM) aan te passen.

Met de Wet van 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek[65] (hierna de BIM-Actualisatiewet) werden belangrijke wijzigingen aan het territoriaal toepassingsgebied van de specifieke en uitzonderlijke methoden doorgevoerd, daarin inbegrepen het onderscheppen van (tele)communicaties (*cf.* art. 18/17 W.I&V) en het binnendringen in informaticasystemen (*cf.* art. 18/16 W.I&V).

Vóór de vernoemde wetswijziging kon een BIM-methode door de VSSE slechts *"op het grondgebied van het Rijk"* worden aangewend. De wet stelt op heden dat de inlichtingendienst de BIM-methoden *"op of vanaf het grondgebied van het Rijk"* uitoefent (*cf.* art. 18/1, 1° W.I&V). De memorie van toelichting[66] van de BIM-Actualisatiewet verduidelijkt hierbij dat de VSSE voortaan de BIM-methoden 'op' het Belgisch grondgebied moet 'aanwenden', wat betekent dat de VSSE-agenten zich niet fysiek naar het buitenland mogen begeven om bijvoorbeeld een woning te doorzoeken, een micro of camera te installeren of een telefoon uit te lezen. Het verzamelen van informatie zelf mag wel in het buitenland gebeuren.[67]

Wat betreft de ADIV ging de wetgever nog een grote stap verder door niet langer enige territoriale beperkingen te koppelen aan de uitoefening van BIM-methoden (*cf.* art. 18/1, 2° W.I&V). De memorie van toelichting[68] van de BIM-actualisatiewet stelt hierover dat deze wijziging is gerechtvaardigd door het feit dat de meerderheid van de opdrachten van de ADIV worden uitgevoerd in het buitenland, zoals bijvoorbeeld de bescherming van de opdrachten van de Krijgsmacht, of van Belgische onderdanen in het buitenland. Verder wordt gesteld dat in het kader van de operaties met een door de Veiligheidsraad van de Verenigde Naties toegekend mandaat vaak van de inlichtingendiensten van de coalitie wordt verwacht dat ze inlichtingenonderzoeken voeren waarvoor specifieke en uitzonderlijke methoden moeten worden aangewend en dat de beperking van het territoriale toepassingsgebied de ADIV verhindert zijn deel van de samenwerking na te komen.[69]

Het is evenwel vermeldenswaardig dat de memorie van toelichting stelt dat de toepassing van specifieke en uitzonderlijke methoden bij operaties in het buitenland niet altijd toepasbaar is.[70]

---

65 Wet van 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek, *BS* 28 april 2017.

66 MvT, *Parl. St.* Kamer 2015-16, nr. 54-2043/001, 46-47.

67 Ter verduidelijking hiervan worden volgende voorbeelden gegeven, die eveneens van onmiddellijk belang zijn voor dit toezichtonderzoek: (1) het binnendringen in een informaticasysteem vanuit België, maar die op een grensoverschrijdend netwerk wordt uitgevoerd, en (2) een doelwit dat afgeluisterd wordt die een buitenlandse oproep ontvangt.

68 MvT, *Parl. St.* Kamer 2015-16, nr. 54-2043/001, 47-50.

69 MvT, *Parl. St.* Kamer 2015-16, nr. 54-2043/001, 6.

70 MvT, *Parl. St.* Kamer 2015-16, nr. 54-2043/001, 7, 84 en 86.

Volgens het Vast Comité I bracht deze BIM-Actualisatiewet een welgekomen verduidelijking wat betreft de territoriale toepassing van de inzet van bijzondere inlichtingenmethoden. Enigszins verrassend heeft het Vast Comité I naar aanleiding van haar uitgevoerde controle op de bijzondere inlichtingenmethoden (BIM's) moeten vaststellen dat de ADIV tot oktober 2022 nooit een BIM-methode in het buitenland heeft ingezet.

Een tweede aanbeveling betrof de Belgische INT-regeling, die de ADIV toelaat buitenlandse communicaties te intercepteren (*Signal Intelligence* of SIGINT). Gezien de technologische ontwikkelingen, beval het Comité aan dat de wetgever de regelgeving hieromtrent zou herevalueren.[71]

In die zin bracht de BIM-Actualisatiewet in 2017 een aantal wijzigingen aan, zoals bijvoorbeeld:

- De interceptiemogelijkheden van de ADIV hebben niet enkel betrekking op elke communicatie "uitgezonden in het buitenland". De mogelijkheden werden uitgebreid in de zin dat ook communicaties "ontvangen in het buitenland" voortaan onder het toepassingsgebied vallen. Hierdoor werd de ADIV bevoegd om elke communicatievorm in het buitenland te intercepteren, ongeacht wie aan de basis van de oproep ligt en waar degene die aan de basis van de oproep ligt zich bevindt, voor zover een deel van de communicatie in het buitenland verloopt.
- Er werd in het kader van de uitvoering van de interceptiebevoegdheid in hoofde van de telecomoperatoren en -providers een wettelijke medewerkingsplicht gecreëerd. *Cable taping*, die reeds sinds de wet van 3 april 2003 (*supra*) tot de wettelijke mogelijkheden van de ADIV behoorde, werd hierdoor meer uitvoerbaar;
- De SIGINT-regeling, zijnde de interceptie van buitenlandse communicatie (*cf*. art. 44 W.I&V), werd uitgebreid naar een CYBER-reglementering, m.n. inzake de intrusie van buitenlandse informaticaystemen (*cf*. art. 44/1 W.I&V) en een reglementering voor de opname van beelden in het buitenland (*cf*. art. 44/2 W.I&V).
- Verder werd de inlichtingenopdracht van de ADIV in belangrijke mate uitgebreid tot inlichtingensteun aan militaire operaties. Vanaf nu behoort ook tot de inlichtingenopdracht van de ADIV: *"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*

---

71 Elementen die bij een dergelijke herziening alleszins moeten bestudeerd worden, zijn de mate waarin intercepties al dan niet gericht moeten gebeuren, de juiste draagwijdte van de mogelijkheid om signalen te 'zoeken', de mate van precisering van het jaarlijkse afluisterplan, de mogelijkheid om aan data-mining te doen in bulkinformatie, en de vraag of buitenlandse SIGINT-operaties moeten kaderen binnen breder een 'internationaal mandaat'. Deze bevoegdheid was al in 2003 uitgebreid tot alle radiocommunicaties van elk type uitgezonden in het buitenland (en dus niet louter alleen maar de militaire communicaties). Mvt, *Parl. St.* Kamer 2003-'04, 50K2059/001, 4-6.

dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties, en er de bevoegde ministers onverwijld over in te lichten" (*cf.* art. 11, §1, 1° *in limine* W.I&V). Deze uitbreiding van het toepassingsgebied creëert logischerwijs eveneens een ruimer toepassingsgebied bij de interceptiebevoegdheid bedoeld in artikel 44 W.I&V;
– Het toezicht werd versterkt met name door een meer ontwikkelde motivering van de jaarlijkse lijst en door de maandelijkse overzending aan het Comité van een gemotiveerde lijst met landen of organisaties en instellingen die het voorwerp zijn geweest van een afluistering intrusie of beeldopnames.

I.4.5. EEN STRIKTE NALEVING VAN ARTIKEL 33 W.TOEZICHT

In een laatste aanbeveling ten slotte wees het Vast Comité I op de verplichting ex artikel 33 W.Toezicht om *'uit eigen beweging aan het Vast Comité I de interne reglementen en richtlijnen over, alsook alle documenten die de handelwijze van de leden van die diensten regelen*' over te zenden. Deze verplichting geldt ook voor afspraken, MOU's of akkoorden gesloten op internationaal vlak, weze het bi- of multilateraal.

Niettegenstaande dit in het verleden regelmatig werd herhaald[72], blijft deze aanbeveling van toepassing. Immers, het doorgeven van richtlijnen, SOP's en andere voorschriften gebeurt nog steeds niet automatisch en systematisch. De naleving van artikel 33 W.Toezicht blijft een werkpunt, zij het veel meer voor de ADIV dan voor de VSSE.

I.5. TOEZICHTONDERZOEK TER NAVOLGING VAN DE ONTHULLINGEN OVER HET GEBRUIK VAN PEGASUS-SOFTWARE

Op 18 juli 2021 onthulden zeventien internationale media, waaronder *Le Soir* en *Knack*, het bestaan van de Pegasus-software. Het bleek te gaan om software die door het Israëlische bedrijf NSO wordt verkocht aan regeringen en hun inlichtingen- en/of veiligheidsdiensten om hen in staat te stellen smartphones te beheren buiten het medeweten van hun eigenaars.

---

72 Hierover werd eerder reeds onderzoek uitgevoerd: VAST COMITE I, *Activiteitenverslag 1996*, 28-32 (Verslag over de toepassing door de inlichtingendiensten van artikel 33 alinea 2 W.Toezicht); *Activiteitenverslag 2001,* 218-220 (De noodzakelijke inlichtingen waarover het Vast Comité I meent te moeten beschikken met het oog op de doeltreffende uitvoering van zijn opdracht); *Activiteitenverslag 2002,* 27 (Het ambtshalve toezenden van bepaalde documenten van de inlichtingendiensten aan het Vast Comité I); *Activiteitenverslag 2006,* 12; *Activiteitenverslag 2013*, 116; *Activiteitenverslag 2014*, 120. .

Het consortium van journalisten onthulde dat zij toegang hadden tot meer dan 50.000 telefoonnummers die het doelwit zouden geweest zijn van klanten van de Pegasus-software. *Le Soir* meldde dat onder de 50.000 telefoonnummers verschillende Belgische nummers voorkwamen en dat, volgens drie bronnen, "*la Belgique figurerait parmi les clients de NSO*".[73]

Het Vast Comité I besliste een toezichtonderzoek in te stellen bestaande uit twee luiken.[74] In de eerste plaats moest worden nagegaan of de Belgische inlichtingendiensten de software (of een equivalent daarvan) gebruiken/hebben gebruikt in het kader van hun opdrachten en of dit gebruik in overeenstemming is met het geldende wettelijke kader. Vervolgens, gezien het gebruik van de Pegasus-software door buitenlandse diensten (inlichtingen- en/of veiligheidsdiensten, particuliere ondernemingen, enz.) tegen Belgische personen en/of rechtspersonen, had het onderzoek tot doel na te gaan of de Belgische inlichtingendiensten zijn uitgerust om deze dreiging te identificeren en te beheersen, of zelfs tegen te gaan. Om beide aspecten aan bod te laten komen, werden vijf thema's besproken.

I.5.1. STAAT HET WETTELIJKE KADER IN BELGIË TOE DAT DE BELGISCHE INLICHTINGENDIENSTEN GEBRUIK MAKEN VAN EEN SOFTWARE VAN HET TYPE PEGASUS?

De Belgische wetgever heeft als algemeen beginsel gesteld dat het verboden is elektronische privé-communicatie af te luisteren, op te nemen en er kennis van te nemen tijdens de overdracht en met behulp van om het even welk toestel. Deze verboden, die betrekking hebben op ernstige inbreuken op de persoonlijke levenssfeer, worden krachtens de artikelen 259*bis* en 314*bis* van het Strafwetboek strafbaar gesteld met geldboetes en gevangenisstraf.

De Belgische wetgever is er echter toe gebracht het uitzonderlijke gebruik van een aanval op de bescherming van de private elektronische communicatie bij bepaalde bedreigingen te regelen. De wetgever heeft getracht *a priori* tegenstrijdige belangen met elkaar te verzoenen, namelijk enerzijds de eerbiediging van de persoonlijke levenssfeer van personen en anderzijds de behoefte aan een doeltreffender bescherming van de samenleving tegen bedreigingen zoals terrorisme of

---

73 *Le Soir*, 18 juli 2021, ('Projet Pegasus : un logiciel de cyberespionnage quasiment indétectable'). De Veiligheid van de Staat (VSSE), noch de Algemene Dienst Inlichting en Veiligheid (ADIV) en evenmin de Federale politie wilden tegenover de media reageren zich beroepend op 'vertrouwelijke' informatie.

74 Het onderzoek werd geopend in juli 2021. Het rapport werd in oktober 2022 overgemaakt aan de Begeleidingscommissie. Na het afsluiten van het rapport, werd ook door Europa hierover gepubliceerd: 'Ontwerpverslag over het onderzoek naar vermeende inbreuken op en gevallen van wanbeheer bij het toepassen van het Unierecht met betrekking tot het gebruik van Pegasus en soortgelijke spyware voor surveillance' van de Enquêtecommissie om het gebruik van Pegasus en soortgelijke spyware voor surveillance te onderzoeken (2022/2077(INI), 28 november 2022, https://www.europarl.europa.eu/doceo/document/PEGA-PR-738492_NL.pdf).

zware en georganiseerde criminaliteit. In het licht van de artikelen 12 en 22 van de Grondwet en artikel 8 van het Europees Verdrag voor de Rechten van de Mens moest duidelijk en nauwkeurig worden bepaald welke bevoegdheden de inlichtingendiensten kunnen hanteren wanneer zij ingrijpen in de uitoefening van individuele rechten en vrijheden. Het doel was het mogelijk te maken om, onder bepaalde voorwaarden en onder strikte jurisdictionele controle, met technische middelen niet voor het publiek toegankelijke communicatie of gegevens in een computersysteem of een deel daarvan te onderscheppen, er kennis van te nemen, deze te onderzoeken en te registreren, of de zoekactie in een computersysteem of een deel daarvan uit te breiden. Deze regels werden in het Wetboek van Strafvordering en in de W.I&V opgenomen.

De W.I&V voorziet dus in al de methoden die door de inlichtingendiensten kunnen worden ingezet, waarbij de meest ingrijpende methoden aan een *a priori* en *a posteriori* jurisdictionele controle dienen onderworpen te worden.[75] Elke bijzondere techniek die niet uitdrukkelijk door de wet wordt toegestaan, is impliciet verboden.

Meer bepaald staat artikel 18/16 W.I&V het binnendringen in een computersysteem en het verzamelen van gegevens toe. Het aftappen, het kennisnemen en het opnemen van communicatie zijn op hun beurt geregeld in artikel 18/17 W.I&V. Het gaat om zogenaamde 'uitzonderlijke' methoden waarvan de toepassing op straffe van nietigheid een met redenen omkleed besluit van het betrokkene diensthoofd vereist.[76]

Er zij op gewezen dat de wetgeving inzake inlichtingendiensten weliswaar een kader biedt voor het beginsel van dergelijke ingrijpende methoden, maar niet ingaat op de 'technieken' van uitvoering. Deze zogenaamde technische kwesties - onder meer met welke *hardware* en *software* de methoden worden toegepast - worden aan het oordeel van de diensten overgelaten, rekening houdend met de permanente evolutie van de technologieën.

Het huidige wettelijke kader staat dus de Belgische inlichtingendiensten toe dit soort *software* te gebruiken in de context van de toepassing van BIM's, mits de beginselen van wettigheid, evenredigheid en subsidiariteit strikt worden nageleefd. Er wordt strenge jurisdictionele controle uitgeoefend om ervoor te zorgen dat het gebruik van elke BIM voldoet aan de eisen van wettigheid, evenredigheid en subsidiariteit.

Bovendien staat bij de huidige stand van het recht niets in de weg dat de ADIV bij de uitoefening van zijn bevoegdheden krachtens artikel 44 W.I&V. *software* van het type Pegasus gebruikt. Dit artikel voorziet in de mogelijkheid voor de ADIV om elke vorm van communicatie uitgezonden of ontvangen in het buitenland op

---

75 Artikel 18/3 W.I&V voorziet in een dubbele controle bij de toepassing van deze bijzondere inlichtingenmethoden (BIM) op het niveau van wettigheid, subsidiariteit en evenredigheid: een controle *a priori* door de administratieve BIM-Commissie en een controle *a posteriori* door het Vast Comité I.

76 Art. 18/10 § 2 W.I&V.

te sporen, te onderscheppen, af te luisteren en er kennis van te nemen, alsook op te nemen. Het gebruik van dit soort procedures wordt ook gecontroleerd, maar op een andere manier dan de controle op de BIM's. Hier treedt immers alleen het Vast Comité I op en oefent een voorafgaande controle, een bijkomende controle en een controle *a posteriori* uit overeenkomstig artikel 44/3 W.I&V.

Het Comité wees er echter op dat de jurisdictionele controle geen betrekking heeft op de technische aspecten van de uitvoering van de bijzondere inlichtingenmethoden (bijvoorbeeld de vraag of een software van het type Pegasus wordt gebruikt bij de uitvoering van een BIM waarvoor machtiging is verleend) of artikel 44 W.I&V. Het Comité beschikt momenteel niet over voldoende personeel noch de technische deskundigheid om een dergelijke evaluatie uit te voeren. Dit gebrek aan middelen kan van invloed zijn op de beoordeling van het subsidiaire en evenredige karakter van de BIM of het in artikel 44 W.I&V bedoelde proces.

I.5.2. MAKEN DE BELGISCHE INLICHTINGENDIENSTEN GEBRUIK VAN *REMOTE INFECTION TECHNOLOGIES* IN HET KADER VAN HUN OPDRACHTEN?

Het Comité onderzocht tevens of de inlichtingendiensten gebruik maken of hebben gebruik gemaakt van Pegasus of gelijkaardige tools. De analyse van het Comité hierover kan niet worden opgenomen in een publiek rapport omwille van de classificatie van de informatie.

Wat betreft de noodzaak voor de Belgische inlichtingendiensten om over dit soort instrumenten te beschikken, concludeert het Vast Comité I dat, rekening houdend met de snelle en complexe evolutie van bedreigingen in een digitale omgeving die zichzelf steeds verder uitbreidt, het gebruik van de meest geavanceerde digitale technologieën essentieel lijkt om de missies van de Belgische inlichtingen- en veiligheidsdiensten zo doeltreffend mogelijk uit te voeren. Het is onweerlegbaar dat het gebruik van technologische inlichtingen- en beveiligingsinstrumenten zoals '*Remote Infection Technologies*' de informatiepositie van de diensten waarschijnlijk aanzienlijk zal versterken. Bovendien moet worden opgemerkt dat de afnemende doeltreffendheid van de meer traditionele maatregelen voor het onderscheppen van communicatie blijkt uit de toenemende complexiteit van het verzamelen en verwerken van informatie. Deze situatie frustreert in toenemende mate, zo niet verhindert, de inlichtingencyclus en zijn doelstellingen om te anticiperen op veiligheidsrisico's en de autoriteiten adequaat advies te geven over de aanpak van bedreigingen, of belemmert deze zelfs rechtstreeks. Echter is het belangrijk dat dit soort technologie met strikte inachtneming van het wettelijk kader wordt gebruikt.

Het Vast Comité I dringt er ook op aan dat deze technologieën idealiter in België worden ontwikkeld. Zoniet moeten de gebruikte technologieën worden ontwikkeld door strategische buitenlandse partners waarmee een veiligheidsovereenkomst is

gesloten en moeten zij worden aangeschaft na een geformaliseerde, grondige en gestandaardiseerde risicoanalyse.

Daarnaast meent het Comité dat de controle die bij het gebruik van dit soort *software* zal moeten worden uitgeoefend, 'grondiger' moet zijn vanwege de ernst van de inbreuk op de persoonlijke levenssfeer.

I.5.3. ZIJN DE VSSE EN DE ADIV BEVOEGD OM HET GEBRUIK VAN PEGASUS (OF SOORTELIJKE SOFTWARE) DOOR BUITENLANDSE DIENSTEN OP TE SPOREN?

Uit onthullingen in de pers is gebleken dat de rechten en de privacy van de Belgische burgers in gevaar kunnen komen door mogelijke spionage door buitenlandse inlichtingendiensten via technologieën van het type Pegasus. De opsporing en het beheer van dit soort bedreigingen liggen bij de VSSE en de ADIV.

Krachtens de artikelen 7 en 8 W.I&V heeft de VSSE immers als opdracht het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige en uitwendige veiligheid van de Staat zou kunnen bedreigen, alsook het wetenschappelijk of economisch potentieel van België, waaronder spionage. Bovendien geeft artikel 7, 3°/1 de VSSE de specifieke opdracht *"het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied*."

Artikel 11, § 1, 5° voorziet in dezelfde opdracht voor de ADIV. Krachtens artikel 11 §1, 1° W.I&V is de militaire inlichtingendienst ook belast met *"het onderzoeken, analyseren en verwerken van inlichtingen betreffende elke activiteit die (...) e) de veiligheid van de Belgische onderdanen in het buitenland (…) bedreigt of zou kunnen bedreigen*."

Het Vast Comité I heeft vastgesteld dat de inlichtingendiensten bepaalde initiatieven genomen hebben, zowel op het vlak van opsporing als op het vlak van preventie om infecties van toestellen te beperken.

In zijn publieke verslag kon het Vast Comité I daarover niet meer informatie geven, gezien het geclassificeerd karakter ervan.

I.5.4. HEBBEN DE BELGISCHE INLICHTINGENDIENSTEN DE CAPACITEITEN OM DE EVOLUTIES IN VERBAND MET *REMOTE INFECTION TECHNOLOGIES* TE VOLGEN?

Wat de controle op de ontwikkelingen op dit gebied betreft, was het Vast Comité I van oordeel dat de twee inlichtingendiensten meer aandacht moeten besteden aan de bedreigingen die de nieuwe technologische mogelijkheden kunnen inhouden op het gebied van gegevensvergaring en economische en politieke spionage, zelfs

indien deze risico's afkomstig zijn van landen waarmee zij strategische betrekkingen onderhouden. In dit verband moeten regelmatig risicoanalyses worden uitgevoerd, met meer aandacht voor de gevolgen van de aanwezigheid van talrijke internationale instellingen op het Belgische grondgebied.

I.5.5. WAT IS DE INFORMATIEPOSITIE VAN DE BELGISCHE INLICHTINGENDIENSTEN OVER DE MOGELIJKE BELGISCHE DOELWITTEN VAN PEGASUS (DOOR BUITENLANDSE INLICHTINGENDIENSTEN)?

Het Vast Comité I merkte op dat de ADIV bij het identificeren van mogelijke Belgische doelwitten van buitenlandse diensten in verband met het gebruik van Pegasus, zich alleen heeft gericht op de mogelijke betrokkenheid van de Rwandese inlichtingendiensten, en de VSSE op de Rwandese en Marokkaanse inlichtingendiensten.

Volgens open bronnen is een verband gelegd tussen de Saoedische en Emiratische inlichtingendiensten en het gebruik van Pegasus en het bespioneren van Westerse (met name Amerikaanse en Britse) mensenrechtenactivisten en journalisten. Tijdens de rapportage, werd echter geen enkel Belgisch doelwit in dit verband genoemd.

De overige door het Comité in zijn oorspronkelijke verslag gebruikte informatie over mogelijke Belgische doelwitten blijft geclassificeerd.

I.6. TOEZICHTONDERZOEK NAAR DE OPVOLGING DOOR DE INLICHTINGENDIENSTEN VAN FILOSOFISCHE ORGANISATIES MET POLITIEKE BEDOELINGEN DIE STRIJDIG ZIJN MET DE DEMOCRATISCHE ORDE

In juli 2021 verzocht de Voorzitster van de Kamer van volksvertegenwoordigers het Vast Comité I een toezichtonderzoek te openen naar de wijze waarop de inlichtingen- en veiligheidsdiensten aandacht besteden "*aan de activiteiten van religieuze sektarische bewegingen met een politieke agenda (andere salafistische bewegingen, Opus Dei, Civitas...)*".

Dit nieuwe toezichtonderzoek betrof het derde luik van een reeks onderzoeken op verzoek van de parlementaire Begeleidingscommissie. Eerder waren de wijze waarop de Veiligheid van de Staat de toenmalige regeringscommissaris Ihsane

Haouach had opgevolgd[77] en de opvolging van de Moslimbroedershap door de inlichtingendiensten[78] aan de orde.

Al snel bleek echter de noodzaak om het voorwerp van het onderzoek nader te bepalen en bij te sturen. In het bijzonder bleek het begrip '*sektarische beweging*' ongeschikt, daar de bewegingen die als voorbeeld werden genoemd in de vraag van de Commissie geen sekten als zodanig zijn.[79]

Het Comité wou zich dus niet beperken tot het bestuderen van de genoemde bewegingen, maar gaf er de voorkeur aan een toezichtonderzoek uit te voeren naar levensbeschouwelijke, confessionele en niet-confessionele organisaties, in de ruimste zin van het woord, met politieke doelstellingen die indruisen tegen de democratische orde. Om het onderwerp van het onderzoek te koppelen aan een concrete dreiging, en dus in het verlengde van de twee voorgaande luiken, stelde het Comité ten slotte voor te kijken naar de dreiging van (potentiële) inmenging, al dan niet geïnitieerd in het buitenland, die deze organisaties kunnen vormen.

Met instemming van de Kamervoorzitster werd de reikwijdte van het onderzoek geherdefinieerd naar het toezicht op levensbeschouwelijke organisaties met politieke doelstellingen en die in strijd zijn met de democratische orde. De vraag aangaande de capaciteiten en strategieën van de inlichtingen- en veiligheidsdiensten om dergelijke organisaties op te sporen en te controleren, bleek voor het Comité van bijzonder belang.

I.6.1. WETTELIJKE BEVOEGDHEDEN

De Wet houdende regeling van de inlichtingen- en veiligheidsdiensten (W.I&V) definieert in haar artikelen 7 en 8 de wettelijke opdrachten die zijn toegewezen aan de VSSE. Bij de dreigingen die de inlichtingendienst moet opvolgen, definieert artikel 8 de schadelijke sektarische organisaties ende criminele organisaties als volgt:

---

77 In dit onderzoek werd de aard van de opvolging door de VSSE onderzocht naar betrokkene die, al dan niet bewust, banden zou hebben met de Moslimbroederschap. In : VAST COMITÉ I, *Activiteitenrapport 2021*, 59 en volgende.

78 Deze enquête trachtte uit te maken of enerzijds de Moslimbroederschap het voorwerp van opvolging door de VSSE en de ADIV uitmaakte, en anderzijds, of de Moslimbroerschap volgens hen een bedreiging betekende voor België. In : VAST COMITÉ I, *Activiteitenrapport 2021*, 63 en volgende.

79 Het Comité had in een heel recent verleden al aandacht besteed aan de opvolging van de terroristische dreigingen die uitgaan van schadelijke sektarische organisaties en criminele organisaties: VAST COMITÉ I, *Activiteitenverslag 2021*, p. 35 en volgende.

– schadelijke sektarische organisatie:[80], [81] *"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";*
– criminele organisatie: *"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, dreiging, 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 artikel 8, 1°, a) tot e) en g), of die destabiliserende gevolgen kunnen hebben op het politieke of sociaal-economische vlak"*.

Opgemerkt moet worden dat niet alle schadelijke sektarische organisaties en niet alle criminele organisaties behoren tot de wettelijke interessesfeer van de VSSE. De W.I&V bepaalt dat die organisaties enkel onder de bevoegdheid van de VSSE vallen zo hun activiteiten een bedreiging kunnen vormen voor de inwendige of uitwendige veiligheid van de Staat en/of voor het economisch of wetenschappelijk potentieel van het land.

Wat betreft de ADIV, bepaalt artikel 11, §1, 1° W.I&V dat de dienst onder andere als opdrachten heeft inlichtingen in te winnen, te analyseren en te verwerken 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. De bevoegdheden van de ADIV ter zake zijn dus beperkt en impliceren dat er een verband is met Defensie of de militaire belangen.

Naast de W.I&V, is het belangrijk om artikel 9 van het Europees Verdrag van de Rechten van de Mens (EVRM) onder de aandacht te brengen, hetwelk de vrijheid van denken, bewustzijn en godsdienst garandeert; deze vrijheid wordt beschouwd als "*een van de grondslagen van de democratische samenleving. In het bijzonder zien de rechters in de vrijheid van godsdienst een vitaal element dat bijdraagt tot het*

---

80 Deze definitie is letterlijk overgenomen uit artikel 2 van de wet van 2 juni 1998 (*B.S.* 25 november 1998) houdende oprichting van een Informatie- en Adviescentrum inzake de schadelijke sektarische organisaties en van een Administratieve coördinatiecel inzake de strijd tegen schadelijke sektarische organisaties.

81 Het schadelijk karakter van een sektarische organisatie wordt onderzocht op basis van de principes welke zijn vastgelegd in de Grondwet, de wetten, de decreten, ordonnanties en in de internationale verdragen inzake de bescherming van de rechten van de mens welke door België werden geratificeerd. Al in 2021 stelde het Comité dat "*algemeen, geen enkele andere buitenlandse inlichtingendienst als officiële opdracht heeft om toezicht uit te oefenen op schadelijke sekten. Deze specifieke opdracht van de Belgische Veiligheid van de Staat vormt dus een uitzondering in de wereld van de inlichtingendiensten. De meeste democratische landen weigeren zelfs deze diensten te betrekken bij het toezicht op religieuze bewegingen. Deze maatregel wordt immers beschouwd als een inbreuk op de vrijheid van godsdienst*" (vrije vertaling). Zie VAST COMITÉ I, *Activiteitenverslag 2021*, 22.

vormen van de identiteit van de gelovigen en hun opvatting van het leven"[82] (vrije vertaling). Die vrijheid geniet strenge bescherming.[83]

I.6.2. OPVOLGING VAN DE PROBLEMATIEK DOOR DE VSSE EN DE ADIV

I.6.2.1. Wat betreft de VSSE

De VSSE bevestigt meteen dat de dienst "*(confessionele of niet-confessionele) organisaties met politieke bedoelingen die strijdig zijn met de democratische orde*" alleen in het strikte kader van een bedreiging opvolgt.

De VSSE verklaart echter dat, meer dan inmenging, de bedreigingen van extremisme en terrorisme in haar ogen doorslaggevender zijn bij de opvolging van ideologische of religieuze groepen die geacht worden problematisch te zijn. Volgens de VSSE zijn immers de belangrijkste bedreigingen die de opvolging van een dergelijke filosofische organisatie rechtvaardigen die van extremisme (artikel 8, lid 1, c) W.I&V) en terrorisme (artikel 8, lid 1, b) W.I&V).

Bij de VSSE zijn de verspreiding van gewelddadige extremistische discours en het risico van overgaan naar gewelddadige handelingen de twee hoofdcriteria die het opsporen oriënteren en de opvolging van een extremistische organisatie bepalen . Daarbij komen nog andere criteria zoals de aanwezigheid in België, het (bijvoorbeeld financiële) verband met een (buitenlandse) organisatie of een vreemde staat.

De VSSE organiseert haar werk rond het onderscheid tussen drie hoofdtypes van extremisme, i.e. religieus extremisme, ideologisch extremisme en exogeen extremisme.

Religieus extremisme

Op het ogenblik van het onderzoek, stelde de VSSE prioritair te werken rond extremistische islam. Hoewel die bewegingen marginaal zijn binnen de '*Belgische*

---

82 Divisie Onderzoek, Europees Hof voor de Rechten van de Mens, 'Aperçu de la jurisprudence de la Cour en matière de liberté de religion' (overzicht van de rechtspraak van het Hof inzake de vrijheid van godsdienst), oktober 2013, p. 27.

83 De instellingen van het Verdrag zijn niet bevoegd om godsdienst te definiëren, maar ze moet wel worden gezien in een niet-restrictieve betekenis. In verband met minderheidsgodsdiensten en religieuze groepen die op nationaal vlak soms als *sekten* worden gekwalificeerd, blijkt uit de rechtspraak van het Hof dat alle groepen een gelijke garantie genieten ten aanzien van het Verdrag. Het Hof, dat het recht op de vrijheid van godsdienst beschouwt als "pijler van een democratische samenleving", heeft de staten er voortdurend op gewezen dat zij een verplichting van neutraliteit en onpartijdigheid hebben in de uitoefening van hun regelgevende bevoegdheden ter zake alsook in hun relaties met de verschillende godsdiensten, erediensten en geloofsovertuigingen.

islam', is de VSSE van mening dat die groepen de meest directe bedreiging vormen inzake extremisme, gelet op het discours dat ze verspreiden en het publiek dat ze aantrekken.

De VSSE concentreert zich in het bijzonder op de opvolging van het salafisme. Volgens de VSSE blijft deze conservatieve en uiterst strenge beweging de meest dynamische en populairste beweging binnen het geheel van "*islamistische groeperingen*". Naast de opvolging van het salafisme op Belgisch grondgebied werkt de VSSE aan het terugdringen van de invloed die sommige Golfstaten uitoefenen op de ontwikkeling van het salafisme in België en in Europa, bijvoorbeeld via gewone financiële steun of zelfs de globale financiering van diverse groeperingen. Aldus volgt de VSSE ook aandachtig de beweging van de Moslimbroeders in haar Belgische en Europese geledingen.[84]

De VSSE verklaart momenteel niet te werken rond organisaties die verband houden met andere erediensten omdat, in dit stadium en volgens de evaluatie van de VSSE geen enkele andere organisatie die verbonden is met andere erediensten een voldoende belangrijke bedreiging vertegenwoordigt.

Ideologisch extremisme

Wat betreft het ideologisch extremisme, verklaarde de VSSE zich prioritair bezig te houden met personen en groeperingen van extreemrechts, geïnspireerd op het nazisme of het ultranationalisme.

Bovendien en in dezelfde geest, heeft de VSSE de voorbije jaren ook vastgesteld, net als andere Belgische of buitenlandse partners, dat er opnieuw een toename is van activisme dat gericht is tegen de islam en tegen immigratie en ook dat er op de Belgische grondgebied zogenaamde 'identitaire' groeperingen verschijnen.

Met betrekking tot extreemlinks, bestaat de bedreiging gevormd door individuen en groeperingen van deze extremistische beweging wel degelijk, maar is vandaag kleiner. In het kader van deze specifieke opvolging, focust de VSSE op gewelddadig extreemlinks dat vijandig staat tegenover de democratische en grondwettelijke orde. Volgens de VSSE komen drie hoofdtendensen naar voren, i.e. opstandig anarchisme, libertair activisme en revolutionair communisme. Daarbij wijst de VSSE er ook op dat extreemlinkse aanvallen veeleer gericht zijn op goederen of infrastructuren dan op specifieke personen.

Exogeen extremisme

Tot slot volgt de VSSE ook exogene extremistische personen en groepen die actief zijn vanaf België. Het gaat om buitenlandse extremistische bewegingen die soms als terroristisch worden beschouwd en waarvan de belangrijkste doelwitten en

[84] Zie VAST COMITE I, *Activiteitenverslag 2021*, 63-69 ('I.12. Een vernieuwde aandacht voor de Moslimbroederschap').

doelstellingen in hun land van oorsprong gesitueerd zijn. In dit kader zijn België in het algemeen en Brussel in het bijzonder zeer geschikte plaatsen voor intens '*gelobby*' of zelfs inmenging van die bewegingen, gelet op de aanwezigheid van vele Europese en internationale instellingen op het nationaal grondgebied. In dit verband voegt de VSSE nog toe dat het vaak ingewikkeld is om zich een beeld te vormen van de bedreiging van inmenging, daar het moeilijk is om het onderscheid te maken tussen inmenging en wettelijke activiteiten van beïnvloeding of gelobby.

1.6.2.2. Wat betreft de ADIV

Voor wat deze materie betreft, vereist de al dan niet bevoegdheid van de ADIV zich tot hethebben van een link met Defensie of de militaire belangen. In 2022 vermeldde de dienst geen filosofische organisaties op te volgen.

I.7. DE OPVOLGING VAN DE IN DE PARLEMENTAIRE ONDERZOEKSCOMMISSIE TERRORISTISCHE AANSLAGEN GEFORMULEERDE AANBEVELINGEN[85]

I.7.1. Contextualisering

I.7.1.1. Aanbevelingen van de parlementaire onderzoekscommissie terroristische aanslagen[86]

Op 22 maart 2016 werd België het doelwit van twee terroristische aanslagen, één op de nationale luchthaven van Zaventem, één in het Brusselse metrostation Maalbeek. Diezelfde dag nog werd de verantwoordelijkheid voor de aanslagen opgeëist door de terreurgroep Islamitische Staat.

Op 11 april 2016 dienden de grotere fracties van de Kamer een gemeenschappelijk voorstel in tot oprichting van een parlementaire onderzoekscommissie.[87] Het omstandige werk van de onderzoekscommissie viel uiteen in drie grote onderdelen: hulpverlening en slachtoffers, veiligheidsarchitectuur en radicalisme. Dat reflecteerde zich in vier tussentijdse verslagen met meer dan 400 eenparig aangenomen aanbevelingen. Deze aanbevelingen gingen zeer breed en overstegen vaak het loutere domein van terrorisme, extremisme en radicalisering.

---

85 Op 15 juni 2022 opende het Vast Comité I het onderzoek in hoofde van zijn bevoegdheid (het luik inlichtingen- en veiligheidsdiensten) en bracht daarvan de voorzitster van de Kamer, de bevoegde ministers alsook de diensthoofden van de VSSE en de ADIV op de hoogte. Het eindrapport werd op 4 oktober 2022 overgemaakt aan de Kamervoorzitster.

86 Geïnspireerd door Kamer van volksvertegenwoordigers, *Onderzoekscommissie terroristische aanslagen 22 maart 2016. Beknopt overzicht van de werkzaamheden en aanbevelingen*, 2018, 84 p.

87 *Parl. St.* Kamer, 2016-17, nr. 54-1752/001.

Het derde tussentijds verslag 'Veiligheidsarchitectuur'[88] was het lijvigste. Het formuleert vaststellingen en aanbevelingen over de werking, regelgeving en procedures van de verschillende veiligheidsdiensten (politie, justitie, inlichtingendiensten en andere). Wat de inlichtingendiensten betreft, werd onder meer aanbevolen de diensten meer armslag te geven, de informatiepositie te verbeteren, het Nationaal Strategisch Inlichtingenplan (NSIP) af te werken, of nog, een flexibel *human resources management* te voeren.

Veel van deze aanbevelingen zijn vrij algemeen geformuleerd. De precieze en concrete implementatie van de aanbevelingen werd schijnbaar overgelaten aan de bevoegde ministers en aan de hoofden van de respectieve diensten. Hier en daar werden wel concrete elementen van verbetering aangereikt, zoals bijv. de aanbeveling om een Kruispuntbank Veiligheid op te richten, en de suggestie van een co-locatie voor het OCAD en het Nationaal Crisiscentrum enerzijds en voor de VSSE en het ADIV anderzijds. Daarnaast werd heel wat aandacht besteed aan de problemen van, en voorstellen tot verbetering inzake de coördinatie tussen de verschillende diensten en de verschillende niveaus (zowel functionele niveaus – bestuurlijk *vs* gerechtelijk – als geografische niveaus – lokaal *vs* bovenlokaal). Hieruit kon worden geconcludeerd dat hier hét grote manco ligt van de veiligheidscultuur en -architectuur in ons land. De onderzoekscommissie deed opmerken dat er al heel wat werk werd verricht door de respectieve diensten, maar kwam tot de vaststelling dat dit gepaard ging met te weinig overleg, te weinig coördinatie, en te weinig aandacht voor complementariteit.

I.7.1.2. (Nog) een evaluatie?

Op het eind van haar werkzaamheden stelde de onderzoekscommissie vast dat de terroristische dreigingen voortdurend evolueren en dat voortdurende waakzaamheid dus geboden is. De onderzoekscommissie beval dan ook de oprichting aan van een opvolgingscommissie die de uitvoering van de aanbevelingen van de parlementaire onderzoekscommissie zou controleren. Er werd een opvolgingscommissie opgericht met betrekking tot de uitvoering van de aanbevelingen over het luik "Veiligheidsarchitectuur". Vervolgens werd deze taak toevertrouwd aan de bevoegde vaste commissies (Binnenlandse Zaken en Justitie). In maart 2021 stelden de ministers een gemeenschappelijke stand van zaken voor[89] en in 2022 werd eenzelfde oefening gemaakt. Ditmaal echter kwamen de respectieve commissies voor Binnenlandse Zaken en voor Justitie elk apart samen.[90] De documenten

88 *Parl. St.* Kamer, 2016-17, nr. 54-1752/008, 15 juni 2017.

89 Gemeenschappelijke vergadering van de commissie voor Justitie en de commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken, 19 maart 2021, CRIV 55 COM 418; Gemeenschappelijke vergadering van de commissie voor Justitie en de commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken, 23 maart 2021, CRIV 55 COM 422.

90 Commissie voor Binnenlandse Zaken, 25 mei 2022; Commissie voor Justitie, 3 juni 2022, CRIV 55 COM 806; Commissie voor Binnenlandse Zaken, 21 juni 2022, CRIV 55 COM 824.

die de ministers van Binnenlandse Zaken en Justitie[91] in 2022 hebben ingediend, schetsen de voortgang inzake de uitvoering van elke aanbeveling en geven voor de aanbevelingen waaraan nog geen uitvoering is gegeven aan of ze al dan niet zijn geprogrammeerd. Aldus stelde de minister van Justitie een lijst op met 50 aanbevelingen voor de VSSE, waarvan er 18 zouden zijn gefinaliseerd, 20 lopende zouden zijn, één zou zijn geprogrammeerd en elf niet zouden zijn geprogrammeerd.[92] Op te merken valt dat de commissie voor Landsverdediging in 2021 noch in 2022 bij deze oefening was betrokken. De voorzitter van de commissie voor Landsverdediging liet weten dat er door de commissie geen specifieke vergaderingen werden gewijd aan de opvolging van de aanbevelingen.[93]

In het 'overzichtsrapport' (infra) gaf de minister van Justitie ten slotte te kennen dat hij, *"om het overzicht te bewaren en de inspanningen beter op elkaar af te stemmen"* had voorgesteld om *"het Coördinatiecomité Inlichtingen en Veiligheid (CCIV) dat in de schoot van de Nationale Veiligheidsraad is opgericht, de opvolging verzekert. Het is dan aan het CCIV om een boordtabel beschikbaar te maken voor de NVR, het SCIV en desgevallend het parlement"*.[94]

Maar de parlementaire Begeleidingscommissie zag hierin ook een rol weggelegd voor het Vast Comité I en gaf een oriëntatie*: "De commissie zou het Vast Comité I de opdracht moeten geven om een bijkomend toezicht op de diensten uit te oefenen, waarbij het zich dient te focussen op de nog niet uitgevoerde aanbevelingen met betrekking tot gegevens- en inlichtingenuitwisseling"* (onze onderlijning).[95] En verder: *"De commissie verzoekt het Vast Comité I om haar […] een bijgewerkte lijst te verstrekken met betrekking tot de voortgang van de aanbevelingen inzake de inlichtingendiensten en in het bijzonder inzake de databanken en de uitwisseling van informatie, alsook een analyse van de stand van zaken met betrekking tot de inlichtingendiensten en de manieren om de werking van de diensten te verbeteren"* (onze onderlijning).[96,97]

---

91 Het door de minister van Justitie voorgelegde document is getiteld "Team Justitie, Overzichtsrapport. Stand van zaken d.d. 01/03/2022 Aanbevelingen Justitie – Parlementaire Onderzoekscommissie Aanslagen Brussel 22 maart 2016, 80 p.". Dit rapport werd op 18 maart 2022 overgemaakt aan de Kamer.

92 Voor het OCAD bevat de lijst acht aanbevelingen waarvan er vier zouden zijn gefinaliseerd en vier lopende zouden zijn.

93 Brief van Commissievoorzitter Peter BUYSROGGE aan het Vast Comité I d.d. 21 juni 2022. Wel werd in de rand vermeld dat de minister van Defensie en de Chef ADIV op 30 maart 2022 tijdens een besloten zitting het Stuurplan 2022 van de ADIV hebben voorgesteld.

94 Team Justitie, *Overzichtsrapport. Stand van zaken d.d. 01/03/2022 Aanbevelingen Justitie – Parlementaire Onderzoekscommissie Aanslagen Brussel 22 maart 2016*, s.d., 3.

95 *Parl. St.* Kamer, 2021-22, 55K2745/001, p. 10.

96 *Ibid.*, p. 16.

97 Hoewel heel wat aanbevelingen werden geformuleerd in het kader van de strijd tegen extremisme en terrorisme, bij prioriteit het domein van het Coördinatieorgaan voor de dreigingsanalyse (OCAD), werd het Comité hiertoe niet expliciet gemandateerd. De naleving van de aanbevelingen m.b.t. het OCAD kan eventueel het voorwerp uitmaken van een navolgend gemeenschappelijk toezichtonderzoek (Vast Comités I en P).

I.7.2. DE KRACHTLIJNEN IN DE AANBEVELINGEN

De onderzoekscommissie heeft een grondige analyse gemaakt van alle aspecten van de Belgische veiligheidsarchitectuur. De grote krachtlijnen in de aanbevelingen waren de volgende[98]:

- De verschillende overheids- en veiligheidsdiensten werkten nog te veel naast elkaar. Ze moeten samen een geoliede veiligheidsmachine worden waarin elk onderdeel een duidelijk gedefinieerde functie heeft;
- Relevante informatie moet vlot doorstromen van het ene beleidsniveau naar het andere, van de ene overheidsdienst naar de andere. Die vlotte informatiedoorstroming moet er ook zijn tussen de internationale tegenhangers van onze diensten en de Belgische diensten. Op die manier moeten de veiligheidsdiensten potentiële terroristen vroeg op het spoor komen, snel kunnen overleggen en flexibel prioriteiten kunnen afbakenen;
- Radicalisme en terrorisme moeten integraal worden aangepakt. Repressie en vervolging zijn uiteraard cruciaal, maar er moet ook voldoende aandacht gaan naar proactief optreden en preventie;
- Diverse veiligheidsorganen hebben meer middelen en meer mensen nodig. In bepaalde geledingen van de veiligheidsmachine zijn schaalvergroting en een verhoogde samenwerking aangewezen, want geografische en operationele versnippering zijn risicofactoren voor een goede werking;
- De Europese en internationale samenwerking moet worden opgedreven. België hoopt op een wijziging van de Europese verdragen, zodat een Europese inlichtingendienst mogelijk wordt. Ondertussen kan België de samenwerking met gelijkgestemde lidstaten intensifiëren in de Counter Terrorism Group van Europol;
- De wildgroei van (internationale en nationale) regels en procedures moet worden ingedamd, want die dreigt het gebrek aan samenhang in het beleid erger te maken;
- De overheid moet erop toezien dat de maatregelen tegen terrorisme en radicalisering de waarden waarop onze democratie is gebouwd, in geen geval uithollen.

De aanbevelingen specifiek gericht aan de Veiligheid van de Staat en de Algemene Dienst Inlichtingen en Veiligheid konden worden gebundeld in onderstaande clusters:

- De informatiepositie van de inlichtingendiensten;
- De samenwerkingsverbanden tussen de VSSE en de ADIV;
- De internationale dimensie van het inlichtingenwezen;
- Informatiebeheer en -doorstroming;

---

98 KAMER VAN VOLKSVERTEGENWOORDIGERS, *Onderzoekscommissie terroristische aanslagen, 22 maart 2016, Beknopt overzicht van de werkzaamheden en aanbevelingen*, 38-39.

– De Joint Intelligence en Joint Decision Centres;
– Het beheer van de *human resources*.

I.7.3. DE INVLOED VAN DE PARLEMENTAIRE COMMISSIE OP HET INLICHTINGENWERK

I.7.3.1. Globale evaluatie

Met een wetswijziging in 1996 wenste de wetgever de gevolgen van een parlementair onderzoek meer gewicht toe te kennen. Voortaan moest elke parlementaire onderzoekscommissie bij afsluiting van haar onderzoek een verslag maken van haar werkzaamheden.[99] Dit verslag dient een eindconclusie te bevatten en formuleert, in voorkomend geval, voorstellen over toekomstige wetgevende initiatieven. De wetgever wou met andere woorden te allen tijde vermijden dat de werkzaamheden van parlementaire onderzoekscommissies zonder gevolg zouden blijven. De activiteiten van een dergelijke parlementaire onderzoekscommissie situeren zich vóór het wetgevende werk (debatten, afwegen van alternatieven, suggereren van mogelijke oplossingen) of ná het wetgevende werk (controle op de uitvoering, naleving en bestraffing, suggereren van andere regels…).

Er kon worden vastgesteld dat door de parlementaire onderzoekscommissie terroristische aanslagen zeker werd voldaan aan art. 13 Wet op het parlementair onderzoek: onder meer wat de Belgische veiligheidsarchitectuur betreft, resulteerden de werkzaamheden van de commissie in een bijzonder lijvig verslag, voorzien van een omvangrijk aantal aanbevelingen. Bovendien werd – voor het eerst - een opvolgcommissie samengesteld die moest toezien op de naleving van de gemaakte aanbevelingen. De opvolging van de implementatie van de aanbevelingen werd *as such* ook aangekondigd in het Regeerakkoord.[100] De terroristische dreiging evolueert immers voortdurend waardoor permanente waakzaamheid geboden is.[101]

De aanbevelingen waren talrijk, bestemd voor alle geledingen (wetgevend, uitvoerende en rechterlijke macht) en oefen(d)en, nog steeds[102], een belangrijke invloed uit op de hervormingen (in de inlichtingensector). Het Comité kon evenwel vaststellen dat tal van aanbevelingen evenwel een herhaling vormden van eerdere

---

99 *"Art. 13. De commissie maakt van haar werkzaamheden een verslag, dat openbaar is. Zij vermeldt haar conclusies en, in voorkomend geval, opmerkingen over de verantwoordelijkheden die door het onderzoek aan het licht zijn gebracht, en voorstellen over een wijziging van wetgeving"*, Wet van 3 mei 1880 op het parlementair onderzoek, *B.S.* 5 mei 1880.

100 Federale Regering, *Regeerakkoord,* 30 september 2020, 74.

101 M. VAN DER HULST, *Onderzoekscommissie terroristische aanslagen 22 maart 2016, Beknopt overzicht van de werkzaamheden en aanbevelingen*, Kamer, 13.

102 Zo werd bijv. in de Memorie van Toelichting in de Wet van 14 juli 2022 tot aanpassing van de Inlichtingenwet in het kader van het toelaten van de plegen van strafbare feiten door menselijke bronnen verwezen naar de aanbevelingen van de parlementaire onderzoekscommissie. *Parl St.* Kamer 2021-2022, 55DOC2706/002.

vaststellingen en aanbevelingen. Heel wat hervormingen waren al vooropgesteld en een reeks geplande hervormingen kwam in een stroomversnelling terecht. Ook diende worden vastgesteld dat (minstens) een deel van de aanbevelingen niet of weinig SMART-geformuleerd, in herhaling viel of een verzuchting was die op korte of zelfs middellange termijn niet realiseerbaar was (bijv. de oprichting van de kruispuntbank). Niettemin werden heel wat aanbevelingen van de onderzoekscommissie ondertussen gerealiseerd: men kan dus terecht spreken van een katalysator-functie.

I.7.3.2. Voortgang van de realisatie van de aanbevelingen[103]

Wat betreft de VSSE

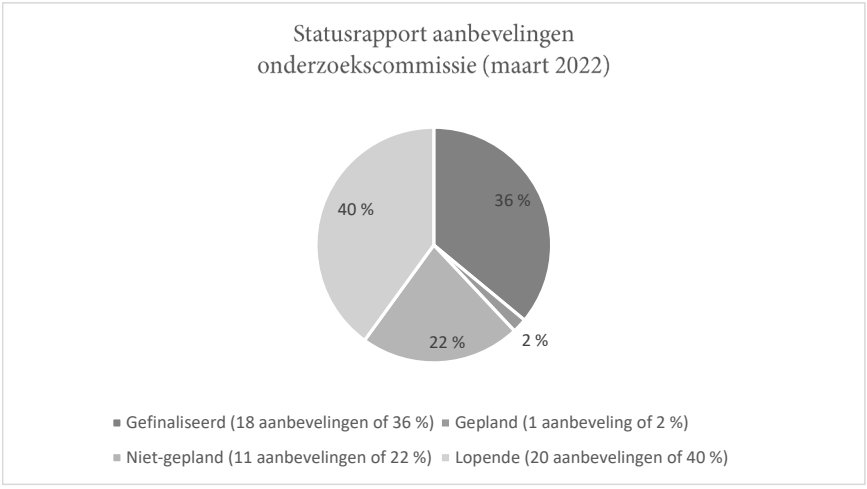
In 2020 en 2021 wisselden de ministers van Justitie en Binnenlandse Zaken in de gemengde commissie in de Kamer van gedachten over de stand van zaken van de aanbevelingen van de parlementaire onderzoekscommissie.[104] In juni 2022 werd de bespreking – op basis van een overzichtsrapport van de minister van Justitie[105] – in de Commissie Justitie herhaald.

[103] Er werd getracht de voortgang inzake de uitvoering van de aanbeveling te duiden, alsook deze van commentaren te voorzien en aandachtspunten voor de toekomst weer te geven. Voor een uitvoerige evaluatie van alle aanbevelingen, wordt verwezen naar het toezichtsrapport dat integraal werd hernomen op de website van het Vast Comité I (www.comiteri.be).

[104] De parlementsleden bleken niet tevreden met deze eerste evaluatiemomenten.

[105] TEAM JUSTITIE, *Overzichtsrapport. Stand van zaken d.d. 01/03/2022 Aanbevelingen Justitie*. 80 p.

Wat betreft het 'statusrapport' van de realisatie van de aanbevelingen (de minister weerhield een vijftigtal[106] aanbevelingen voor de VSSE), werd volgende stand van zaken meegegeven:



Volgens de minister zijn 36% van de aanbevelingen gefinaliseerd en zowat 40% lopende; eerder werd opgemerkt dat het gros op het totaal van de 'niet geplande' aanbevelingen, bij de VSSE zit.[107] Niet alle aanbevelingen werden uitgevoerd of staan ingepland.[108] Voor een aantal van deze vooralsnog niet uitgevoerde of niet geplande aanbevelingen, werd door de inlichtingendiensten een argumentatie aangehaald.

Deze evaluatie betreft een momentopname, met evolutief karakter: aanbevelingen die in maart nog stonden aangestipt als zijn 'lopende', werden ondertussen (enkele maanden later) gerealiseerd (bijv. het plegen van misdrijven door bronnen). Omwille van de onduidelijkheid van de aanbevelingen, werden ook tegenstrijdigheden opgemerkt: wat de politie betreft, was de aanbeveling met betrekking tot de JIC/JDC 'lopende', terwijl deze voor de VSSE aangestipt stond als 'gefinaliseerd'. 'Gefinaliseerd' in Brussel, maar nog lopende in andere hoven van Beroep; en 'gefinaliseerd' als zijnde operationeel, maar niet 'wettelijk verankerd', zoals voorgeschreven in de aanbeveling van de onderzoekscommissie. Of sommige aanbevelingen als zijn 'gerealiseerd' mogen worden beschouwd, hangt vaak af van

106 In zijn exposé weerhield de minister van Justitie in totaal 142 aanbevelingen (ook voor politie, OCAD…), waarvan er 69 werden aangegeven als zijnde 'gefinaliseerd'. 54 aanbevelingen zijn 'lopende'.

107 *Hand.* Kamer 2021-22, CRIV 55 COM 806, 3 juni 2022, 23.

108 Een parlementslid stelde zich de vraag *tot op welk punt een overheidsdienst het verstandig mag achten de aanbevelingen van het parlement uit te voeren* (*Hand.* Kamer 2021-22, CRIV 55 COM 806, 3 juni 2022, 26). De minister was van oordeel dat er soms sprake was van gewijzigde inzichten.

de invalshoek van waaruit wordt gekeken. Is de aanbeveling in verband met het opzetten van een netwerk van liaisonofficieren gerealiseerd als één of twee liaisonofficieren in functie zijn, of is het in deze beter te spreken van een 'nog lopende' aanbeveling? Het was ook niet steeds duidelijk wat met bepaalde aanbevelingen nu concreet werd bedoeld. Of zoals de minister van Justitie zelf stelde: '*als men aan vier experts vraagt naar de Kruispuntbank Veiligheid, dan krijgt men vijf verschillende antwoorden*'. Aan sommige aanbevelingen die werden aangestipt als 'niet gepland', werd dan weer een andere invulling gegeven. En sommige aanbevelingen blijken ook meermaals te worden herhaald, wat mogelijks een vertekening oplevert van de realiteit (en bij uitbreiding het taartdiagram). Ten slotte bleken sommige voor de hand liggende aanbevelingen (bv. '*datalekken bestrijden*') niet te zijn weerhouden door de VSSE.

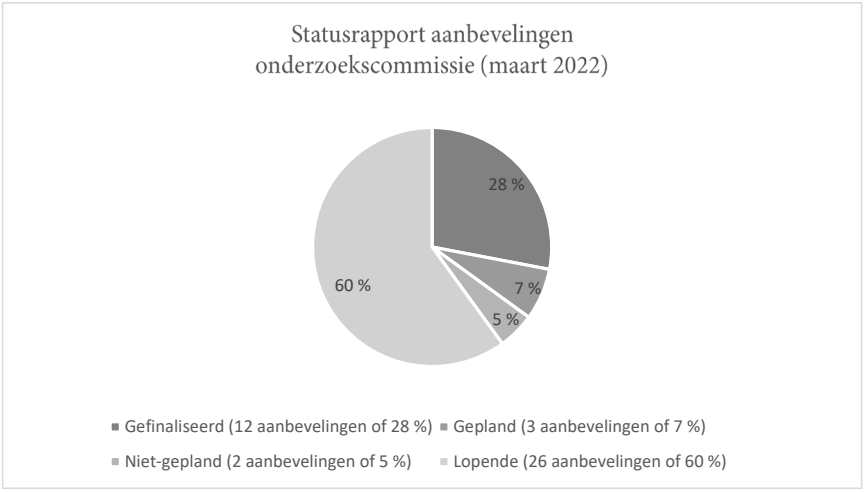
Niettegenstaande het Comité het niet noodzakelijk eens was met de hele evaluatie, kan het zich globaal genomen vinden in de door de VSSE geformuleerde antwoorden, waarmee het belang van (de aanbevelingen van) de parlementaire onderzoekscommissie wordt geduid. Dit werd door experten als volgt vertaald: "*Door zijn politiek gewicht is het verslag van de onderzoekscommissie van het grootste belang voor de diensten die zich erop moeten baseren. Maar terwijl sommigen vinden dat 'de onderzoekscommissie de zaken wat heeft versneld', wijzen de agenten er meer in het algemeen op dat zij niet op de commissie hebben gewacht om hun praktijken te reorganiseren en hun samenwerking te versterken*" [vrij vertaald].[109]

Wat betreft de ADIV

In tegenstelling tot de VSSE, en bij uitbreiding de minister van Justitie, werd door de ADIV eerder nog geen overzicht geboden van de door de parlementaire onderzoekscommissie geformuleerde aanbevelingen. Nochtans zijn heel wat van de aanbevelingen eveneens van groot belang voor de militaire inlichtingendienst.

[109] THOMAS C. (2021), *'Une menace possible et vraisemblable'. Dire et faire la sécurité : l'Organe de Coordination pour l'Analyse de la Menace et la structuration du champ antiterroriste belge*, Université Saint-Louis - Bruxelles, december 2021.

Gelijkaardig aan deze van de minister van Justitie, werd door het Comité een overzicht op gemaakt dat werd voorgelegd aan de ADIV. 43 aanbevelingen werden weerhouden. De status van de uitvoering van deze aanbevelingen werd als volgt geïnterpreteerd door de ADIV:



ADIV blijkt in vergelijking met de VSSE minder aanbevelingen als zijnde 'gefinaliseerd' te beschouwen (28%); veel meer (60%) blijken, vijf jaar na publicatie van het rapport, nog steeds 'lopende'. Slechts 5% kreeg de statut 'niet gepland', wat een opmerkelijk verschil is met de VSSE (22%).

Zoals gemeld, betreft dit statusrapport een momentopname, dewelke vervolgens werd gevisualiseerd. Afhankelijk van de parameters die worden gebruikt, kan een aanbeveling als zijnde 'gerealiseerd' dan wel als 'nog lopende' worden beschouwd, wat vervolgens snel een ander beeld zou geven. Dit betekent dat dergelijke taartdiagrammen met de nodige omzichtigheid moeten worden benaderd. Het geeft een indicatie, maar daar houdt het ook bij op.

I.7.3.3. (Prioritaire) aandachtspunten voor de toekomst

Naar luid van het Vast Comité I en op basis van bovenstaande vaststellingen, kan worden gesteld dat de balans van deze onderzoekscommissie (voor wat betreft *in casu* werd bestudeerd) overwegend positief is.[110]

Toch bleven er een aantal belangrijke aandachtspunten. Deze worden hieronder – niet exhaustief en niet in volgorde van belangrijkheid - hernomen:

– Het Vast Comité I wil een lans breken voor de, zoals de commissie tevens voorzag, wettelijke verankering van een aantal principes. Deze blijken nu te

[110] Ook anderen kwamen tot deze vaststelling, zie bijv.: A. KENTANE, *Invloed van parlementaire onderzoekscommissies op het strafrechtelijk beleid*, Universiteit Gent, 2020.

ontbreken (bijv. in het kader van primaire disruptie, de implementatie van de JIC/JDC, de verhouding tussen art. 29 Sv en 19/1 W.I&V), de modaliteiten voor de internationale samenwerking…. Gezien de mogelijke impact, acht het Comité het essentieel dat de noodzakelijke juridische waarborgen worden voorzien, waarbij niet alleen de toepassingsvoorwaarden worden geschetst, maar ook de vereiste controlemechanismen worden voorzien;
– Het Comité pleitte al langer voor het wegwerken van deficits en het versterken van de inlichtingendiensten. Uiteraard was dit niet exclusief gericht op een betere strijd tegen terrorisme en extremisme: de toekenning van de noodzakelijke (personele) middelen moet toelaten om alle in de Inlichtingenwet opgesomde taken naar behoren uit te voeren. Nu zowel de VSSE als de ADIV hun personeelsbestand uitgebreid zien, dient actief te worden ingezet op rekrutering en versneld gestreefd worden naar een uniek personeelsstatuut[111];
– De coördinatie en samenwerking tussen beide inlichtingendiensten moet blijvend verbeterd worden, meer bepaald door een gedeelde, planmatige aanpak van fenomenen, de rationele exploitatie van de middelen, een meer én betere, horizontale informatie-uitwisseling en doorstroming, versterkte samenwerking op vlak van OSINT, SOCMINT, HUMINT en SIGINT, zonder dat de diensten daarbij hun identiteit of specifieke kenmerken verliezen;
– Informatie- en communicatietechnologie (ICT) blijft een prioritair aandachtsdomein voor de inlichtingen- en veiligheidsdiensten waar de nodige personele en budgettaire middelen dienen tegenover te staan (hoogwaardige ICT-tools voor de diensten; open source ICT; de ontwikkeling van een beveiligd communicatienetwerk[112]; encryptie van informatie, de interconnectie van de gegevensbanken; …). Dit vergt meer tijd en middelen dan er thans binnen de diensten beschikbaar zijn. Het Comité beveelt aan hier met de hoogste prioriteit (verder) werk van te maken;
– De parlementaire onderzoekscommissie hield eveneens een pleidooi voor het 'rationaliseren, verduidelijken en actualiseren van de wet- en regelgeving'. Het Vast Comité I stelt vast dat de logica en het evenwicht in het kader van de inzet van bijzondere inlichtingenmethoden en de zgn. gewone methoden plus onder druk komt te staan. Door opeenvolgende wetswijzigingen is de interne logica zoek (bijv. de mate van intrusiviteit), zijn de controlemogelijkheden omzeggens voor elke methode verschillend geregeld… Een rationalisering dringt zich op;

---

111 In haar inleiding van het activiteitenrapport 2021-2022, bevestigde de Administrateur-generaal a.i. van de VSSE dat wordt gewerkt aan de invoering van een eengemaakt statuut (VSSE, *Intelligence Report 2021-2022*, 2023, *www.vsse.be*, p. 5).

112 Het Comité beveelt de grootste omzichtigheid aan bij de keuze van beveiligde technische uitrustingen voor de verwerking van gevoelige en geclassificeerde informatie. Technische uitrustingen moeten worden geëvalueerd, gecertificeerd en gehomologeerd – wat betreft hun betrouwbaarheid en veiligheid – volgens criteria en procedures die beantwoorden aan de normen van de Europese Unie.

– De diensten moeten blijvend inzetten wat betreft de internationale samenwerking (uitwisseling van informatie, in de aanstelling van liaisonofficieren…). Maar ook een en duidelijk wettelijk kader voor de uitwisseling van informatie en persoonsgegevens met het buitenland drong zich op.

Ten slotte wou het Comité de aandacht vestigen op een aantal andere punten:
– Het Vast Comité I beveelt een breder maatschappelijk (parlementair) debat aan over het in de Inlichtingenwet van 1998 voorziene takenpakket van de twee inlichtingendiensten en de hieraan gekoppelde prioriteitenstelling. Dit vergt een 'strategisch' onderbouwde discussie over de beschikbaarstelling van voldoende capaciteiten en middelen om elk dienst in staat te stellen alle bedreigingen van de (inter)nationale veiligheid naar behoren op te sporen, te bewaken en te beheersen. De inlichtingen- en veiligheidsdiensten moeten het voorwerp van parlementaire aandacht uitmaken, en dit niet alleen op het moment dat er zich individuele problemen voordoen (steekvlampolitiek);
– Essentieel bij het uitbreiden van de bevoegdheden, de materiële en personele middelen van de inlichtingen- en veiligheidsdiensten, is dat dit met voldoende aandacht voor de principes van de rechtsstaat gebeurt. Er moet aan de nodige *checks and balances* worden voldaan. Tegenover deze uitbreiding, moet ook worden voorzien in een uitbreiding van de effectieven van de toezichtsorganen. Zoniet dreigt de democratische controle te verworden tot een vorm van *window dressing*.[113] Hoewel kan worden vastgesteld dat de afgelopen jaren het takenpakket en de bevoegdheden van het Vast Comité I aanzienlijk werd uitgebreid, doch blijft het budget en de personeelsuitbreiding achterwege;
– Het Vast Comité I wil bij uitbreiding ook de aandacht vestigen op het gegeven dat het jaarlijks ten behoeve van de wetgever en de uitvoerende macht eveneens aanbevelingen doet die in het bijzonder betrekking hebben op de rechtmatigheid, de coördinatie en de doelmatigheid van het optreden van de twee Belgische inlichtingendiensten (en het OCAD). Deze aanbevelingen vloeien voort uit de diverse toezichtonderzoeken en adviezen. Deze werden, ten behoeve van de parlementaire Begeleidingscommissie gebundeld in een overzicht (1994-2005)[114], (2006-2016)[115] en recent een actualisering tot 2021. Een (omvangrijk) aantal van deze aanbevelingen werden ondertussen gerealiseerd, sommige aanbevelingen overlappen met deze van de onderzoekscommissie, en nog anderen dienen nog ter uitvoering worden gebracht. Het Vast Comité I suggereert de Begeleidingscommissie de lezing van beide werkzaamheden samen aan te vatten;

---

113 Het ligt in de bedoeling het aantal personeelsleden van de VSSE van ca. 600 te laten evolueren naar 1000; ook de ADIV werkt aan een personeelsuitbreiding (naar 1200). Het aantal personeelsleden ingezet voor het democratisch toezicht op de werking van de inlichtingen- en veiligheidsdiensten, dient navenant te evolueren. Zoniet dreigt een democratisch deficit.

114 VAST COMITÉ I, *Activiteitenverslag 2006*, 1-21.

115 VAST COMITÉ I, *Activiteitenverslag 2017*, 128-152.

– Een gelijkaardige evaluatieoefening voor wat betreft de door de onderzoekscommissie gedane aanbevelingen met betrekking tot het Coördinatieorgaan voor de dreigingsanalyse (OCAD), dringt zich op. Dit moet evenwel het voorwerp uitmaken van een gemeenschappelijk toezichtonderzoek met het Vast Comité P.

I.8. POGINGEN TOT RUSSISICHE INMENGING IN HET BELGISCHE POLITIEKE LEVEN

Midden-september 2022 werd een gedeclassificeerd uittreksel uit een verslag van de Amerikaanse inlichtingendiensten gepubliceerd dat heel wat aandacht zou krijgen in de internationale pers. Daarin was sprake van (pogingen tot) Russische inmenging in het politieke leven van verschillende landen over heel de wereld.[116] Volgens dit verslag "*Russia has covertly transferred over $300 million, and planned to covertly transfer at least hundreds of million more, to foreign politicial parties, officials, and politicians in more than two dozen countries and across four continents since 2014*".[117] Het doel van het Kremlin zou erin bestaan democratieën te verzwakken en politieke bewegingen te versterken die worden geacht 'op één lijn te staan' met de Russische belangen.[118]

Hoewel er in het verslag wordt dus niet expliciet verwezen naar enig land, werd er in persartikels verwezen naar anonieme commentaren van hooggeplaatste Amerikanen die wat betreft Brussel verklaarden: "*the Kremlin had used Brussels as a hub for foundations and other fronts that back far-right candidates. Fictitious companies were said to be used to fund European parties and to buy influence elsewhere*". [119]

Naar aanleiding van deze onthullingen stuurde de Kamervoorzitter begin december 2022 een brief aan het Vast Comité I met het verzoek '*na te gaan hoe de diensten op deze informatie hebben gereageerd en haar binnen een maand een*

116 Meer bepaald: "*Russia Secretly Gave $300 Million to Political Parties and Officials Worldwide, U.S. Says*", The New York Times, 13 september 2022; "*Russia has spent $300m since 2014 to influence foreign officials, US says*", The Guardian, 13 september 2022; "*Russia spent $300 million secretly interfering in foreign politics, U.S. says*", NBC News, 14 september 2022.

117 Het Vast Comité I heeft een kopie het uittreksel uit dat Amerikaanse verslag ontvangen van het kabinet van de minister van Buitenlandse Zaken. Het uittreksel telt drie pagina's en geen enkel land, geen enkele politieke figuur of geen enkele politieke partij wordt bij naam genoemd. Bovendien gaan de inlichtingendiensten ervan uit dat er veel hogere bedragen zijn doorgegeven en dat meer landen betrokken zijn, zonder in dit opzicht echter over bewijselementen te beschikken.

118 Uit het verslag blijkt ook nog dat de Russische betalingen gewoonlijk worden verricht door leden van de inlichtingendiensten maar ook door Russische oligarchen. Er worden verschillende soorten betaalmiddelen gebruikt (cash geld, cryptomunten, ...). De financiële verrichtingen verlopen via tussenpersonen (*think tanks*, stichtingen, criminele groepen, ...) en de middelen van de Russische ambassades worden vaak aangewend ter ondersteuning van deze handelwijzen.

119 "*Russia covertly spent $300m to meddle abroad – US*", BBC news, 14 september 2022; "*Comment la Russie a pesé sur des élections étrangères à coups de millions de dollars*", L'Express, 14 september 2022.

gedetailleerde nota te doen toekomen over de informatiepositie van de diensten over deze wijze van inmenging' (vrije vertaling).

I.8.1. EEN GEKENDE PROBLEMATIEK

De in het Amerikaans rapport beschreven problematiek van Russische inmenging is niet nieuw en krijgt sinds vele jaren heel wat aandacht. Sinds de Amerikaanse presidentsverkiezingen van 2016 waar inmenging door Rusland werd vastgesteld door de Amerikaanse inlichtingendiensten (meer bepaald door de selectieve verspreiding van informatie, propaganda-acties en pogingen om stemapparatuur te *hacken*)[120] is de Russische inmenging in verkiezingsprocessen een reden voor ongerustheid in vele Europese landen en meerdere verkiezingen blijken overigens te zijn beïnvloed door het Kremlin.[121]

In België vormde de bedreiging van inmenging in de Europese, federale en gewestelijke verkiezingen van mei 2019 een prioritair aandachtspunt voor de VSSE. Ook de ADIV stelt belang in deze problematiek en boog zich over "*het fenomeen van cyberinmenging in verkiezingen*".[122] In een eerdere toezichtonderzoek kon het Vast Comité I vaststellen dat "*de twee inlichtingendiensten de nodige stappen hadden ondernomen om mogelijke bedreigingen ten aanzien van de Belgische en Europese verkiezingen van mei 2019 tegen te gaan. De diensten hadden tijdig de problematiek herkend en opgenomen; de risico's en bedreigingen onderzocht en in kaart gebracht; zich naar behoren georganiseerd; de nodige samenwerking met elkaar en met andere actoren tot stand gebracht; de Regering en andere stakeholders gesensibiliseerd en regelmatig op de hoogte gehouden, zodat zo nodig maatregelen hadden kunnen worden genomen.*"[123] Op het einde van de verrichtingen hadden de diensten geen

---

120 SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE, Report "*Russian Active campaigns and interference in the 2016 U.S. Election*", july 2020 : Publications | Intelligence Committee; NAVO, "*L'ingérence de la Russie dans les élections des pays de l'Alliance*", Rapport van de Commissie voor wetenschap en technologie (Algemeen rapporteur: Susan Davis), november 2018, Rapport général STC 2018 (nato-pa.int).

121 Zie bijvoorbeeld : Intelligence and Security Committee of Parliament; Report "*Russia*", 21 July 2020, *HC 632 – Intelligence and Security Committee of Parliament - Russia (independent.gov.uk)*; "*Russia report reveals UK governement failed to investigate Kremlin interference*", The Guardian, 21 juli 2020; NAVO, '*L'ingérence de la Russie dans les élections des pays de l'Alliance*", Rapport van de Commissie voor wetenschap en technologie (Algemeen rapporteur: Susan Davis), november 2018, Rapport général STC 2018 (nato-pa.int), p.9; "*Nederlandse geheime dienst: Russen beïnvloeden verkiezingen met nepnieuws*", De Morgen, 4 april 2017; "*Ingérence russe : enquête en Allemagne sur les liens avec l'extrême droite*", Le Figaro, 14 februari 2019; "*Européennes : Berlin « attentif » face au risque d'ingérence russe*", Le Point, 13 mei 2019.

122 VAST COMITE I, *Activiteitenverslag 2020*, pp.27-28. Wat betreft de bevoegdheid van de ADIV ter zake verklaarde het Comité: "*De bevoegdheid van de ADIV leek op het eerste zicht ter zake minder evident dan deze van de VSSE. De ADIV is immers in de eerste plaats een militaire inlichtingendienst die zich op militaire materies moet richten. Toch boog de ADIV zich over het fenomeen van cyberinmenging in verkiezingen, nu (sic) clandestiene beïnvloeding van politieke processen veelal een militaire oorsprong kent.*"

123 VAST COMITE I, *Activiteitenverslag 2020*, pp.27-28.

sporen van grootschalige activiteiten van inmenging aangetroffen ter gelegenheid van deze verkiezingen in België.[124]

In zijn nota verwees het Permanent Comité I naar verschillende initiatieven die rechtstreeks verband houden met deze kwestie, bijvoorbeeld de speciale commissie van het Europees Parlement inzake buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie[125] of binnen het Belgische parlement.[126]

I.8.2. DE OPVOLGING DOOR DE BELGISCHE INLICHTINGENDIENSTEN

Op basis van de antwoorden van de diensten in december 2022 concludeerde het Vast Comité I dat het politieke leven in België - lees Belgisch, maar ook Europees - een potentieel doelwit is van Russische inmengingspogingen. De Belgische inlichtingendiensten zijn zich bewust van deze dreiging en volgen deze vanuit verschillende invalshoeken, rekening houdend met hun respectieve bevoegdheden.

I.8.2.1. Een sterke informatiepositie volgens de VSSE

De VSSE voert onderzoek naar inmenging volgens haar wettelijke opdrachten wat betreft het beschermen van de inwendige en de uitwendige veiligheid van de

---

124 VSSE, Jaarverslag 2019, 22; VAST COMITE I, *Activiteitenverslag 2020*, 27-28.

125 Zie Europees Parlement, Resolutie van 10 oktober 2019 over buitenlandse inmenging in verkiezingen en desinformatie in de nationale en Europese democratische processen (2019/2810(RSP)); Europees Parlement, Resolutie van 9 maart 2022 over buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (2020/2268(INI)); Besluit van 10 maart 2022 over de instelling, bevoegdheden, aantal leden en ambtstermijn van een Bijzondere Commissie buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (INGE 2) (2022/2585 (RSO)).

126 Zie in het bijzonder: Belgische Senaat, Verzoek tot het opstellen van een informatieverslag ter bestrijding van de inmenging door buitenlandse mogendheden met het oog op het ondermijnen van de democratische rechtsstaat, zitting 2021-2022, 22 april 2022, *7-344-1.indd (senaat.be)*; Kamer van Volksvertegenwoordigers, Wetsvoorstel tot wijziging, teneinde de buitenlandse financiering van politieke partijen te verbieden, van de wet van 4 juli 1989 betreffende de beperking en de controle van de verkiezingsuitgaven voor de verkiezingen van de Kamer van volksvertegenwoordigers, de financiering en de open boekhouding van de politieke partijen, DOC 55 2905/001, 27 september 2022; Wetsvoorstel tot wijziging van de wet van 4 juli 1989 betreffende de beperking en de controle van de verkiezingsuitgaven voor de verkiezingen van de Kamer van volksvertegenwoordigers, de financiering en de open boekhouding van de politieke partijen teneinde giften door niet-Belgen en sponsoring door ondernemingen, feitelijke verenigingen en rechtspersonen die hun maatschappelijke zetel niet in België hebben, te verbieden, DOC 55 2997/001, 10 november 2022; Voorstel van resolutie betreffende het efficiënt en effectief bestrijden van de buitenlandse beïnvloeding en de ondermijning van onze democratie, DOC 55 3045/001, 30 november 2022.

staat.[127] De dienst stelt dat reeds lang wordt vastgesteld dat Rusland Belgische politieke middens net zoals de publieke opinie en bepaalde media viseert. Wat betreft de uitwendige veiligheid van de staat, volgt de VSSE ook Russische inmenging m.b.t. internationale organisaties die hun hoofdkwartieren in België hebben – in het bijzonder de Europese Unie en NAVO. De VSSE verklaarde dan ook dat de mogelijke impact van Russische inmenging op de Belgische buitenlandse relaties ook een onderdeel van haar onderzoeken vormt.

Volgens de VSSE valt Russische inmenging moeilijk te kwantificeren. Toch verwijst de dienst naar een waarschijnlijke tendens tot intensifiëring van de Russische inmenging afgelopen jaren, tot aan de oorlog in Oekraïne. De VSSE vult verder aan dat *'individuen die voordien geen probleem zagen in banden met Rusland voor het overgrote deel niet langer met Rusland wensen geassocieerd te worden'*.

De VSSE kwalificeert de Russische strategie op dat vlak als zijnde hybride, en dat op twee vlakken. Eerst zijn de Russische inlichtingendiensten niet de enige Russische actoren die aan inmenging doen, maar ook andere organisaties en individuen die op eigen initiatief handelen om zo dichter bij Russisch president Poetin te komen. Daarna gebeurt, volgens de VSSE, Russische inmenging op verschillende manieren, via agenten (het gebruiken van personen om Russische boodschappen te verspreiden …), cyberoperaties (vb. de gekende *troll farms*) en media (desinformatie in Russische staatsmedia, …).

De dienst bekwam een sterke informatiepositie betreffende Russische inmenging omwille van de mensen en middelen ingezet in de opvolging van deze dreiging. De VSSE heeft het Vast Comité I meegedeeld dat sinds 2017 meer dan 100 BIM's naar aanleiding van deze thematiek gelanceerd werden.

Op basis hiervan vermeldt de VSSE over geen concrete elementen te beschikken die aantonen dat Belgische politieke partijen op een structurele wijze gefinancierd worden door buitenlandse mogendheden (Rusland dan wel andere mogendheden). De dienst herinnert er ook aan dat het onderzoek dat in samenwerking met de ADIV werd uitgevoerd naar de mogelijke Russische inmenging in de Belgische verkiezingen van 2019, geen significante inmenging heeft aangetoond.

De VSSE stelt ook dat de dienst in deze kwestie nauw samenwerkt met de ADIV. Tijdens (twee)maandelijkse ontmoetingen wisselen beide diensten inlichtingen en inschattingen uit. Volgens de VSSE zorgt de taakverdeling tussen het opvolgen van de militaire dienst GRU (ADIV) en burgerlijke dienst SVR (VSSE) over het algemeen voor een vlotte samenwerking, maar het onderscheid tussen beiden is niet steeds eenvoudig te maken, vandaar dat er ook geregeld overleg plaatsvindt betreffende concrete dossiers.

---

127 Volgens de VSSE komt het beschermen van de wetenschappelijke en economische potentieel (WEP) minder voor in de onderzoeken naar inmenging (art. 7 W.I&V).

I.8.2.2. Een opvolging door de ADIV aangestuurd door de militaire belangen

Hoewel de ADIV nauwlettend de spionage- en inmengingsdreigingen vanuit Rusland opvolgt, wordt dit enkel bestudeerd vanuit het oogmerk van de Belgische militaire belangen en Belgische belangen in het buitenland. Daarom verduidelijkt de ADIV dat het opvolgen van geldstromen vanuit Rusland naar Belgische politieke partijen niet zijn eerste prioriteit is.

De ADIV bevestigt dat inmenging een van de middelen is die Rusland gebruikt om zijn doelstellingen te verwezenlijken en heeft het meer in het bijzonder over de Russische methoden van desinformatie en manipulatie van de informatie.

Wat betreft de doelwitten van dergelijke inmenging, deelt de ADIV mee dat ze beschikken over indicaties die erop wijzen dat de Russische inlichtingendiensten speciaal aandacht geven aan extremistische partijen waarvan zij inschatten dat zij op termijn een politieke koers kunnen afdwingen die gunstiger is voor Rusland. Met name partijen en individuen die de internationale liberale orde, die zich sinds de Tweede Wereldoorlog voltrekt, in vraag stellen, zijn ideologische bondgenoten van de Russische inlichtingendiensten. Anti-atlantisme en een afkeer van migratie zijn kenmerken van deze doelwitten.

I.8.2.3. Conclusies

Het Comité concludeerde dat de dreiging van inmenging verder gaat dan de kwestie van de Russische financiering van politieke actoren en beval aan een toezichtonderzoek in te stellen om na te gaan of de Belgische inlichtingendiensten over voldoende (wettelijke en operationele) middelen beschikken om de dreiging van inmenging door buitenlandse mogendheden via de financiering van politieke partijen, politieke instellingen of politieke figuren in België op te sporen.

I.9. JURIDISCHE ANALYSE INZAKE DE BEWAPENING EN DE UITRUSTING VAN DE AGENTEN BEHORENDE TOT HET INCIDENT RESPONSE TEAM (VSSE)[128]

Sinds de inwerkingtreding van de Wet van 30 maart 2017[129] bepaalt de Inlichtingenwet[130] dat er binnen elke inlichtingendienst – dus zowel binnen de Veiligheid

[128] Zie B. VERSCHAEVE, "Het incident response team van de staatsveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht", *Politie & Recht*, 2022, n°1, pp. 3-20.

[129] Wet van 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek (*BS* 28 april 2017; hierna: BIM-actualisatiewet).

[130] Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (*BS* 18 december 1998; hierna: Inlichtingenwet of W.I&V).

van de Staat (VSSE) als binnen de Algemene Dienst Inlichting en Veiligheid bij de Krijgsmacht (ADIV) – een interventieteam kan worden opgericht met als opdracht de bescherming van het personeel, de infrastructuur en de goederen van de betrokken dienst. Binnen de VSSE werd een dergelijk interventieteam daadwerkelijk opgericht, genaamd het *Incident Response Team* (IRT). Binnen de ADIV werd vooralsnog geen interventieteam ingesteld.

Het binnen de VSSE opgerichte interventieteam zag reeds eerder, in mei 2015, het levenslicht. De oprichting vormde een antwoord van de VSSE op het gevaar en de toenemende onveiligheid waarin de inlichtingendienst reeds enige tijd opereerde. Via de oprichting van het interventieteam – initieel het *Intervention Response Team* genoemd, kortweg het IRT – werd binnen de VSSE een permanente beveiligingscapaciteit in het leven geroepen om de activiteiten van het personeel met meer veiligheidsgaranties te omkaderen. In september 2016 diende de regering een wetsontwerp in tot wijziging van de Inlichtingenwet om, onder andere, het IRT op te waarderen. Het doel was om het team een wettelijk statuut en opdracht te verschaffen. Ook bevatte het ontwerp een arsenaal aan politioneel-bestuurlijke dwangbevoegdheden voor het IRT en creëerde het een bijzonder stelsel van burgerlijke aansprakelijkheid en rechtshulp voor de leden van het IRT. Dit geheel was noodzakelijk voor de uitbouw van het IRT tot een gedegen en volwassen beveiligingsdienst, een behoefte die zich veruitwendigde na de terroristische aanslagen in Parijs (13 november 2015) en Brussel (22 maart 2016). Als onderdeel van de BIM-Actualisatiewet van 30 maart 2017 werd de opwaardering en verdere uitbouw van het IRT een feit. In juni 2017 werd de naam gewijzigd in het *Incident Response Team* (eveneens afgekort als het IRT).[131]

Begin oktober 2022 startte het Vast Comité I een juridische analyse inzake de bewapening en uitrusting van dit *Incident Response Team*. Het onderzoek werd evenwel zonder voorwerp. Het ministerieel besluit van 6 mei 2003 *'tot bepaling van de wapens en munitie die behoren tot de voorgeschreven uitrusting van de agenten van de buitendiensten van de Veiligheid van de Staat'* werd opgeheven en de minister van Justitie creëerde een algemeen juridisch kader voor het bezit en de dracht van wapens door de agenten van de VSSE. Het ministerieel besluit van 16 juni 2022 *'tot bepaling van de voorgeschreven uitrusting van de agenten van de Veiligheid van de Staat en tot vaststelling van bijzondere bepalingen betreffende het voorhanden hebben, het dragen en het bewaren van de bewapening*'[132] biedt de agenten van de VSSE de mogelijkheid om voor de uitvoering van hun opdrachten een wapen te dragen. De tekst laat ook de dracht van bijkomende wapens toe door de leden van het interventieteam. Het MB trad in werking op 29 oktober 2022.

131 Net zoals de oorspronkelijke benaming van het IRT, hanteert de Inlichtingenwet (artt. 22 tot 35 W.I&V, ingevoegd door artt. 52 tot 69 BIM-actualisatiewet) de begrippen 'interventieteam' en 'leden van het interventieteam'.

132 *BS* 19 oktober 2022.

I.10. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2022 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2022 WERDEN OPGESTART

I.10.1. DE TOEPASSING VAN NIEUWE (BIJZONDERE) INLICHTINGENMETHODEN

Het Comité kreeg een aantal controlemogelijkheden bij voor wat betreft sommige 'gewone' methoden. Het betreft onder meer het toezicht op de identificatie van de gebruiker van telecommunicatie (art. 16/2 W.I&V), de toegang tot passagiersgegevens (Passenger Name Record) (art. 16/3 W.I&V), de toegang tot politionele camerabeelden (art. 16/4 W.I&V), of nog, de controle voorafgaand aan intercepties, intrusies in een informaticasysteem en de opname van bewegende beelden (art. 44/3 W.I&V). Het Comité besliste om deze thematiek te bestuderen in zijn in 2019 geopende '*toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten de recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld*'.

In 2020 kwam het accent te liggen op de ontwikkeling van een methodologie in het kader van de controle op de identificatie van het gebruik van telecommunicatie (art. 16/2 W.I&V) alsook de toegang tot PNR-gegevens (art. 16/3 W.I&V). Begin 2021 werd het methodologische luik aangaande de controle voorafgaand aan intercepties, intrusies in een informaticasysteem en de opname van bewegende beelden (art. 44/3 W.I&V) gefinaliseerd. In 2021 boog het Comité zich over de operationalisering van artikel 16/4, §2 W.I&V. Dit artikel regelt de retroactieve opvraging van politionele camerabeelden door de inlichtingendiensten. De wetsbepaling kent een algemene werking. Dit zorgt ervoor dat de erin gestelde procedurele vereisten zowel van toepassing zijn op de gerichte opvragingen van politionele camerabeelden via een rechtstreekse (*online*) toegang tot de betrokken politionele gegevensbanken alsook op de gerichte opvragingen via een schriftelijke bevraging van de bevoegde politiedienst (i.c. de Directie van de politionele informatie en de ICT-middelen bij de Federale Politie (DRI)).[133] Omwille van een DPA-klacht werd het onderzoek opgeschort. De klacht vormde de aanleiding tot de '*Verwerkingsinstructie van het Vast Comité I (DPA) m.b.t. de door de inlichtingendiensten ingestelde retroactieve opvragingen van politionele camerabeelden gegrond op artikel 16/4, §2 W.I&V*'.

[133] Koninklijk besluit tot wijziging van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, *B.S.*, 4 november 2019.

In 2022 ontving het Comité de statistieken van de twee inlichtingendiensten met betrekking tot de inzet van deze methode en sloot het juridische luik af van zijn analyse. Het toezichtrapport kon evenwel, omwille van andere prioritaire dossiers, niet worden afgerond. Dit wordt voorzien in de loop van 2023.

I.10.2. HET RISICO OP INFILTRATIE BIJ DE TWEE INLICHTINGENDIENSTEN

Afgelopen jaren werd de internationale inlichtingenwereld opgeschrikt door een aantal *cases* van infiltratie (en *insider threat*). Het Comité nam het initiatief een toezichtonderzoek op te starten naar de wijze waarop de twee inlichtingendiensten met het risico op infiltratie omgaan: welke risico's worden onderkend, welke tegenmaatregelen worden genomen om ze te beheersen en om er op te reageren indien ze zich voordoen?

Er vonden diverse werkvergaderingen met de ADIV en de VSSE plaats over de thematiek 'cartografie en risico-evaluatie van infiltratie in de schoot van de inlichtingendiensten'. Het proces van risicomanagement zoals hernomen in de ISO 31000-norm vormde daarbij de vertrekbasis.[134]

Na een onderbreking in 2021 wegens andere prioritaire dossiers en de gevolgen van de sanitaire crisis, werden de onderzoekstaken in 2022 hervat. De reeds verzamelde informatie werd verwerkt en er werd aanvullende informatie gevraagd aan de diensten. De verwerking van hun antwoorden en het eindverslag zullen in de loop van 2023 worden afgerond.

I.10.3. CONTROLE OP DE SPECIALE FONDSEN: OPVOLGONDERZOEK

Zoals elke overheidsdienst, krijgen ook de inlichtingendiensten overheidsgeld toegekend voor de uitoefening van hun wettelijke opdrachten. De regel bij de besteding van die gelden is dat er volledige transparantie en controle moet zijn. Maar aangezien bepaalde taken van de VSSE en de ADIV onvoorzienbaar zijn of geheim moeten blijven, ontsnapt een deel van hun budget aan die regel. Dat deel is beter gekend als de 'speciale fondsen'. Hoewel het bedrag van die fondsen deel uitmaakt van het budget dat aan de diensten wordt toegewezen, gelden er bijzondere regels voor het beheer, het gebruik en de controle ervan. Het Comité onderzocht in 2015[135] onder meer welke de 'speciale fondsen' zijn, om welke bedragen het gaat en hoe ze worden verdeeld. Het controleerde ook de wijze waarop de middelen

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

135 VAST COMITE I, *Activiteitenverslag 2015*, 12-15 ('Het beheer, het gebruik en de controle van de speciale fondsen').

werden aangewend en hoe de wisselwerking verloopt tussen deze 'speciale fondsen' en de 'normale' budgetten. Ook werd het reglementaire kader bestudeerd en onderzocht welke controlemechanismen er bestaan, en dit zowel intern (binnen de diensten) als extern (Rekenhof, Vast Comité I...). Diverse aanbevelingen werden geformuleerd.

Sinds 2018 (VSSE) en 2020 (ADIV) uitte het Rekenhof het voornemen om eveneens een periodieke controle te doen van deze fondsen.[136] Daarbij kon het Rekenhof beroep doen op de technische ondersteuning zoals voorgeteld door het Vast Comité I.[137] Het Comité op zijn beurt kon dan weer "*exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds*". In 2020 werd een opvolgonderzoek opgestart naar het beheer, het gebruik en de controle van de speciale fondsen. Onderbroken omwille van andere, meer prioritaire dossiers in 2021, werden de onderzoeksactiviteiten hernomen in 2022. Het onderzoek kon begin 2023 worden afgerond en de resultaten werden voorgelegd aan de parlementaire Begeleidingscommissie.

I.10.4. DE OPVOLGING VAN IMAM TOJGANI DOOR DE VSSE

In januari 2022 meldde de pers dat Mohamed TOJGANI, hoofdimam van de Al Khalil-moskee in Molenbeek, bij de Raad voor Vreemdelingenbetwistingen (RVB) in beroep was gegaan tegen de beslissing om zijn verblijfsvergunning in België in te trekken. Hierover ondervraagd in de plenaire vergadering van de Kamer van volksvertegenwoordigers, bevestigde de Staatssecretaris voor Asiel en Migratie de op basis van informatie van de inlichtingendiensten genomen beslissing.

Op verzoek van de Kamervoorzitster stelde het Vast Comité I een toezichtonderzoek in naar de wijze waarop de VSSE de imam heeft opgevolgd. Meer in het bijzonder betreft het een onderzoek naar de informatiepositie van de VSSE aangaande de imam alsook de wijze waarop de dienst zijn opvolging verzekerde.

Tevens wordt de verwerking van en verspreiding naar andere administraties van persoonsgegevens van Mohamed TOJGANI door de VSSE bestudeerd. In dit verband toetst het Comité enerzijds de adequaatheid van de aan de autoriteiten meegedeelde informatie met de door de dienst verzamelde en geanalyseerde informatie, en wordt anderzijds nagegaan of er is voldaan aan de vereisten van de wetgeving inzake de bescherming van persoonsgegevens.

---

136 Het Comité kreeg in 2020 kopie van de in 2019 door het Rekenhof uitgevoerde controle bij de VSSE voor het boekjaar 2018 COUR DES COMPTES, *Sûreté de l'Etat. Contrôle 2019 des fonds spéciaux. Rapport adressé au ministre de la Justice*, 20 mai 2020.

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

De onderzoeksopdrachten en de analyse van de bekomen resultaten werden eind 2022 voltooid; het Comité kon zijn toezichtrapport in het eerste kwartaal van 2023 aan de Begeleidingscommissie voorleggen.

I.10.5. VEILIGHEIDSSCREENINGS VAN KANDIDAAT-PERSONEELSLEDEN VAN DE VSSE

In het nabije verleden formuleerde het Vast Comité I heel wat aanbevelingen met betrekking tot veiligheidsscreenings: over de nood aan veiligheidsscreenings voor vertrouwensfuncties[138], meer screenings van militairen en burgerpersoneel bij Defensie[139], over de correcte toepassing van de mogelijkheid om veiligheidsscreenings aan te vragen[140]… Ook in het kader van het specifieke toezichtonderzoek naar veiligheidsscreenings, werden diverse aanbevelingen geformuleerd.[141] In het verlengde hiervan werd door het Comité de prescreening van kandidaat-personeelsleden bij de VSSE aangekaart en werd besloten, vanuit zijn hoedanigheid van Bevoegde Toezichthoudende Autoriteit (BTA) zoals bedoeld in de Wet van 30 juli 2018, dit nader te onderzoeken. Eind 2022 werden diverse onderzoeksdaden werden verricht; een eindrapport zal worden opgesteld in de loop van 2023.

I.10.6. KLACHT VAN DE MOSLIMEXECUTIEVE VAN BELGIË TEGEN VERMEENDE LEKKEN VAN DE VSSE

Op 14 februari 2022 werd door het Executief van de Moslims van België (hierna: de Molsimexecutieve of EMB) bij het Vast Comité I een '*formele, schriftelijke klacht neergelegd aangaande de werking, het optreden, het handelen of het nalaten te handelen van de Veiligheid van de Staat*'.[142] In zijn brief stelt de Moslimexecutieve dat '*de laatste jaren rapporten en nota's van de Staatsveiligheid vaak als middel worden ingezet om moslims en moskeeën in diskrediet te brengen*', en wordt klacht ingediend '*over de werking van de Staatsveiligheid, meer bepaald met betrekking tot het systematisch lekken van rapporten en het verlenen van inzage in rapporten aan journalisten, terwijl de personen die onderwerp uitmaken van deze rapporten deze mogelijkheid niet hebben*'.

138 VAST COMITE I, *Activiteitenverslag 2021*, 218;
139 VAST COMITE I, *Activiteitenverslag 2021*, 207.
140 VAST COMITE I, *Activiteitenverslag 2021*, 206.
141 VAST COMITE I, Activiteitenverslag 2019, 2-18 ('I.1. De uitvoering van veiligheidsscreenings door de inlichtingendiensten') en 124-127 (XI.2.1. Diverse aanbevelingen naar aanleiding van het toezichtonderzoek naar veiligheidsscreenings').
142 Schrijven van meester Verbist, optredend als advocaat van het Executief van de Moslims in België, d.d. 14 februari 2022 betreffende 'klacht inzake het lekken van documenten van de Veiligheid van de Staat aangaande de moslimgemeenschap'.

Door de gelekte nota's zou een (blijvend) negatief en stigmatiserend beeld worden gecreëerd over de Islam en de moslims in Vlaanderen. Dat systematisch lekken naar de media vormt, aldus de Moslimexecutieve, een inbreuk op het privéleven van de personen die onderwerp uitmaken van deze rapporten (art. 22 Grondwet en art. 8 EVRM). Er werden een vijftal voorbeelden[143] opgesomd alsook tal van vragen voorgelegd.

Begin maart 2022 informeerde het Vast Comité I de Kamervoorzitster en tevens de klager over het openen van een toezichtonderzoek naar de klacht van de Moslimexecutieve tegen vermeende lekken in hoofde van de Veiligheid van de Staat. Er werd tevens meegedeeld dat, omwille van andere prioriteiten, het onderzoek pas zou worden opgestart in het najaar van 2022.

I.10.7. DE TOEGANG TOT POLITIONELE CAMERABEELDEN VOOR DE INLICHTINGENDIENSTEN

Half mei 2022 werd door de korpschef van een lokale politiezone een schrijven gericht aan het Vast Comité I met betrekking tot de toegang tot politionele camerabeelden voor de inlichtingendiensten.

In toepassing van de Inlichtingenwet en de Wet op het Politieambt kunnen inlichtingendiensten, mits verschillende voorwaarden, toegang krijgen tot de beelden van videobewakingscamera's van de politiediensten. De korpschef meldde in kennis te zijn gebracht van overeenkomsten of akkoorden met politiezones voor de overdracht van gegevens op afstand (m.a.w. de VSSE die vanuit Brussel de controle over elders in België verzamelde beelden overneemt). De geijkte methode is om de beelden *in situ* op te vragen waarbij en politieoperator aanwezig is in het beheercentrum van de politiezone. De korpschef was van oordeel dat, teneinde de rechtszekerheid van alle actoren te waarborgen, de toepassing van deze methode een juridische analyse vereiste.

143 Zo onder meer over het uitlekken van de nota van de VSSE over de mogelijke banden tussen Ihsane Haouach en de Moslimbroederschap. Dit maakte reeds het onderwerp van onderzoek uit door het Vast Comité I ('Toezichtonderzoek naar de wijze waarop de VSSE de regeringscommissaris Ihsane Haouach opvolgde', zie : www.comiteri.be).

I.10.8. JURIDISCHE ANALYSE AANGAANDE DE WETTELIJKE MOGELIJKHEDEN TOT VERSTORING

In 2022 heeft het Vast Comité I een juridische analyse gemaakt van de wettelijke mogelijkheden waarover de inlichtingendiensten beschikken met betrekking tot disruptie (of verstoring). Deze analyse had tot doel opheldering te verschaffen over een kwestie die was gerezen in verschillende door het Comité onderzochte zaken, waaronder het toezichtonderzoek naar de wijze waarop de Veiligheid van de Staat imam Mohamed TOJGANI heeft opgevolgd. In het kader van zijn bevoegdheid als gegevensbeschermingsautoriteit (DPA) ten aanzien van de VSSE en de ADIV, met name in het kader van de behandeling van DPA-klachten, wordt het Comité ook af en toe met deze kwestie geconfronteerd.

Met deze analyse wilde het Comité nagaan hoe de VSSE haar interne verstorings-strategie organiseert. Het Comité heeft zich gericht op de interne regelgeving en de overeenstemming daarvan met het wettelijk kader dat van toepassing is op de VSSE. Het Comité heeft in dit stadium niet onderzocht hoe de civiele inlichtingendienst zijn theorie over verstoring in praktijk brengt. Hoewel oorspronkelijk de VSSE werd bestudeerd, is ook gekeken naar de voorwaarden waaronder de ADIV bevoegd is veiligheidsdreigingen te bestrijden en te verstoren.

De juridische analyse van het Comité en de daaruit voortvloeiende aanbevelingen zijn toegezonden aan de inlichtingendiensten en in het eerste kwartaal van 2023 besproken in de parlementaire Begeleidingscommissie.

HOOFDSTUK II.

DE CONTROLE OP DE BIJZONDERE EN BEPAALDE GEWONE INLICHTINGENMETHODEN

Artikel 35 van de Toezichtwet draagt het Comité op om in zijn activiteitenverslag "*specifiek aandacht [te besteden] aan de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, zoals bedoeld in artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten […]. Het verslag bevat het aantal gegeven machtigingen, de duur van de uitzonderlijke methoden voor het verzamelen van gegevens, het aantal betrokken personen en, in voorkomend geval, de behaalde resultaten*".

Naast deze bijzondere methoden zijn er de gewone methoden waarbij aan het Comité een specifieke, beperkte controlemodaliteit werd toegekend of waarbij de inlichtingendiensten verplicht worden om aan het Comité bepaalde informatie te verstrekken die hem kan helpen bij zijn reguliere toezichtstaak. Ze worden door het Comité aangeduid als 'gewone methoden plus'. Voor enkele van die methoden heeft de wetgever voorzien in een specifieke rapportage aan het Parlement (met name de methoden voorzien in art. 16/2 W.I&V). Het Comité heeft er echter voor geopteerd om elk van die methoden kort te bespreken.

Hetzelfde geldt voor de zogenaamde beschermings- en ondersteuningsmaatregelen die door de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) kunnen worden ingezet naar aanleiding van een inlichtingenopdracht. In de mate waarin hier aan het Comité enige rol werd toegekend, worden ze kort toegelicht.

De regelingen inzake de bijzondere methoden, de 'gewone methoden plus' en de beschermings- en ondersteuningsmaatregelen kenden in 2022 een aantal grondige wijzigingen. Twee wetten zijn hiervoor verantwoordelijk:

– de Wet van 14 juli 2022 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten[144]; en

[144] Zie hierover ook VAST COMITÉ I, *Activiteitenverslag 2021*, 148 e.v. (Hoofdstuk VI.4. Advies over het voorontwerp van wet tot wijziging van de Inlichtingenwet).

– de Wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten.[145]

In deze tweede wet werd aan het Comité nog een bijzondere controle opgedragen die verband houdt met de dataretentie. Ze wordt besproken in II.5 van onderhavig hoofdstuk.

II.1. DE BIJZONDERE INLICHTINGENMETHODEN

II.1.1. EEN OVERZICHT VAN DE BELANGRIJKSTE WETSWIJZIGINGEN IN 2022

Sinds midden augustus 2022 mogen ook specifieke en uitzonderlijke methoden worden aangewend voor de beoordeling van de betrouwbaarheid van menselijke bronnen of ter verzekering van hun bescherming (art. 18 § 2, 18/1, 3° en 18/9 § 1 W.I&V).

Tevens werd de bevoegdheid van de ADIV uitgebreid tot het neutraliseren, in het kader van een nationale *cybersecurity* crisis[146], van een cyberaanval op informatica- en verbindingssystemen niet beheerd door de minister van Landsverdediging en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht (art. 11 § 1, 2° /1, W.I&V).

Wat betreft de in te zetten specifieke methoden, vallen volgende wijzigingen te noteren:

– Op basis van de specifieke methode voorzien in artikel 18/7 § 1, 2°, W.I&V kan de VSSE of de ADIV ook de mededeling vorderen van de facturen met betrekking tot de geïdentificeerde abonnementen;
– Totaal nieuw is de bevoegdheid om in de virtuele wereld te infiltreren onder dekmantel van een fictieve identiteit of fictieve hoedanigheid (art. 18/5/1 W.I&V).

Wat betreft de in te zetten uitzonderlijke methoden zijn volgende wijzigingen te noteren:

---

145 Zie hierover ook VAST COMITÉ I, *Activiteitenverslag 2021*, 144 e.v. (Hoofdstuk VI.3. Advies over dataretentie).

146 Een nationale *cybersecurity* crisis is elke *cybersecurity* gebeurtenis die wegens haar aard of gevolgen de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt, een dringende besluitvorming vereist en de gecoördineerde inzet van verscheidene departementen en organismen vergt.

– Op basis van artikel 18/12/1 W.I&V kunnen de inlichtingen- en veiligheidsdiensten in de reële wereld infiltreren, conform de richtlijnen van de Nationale Veiligheidsraad. Het Comité heeft geen kennis van dergelijke richtlijn. Deze methode kan derhalve nog niet worden aangewend;
– Het opvragen van financiële informatie werd uitgebreid onder meer door de verwijzing naar het centraal aanspreekpunt gehouden door de Nationale Bank van België (art. 18/15 W.I&V).

II.1.2. DE BIM-METHODEN IN CIJFERS

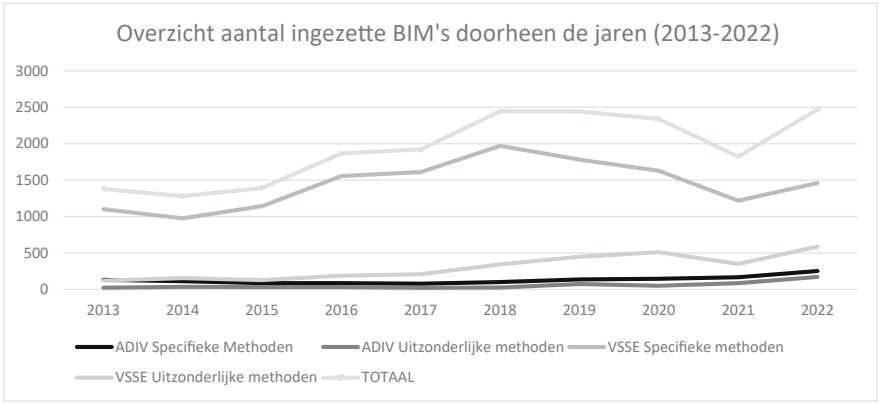
II.1.2.1. Algemene trends

Tussen 1 januari en 31 december 2022 werden door de twee inlichtingendiensten samen 2472 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 2047 door de VSSE (waarvan 1460 specifieke en 587 uitzonderlijke) en 425 door de ADIV (waarvan 253 specifieke en 172 uitzonderlijke). Niettegenstaande opnieuw een kleine inhaalbeweging werd vastgesteld, blijft de VSSE het leeuwendeel (ca. 83%) van de ingezette bijzondere inlichtingenmethoden voor zijn rekening te nemen.

Onderstaande tabel maakt een vergelijking met de cijfers van de afgelopen tien jaren.

	ADIV		**VSSE**		**TOTAAL**
	Specifieke Methoden	**Uitzonderlijke methoden**	**Specifieke methoden**	**Uitzonderlijke methoden**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445
2019	138	76	1781	449	2444
2020	146	51	1629	511	2337
2021	166	87	1220	350	1823
2022	253	172	1460	587	2472

Dit kan als volgt grafisch worden weergegeven:



Deze cijfers tonen aan dat de significante daling die zich in 2021 manifesteerde volledig teniet is gedaan. De globale BIM-cijfers zitten opnieuw op het niveau van 2019-2020. Als de cijfers worden uitgesplitst, kan worden vastgesteld dat bij de ADIV de in 2020 ingezette stijging van specifieke methoden (van 166 in 2021 naar 253 in 2022) blijft voortduren. Daarnaast merken we een enorme stijging van het aantal ingezette uitzonderlijke methoden bij ADIV, zelfs ten opzichte van 2019-2020. Het betreft meer dan een verdubbeling (van 87 naar 172). Een gelijkaardige beweging tekent zich af bij de VSSE: het aantal ingezette specifieke methoden neemt gestaag toe (van 1220 in 2021 naar 1460 in 2022), maar de stijging is vooral opmerkelijk voor wat betreft het aantal uitzonderlijke methoden (van 350 in 2021 naar 587 in 2022).

II.1.2.2. Methoden aangewend door de ADIV

De specifieke methoden

Specifieke methoden (ADIV)	**Aantal toelatingen 2021**	**Aantal toelatingen 2022**
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)	12	38
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	1

Specifieke methoden (ADIV)	Aantal toelatingen 2021	Aantal toelatingen 2022
Infiltreren in de virtuele wereld onder dekmantel van een fictieve identiteit of fictieve hoedanigheid (art. 18/5/1 W.I&V).	nvt	nvt
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 (art. 18/7 §1, 1° W.I&V)	6	12
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 §1, 2° W.I&V)	0	2
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8, §1, 1° W.I&V)	75	100
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator en de mededeling vorderen van de facturen (art. 18/8, §1, 2° W.I&V)	73	100
TOTAAL	**166**	**253**

Wat betreft de inzet van specifieke methoden, vormen het 'opsporen van verkeersgegevens van elektronische communicatiemiddelen' (art. 18/8, §1, 1° W.I&V) en het 'kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer' (art. 18/8, §1, 2° W.I&V) het merendeel van de ingezette methoden. Deze methoden, die doorgaans samen worden ingezet, spannen zoals steeds de kroon (200 van de 253 ingezette specifieke methoden). Er vonden ook driedubbel zoveel observaties plaats in publiek toegankelijke plaatsen met een technisch middel dan in 2021 (van 12 naar 38 in 2022).

Volgens de ADIV werd in 2021 een aantal methoden niet ingezet wegens gebrek aan personeel. Daarnaast kwam men bij de ADIV tot de vaststelling dat een aantal specifieke methoden te weinig ingeburgerd zijn bij de medewerkers en bijgevolg te weinig werden ingezet. Om aan dit euvel te verhelpen, werden begin 2022 interne briefings georganiseerd.

De uitzonderlijke methoden

Uitzonderlijke methoden (ADIV)	Aantal toelatingen 2021	Aantal toelatingen 2022
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)	3	20
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)	2	10
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	2	4
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	8	19
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	14	24
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	60	95
TOTAAL	**89**	**172**

Er wordt een sterke stijging van het aantal ingezette uitzonderlijke methoden vastgesteld. De procentueel sterke stijging (bijna verdubbeling) van het aantal door de ADIV ingezette uitzonderlijke methoden, situeert zich voornamelijk in het kader van het binnendringen in een informaticasysteem (art. 18/16 W.I&V) (van 14 in 2021 naar 24 in 2022) en het afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V) (van 60 in 2021 naar 95 in 2022). Ook het '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' kent een sterke toename (van 2 naar 10). Het 'inzetten van een fictieve rechtspersoon om gegevens te verzamelen (art. 18/13 W.I&V)' als uitzonderlijke methode werd door de ADIV sinds de invoegetreding van de Wet van 2010 nog nooit toegepast. Al in 2016 werd dezelfde vaststelling gedaan en toen verklaard door het feit dat "*de procedure voor de oprichting te omslachtig is om die voor een enkel dossier in gang te zetten*".[147]

147 Memorie van toelichting bij het wetsontwerp tot wijziging van de wet van 30 november 1998, *Parl. St.* Kamer, 2015-16, 54K2043/001, 11.

Het Comité wees de ADIV eerder[148] op de verplichting om de BIM-Commissie tweewekelijks in te lichten over de uitvoering van deze uitzonderlijke methoden (art. 18/10 §1, derde lid W.I&V en art. 9 KB 12 oktober 2010). Daarop werd een tweewekelijks overleg in het leven geroepen. De sanitaire maatregelen opgelegd in het kader van het coronavirus, maakten dat deze vergaderingen niet meer konden plaatsvinden. Ze werden in het voorjaar van 2022 opnieuw opgestart. Hierdoor kon een betere kwalitatieve *follow-up* van de dossiers door zowel de BIM-Commissie als het Vast Comité I worden gerealiseerd.

De opdrachten en de dreigingen die de inzet van (de gewone en) bijzondere methoden rechtvaardigen[149]

De ADIV mag de specifieke en uitzonderlijke methoden aanwenden in het kader van zes opdrachten, daarbij rekening houdend met verschillende dreigingen.

1. De inlichtingenopdracht (art. 11, 1° W.I&V)
   Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties.
   Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die volgende belangen bedreigt of zou kunnen bedreigen:
   - de onschendbaarheid van het nationaal grondgebied of het voortbestaan van de gehele of een deel van de bevolking;
   - de militaire defensieplannen;
   - het wetenschappelijk en economisch potentieel op vlak van defensie;
   - de vervulling van de opdrachten van de strijdkrachten;
   - de veiligheid van de Belgische onderdanen in het buitenland.
2. De zorg voor het behoud van de militaire veiligheid (art. 11, 2° W.I&V)
   - de militaire veiligheid van het personeel dat onder de minister van Landsverdediging ressorteert;
   - de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen;
   - in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten.

148 VAST COMITÉ I, *Activiteitenverslag 2017*, 109 ('XII.II.3.3. Informatieplicht in het kader van uitzonderlijke methoden').

149 Per toelating kunnen meerdere opdrachten en dreigingen aan de orde zijn.

3. Het neutraliseren, in het kader van een nationale cybersecurity crisis, van een cyberaanval op informatica- en verbindingssystemen niet beheerd door de minister van Landsverdediging en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht (art. 11 § 1, 2° /1, W.I&V)
4. 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.
5. 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).
6. De beoordeling van de betrouwbaarheid van menselijke bronnen of ter verzekering van hun bescherming (art. 18 § 2, 18/1, 3° en 18/9 § 1 W.I&V).

De inzet van bijzondere methoden is sinds 2017 niet meer beperkt tot het Belgische grondgebied (art. 18/1, 2° W.I&V). Van deze mogelijkheid werd nog nooit gebruik gemaakt. Nochtans werd ze in de wet ingeschreven omdat de ADIV ze als een noodzakelijkheid beschouwde om toe te laten haar buitenlandse opdrachten (in het bijzonder deze in het kader van de operaties met een mandaat van de Veiligheidsraad van de Verenigde Naties) naar behoren uit te kunnen voeren.[150] Nader onderzoek moet uitwijzen of de ADIV daadwerkelijk geen BIM-methoden heeft aangewend in het buitenland – wat dan wel een negatie zou betekenen van de argumentatie in de memorie van toelichting om het territoriale toepassingsgebied van de BIM-methoden te wijzigen – of als de situatie bestaat dat de ADIV wel BIM's in het buitenland aanwendt zonder evenwel gebruik te maken van de verplicht toe te passen BIM-procedure. Het Comité zal in 2023 nagaan of de ADIV exclusief gebruik maakt van de INT-regeling beschreven in artikel 44 W.I&V. Dit initiatief schrijft zich in in de filosofie van de memorie van toelichting van de wet van 2017 waarin wordt gesteld dat "*Binnen vijf jaar wordt de situatie opnieuw geëvalueerd om na te gaan of de voorrechten van de ADIV in het buitenland uitvoerbaar zijn en of zij de mandaten van de Verenigde Naties voldoende dekken*".

Er werden ook geen bijzondere inlichtingenmethoden ingezet op vraag van buitenlandse partnerdiensten.[151] Wel kan, aldus de ADIV, informatie verkregen

150 MvT, *Parl. St.* Kamer 2015-16, 54K2043/001.

151 Dit bleek soms wel het geval voor de inzet van 'gewone methoden plus' (maar enkel indien er ook een aanwijsbaar nut is voor de ADIV zelf).

van buitenlandse diensten de directe aanleiding vormen tot het opstarten van een bijzondere inlichtingenmethode.

De praktijk wijst uit dat per toelating verschillende dreigingen aan de orde kunnen zijn. Er kan een daling worden opgetekend voor wat betreft de inzet van BIM's in het kader van de dreigingen 'inmenging en criminele organisaties'. Opmerkelijk is de sterke stijging van het aantal uitzonderlijke methoden ingezet in het kader van de dreiging 'spionage' (van 120 in 2021 naar 309 in 2022).

AARD DREIGING	AANTAL 2021	AANTAL 2022
Spionage	120	309
Inmenging	16	4
Extremisme - radicalisme	82	95
Terrorisme	9	0
Criminele organisatie	26	16
Andere	0	1
Totaal	**253**	**425**

II.1.2.2. Methoden aangewend door de VSSE

De specifieke methoden

Specifieke methoden (VSSE)	Aantal toelatingen 2021	Aantal toelatingen 2022
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)	195	231
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	33	23
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 (art. 18/7 §1, 1° W.I&V)	22	39

Specifieke methoden (VSSE)	Aantal toelatingen 2021	Aantal toelatingen 2022
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 §1, 2° W.I&V)	2	3
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8, §1, 1° W.I&V)	491	595
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator en de mededeling vorderen van de facturen (art. 18/8, §1, 2° W.I&V)	477	567
TOTAAL	**1220**	**1460**

De sterke daling van het aantal specifieke methoden in 2021 werd omgebogen naar een stijging, maar bereikt het niveau van 2020 met 1629 toelatingen nog niet. De huidige stijging doet zich voor bij zowat alle specifieke methoden.

De uitzonderlijke methoden

Uitzonderlijke methoden (VSSE)	Aantal toelatingen 2021	Aantal toelatingen 2022
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	37
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)	11	23
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	13	22

Uitzonderlijke methoden (VSSE)	Aantal toelatingen 2021	Aantal toelatingen 2022
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	73	108
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	61	67
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	192	330
TOTAAL	**363**	**587**

Net als de inzet van specifieke methoden, nam ook het aantal door de VSSE ingezette uitzonderlijke methoden toe (van 363 in 2021 naar 587 in 2022).

De opdrachten en de dreigingen die de inzet van bijzondere methoden rechtvaardigen

De volgende tabel toont in het kader van welke (potentiële) dreigingen de VSSE specifieke en uitzonderlijke methoden toepasten. 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).

Soms zal de potentiële dreiging niet vooraf gekend zijn. Dit kan bijvoorbeeld bij de beoordeling van de betrouwbaarheid van menselijke bronnen of ter verzekering van hun bescherming (art. 18 § 2, 18/1, 3° en 18/9 § 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 2021	AANTAL 2022
Spionage	478	612
Inmenging	121	325
Extremisme - radicalisme	279	362
Proliferatie	2	4
Schadelijke sektarische organisaties	0	0
Terrorisme	690	715
Criminele organisaties	0	29
Activiteiten buitenlandse diensten in België opvolgen	(inbegrepen in bovenstaande cijfers)	(inbegrepen in bovenstaande cijfers)
TOTAAL	**1570**	**2047**

Bovenstaande tabel toont aan dat wat betreft de inzet van BIM-methoden in 2022 de dreiging 'terrorisme' licht toeneemt (van 690 in 2021 naar 715 in 2022), en daarmee de absolute prioriteit blijft voor de VSSE en dit gevolgd door spionage (612). Waar in 2020 nog sprake was van een sterke afname van het aantal 'inmengingsdossiers', kan opnieuw een sterke stijging worden vastgesteld (van 121 in 2021 naar 325 in 2022). Het is in de praktijk evenwel niet altijd evident om een duidelijk onderscheid te maken tussen spionage (het clandestien gegevens ophalen) en inmenging (beïnvloeden van beslissingsprocessen). De dreiging 'extremisme-radicalisme' steeg eveneens opmerkelijk (van 279 dossiers in 2021 naar 362 dossiers in 2022). Ook de dreiging 'criminele organisaties' komt opnieuw voor in de cijfergegevens (29).[152]

Op vlak van territorialiteit, is de VSSE bevoegd om BIM's in te zetten 'op en vanaf Belgisch grondgebied' (art. 18/1, 1 W.I&V). Net zoals bij de ADIV, werden door de VSSE geen bijzondere inlichtingenmethoden ingezet in het buitenland. Ook de inzet van dergelijke methoden in België op vraag van buitenlandse partnerdiensten, is verwaarloosbaar. Wel werd op basis van informatie ontvangen van partnerdiensten beslist om bijzondere inlichtingenmethoden toe te passen. 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;
4. De beoordeling van de betrouwbaarheid van menselijke bronnen of ter verzekering van hun bescherming (art. 18 § 2, 18/1, 3° en 18/9 § 1 W.I&V).

152 *Hand.* Kamer Gezamenlijke Commissie Binnenlandse Zaken en Justitie 2022-2023, 24 oktober 2022, 10-11 (integraal verslag nr. CRIV 55 COM 913).

Net als bij de ADIV, worden door de VSSE verschillende belangen gecombineerd. Wel kan worden vermeld dat de 'vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel' weinig voorkwam.

Zoals boven gezegd, 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.1.3. DE CONTROLE DOOR HET VAST COMITÉ I

II.1.3.1. De cijfers

In wat volgt wordt ingegaan op de jurisdictionele controle van het Vast Comité I met betrekking tot de specifieke en uitzonderlijke inlichtingenmethoden. Daarbij dient 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 een eventuele vatting.

Artikel 43/4 W.I&V stelt dat het Vast Comité I op vijf manieren kan worden gevat:

1. Op eigen initiatief;
2. Op verzoek van de Gegevensbeschermingsautoriteit (GBA);
3. Op klacht van een burger;
4. Van rechtswege als de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden;
5. Van rechtswege als de bevoegde minister een toelating heeft verleend op basis van artikel 18/10 § 3 W.I&V.

Daarnaast kan het Comité ook gevat worden in zijn hoedanigheid van 'prejudicieel adviesverlener' (art. 131*bis*, 189*quater* en 279*bis* Sv.). In dat geval geeft het Comité een advies over de al dan niet rechtmatigheid de specifieke of uitzonderlijke methoden die inlichtingen hebben opgeleverd die in een strafzaak worden gebruikt. De beslissing om een advies te vragen berust bij de onderzoeksgerechten of de strafrechters. Strikt genomen treedt het Comité alsdan niet op als jurisdictioneel orgaan.

WIJZE VAN VATTING	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
1. Op eigen initiatief	16	12	16	3	1	1	4	2	1	5
2. Gegevensbeschermingsautoriteit	0	0	0	0	0	0	0	0	0	0
3. Klacht	0	0	0	1	0	0	0	0	0	0
4. Exploitatieverbod door BIM-Commissie	5	5	11	19	15	10	12	9	8	9
5. Toelating minister	2	1	0	0	0	0	0	0	0	0
6. Prejudicieel adviesverlener	0	0	0	0	0	0	0	0	0	0
TOTAAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**	**9**	**14**

Het aantal door het Comité genomen beslissingen stijgt voor het eerst sinds twee jaar en volgt daarmee de stijging van het aantal BIM-methoden. Het aantal vattingen steeg van 9 naar 14 en dit voor een stijging van 650 BIM-methoden tussen 2021 en 2002. De toename van het aantal vattingen is evenredig met de toename van het aantal BIM-methoden. Wel blijven de meeste vattingen opnieuw het gevolg van een schorsing door de BIM-Commissie (9 op 14 vattingen). 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 waarvan hij drager is te moeten bewaren omdat de onthulling ervan nadelig is voor de bescherming van de bronnen, de bescherming van de persoonlijke levenssfeer van derden of de vervulling van de opdrachten van de inlichtingendienst (art. 43/5 § 4, derde lid, W.I&V);
11. Stopzetting van een methode indien ze nog steeds in uitvoering is of indien zij werd geschorst door de BIM-Commissie en bevel dat de gegevens die met deze methode werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd (art. 43/6 § 1, eerste lid, W.I&V);
12. Gedeeltelijke stopzetting van een toegelaten methode. Hier wordt de situatie bedoeld waarbij bijvoorbeeld één methode in tijd wordt beperkt, niet de situatie waarbij in één toelating van een diensthoofd meerdere methoden worden gemachtigd en het Comité slechts één ervan stopzet;
13. Gehele of gedeeltelijke opheffing van de schorsing en het verbod die door de BIM-Commissie was uitgesproken (art. 43/6 § 1, eerste lid, W.I&V). Dit houdt in dat de door het diensthoofd toegelaten methode door het Comité wel (gedeeltelijk) wettelijk, proportioneel en subsidiair werd bevonden;
14. Onbevoegdheid van het Vast Comité I;
15. Ongegrondheid van de aanhangige zaak en geen stopzetting van de methode;
16. Advies als prejudicieel adviesverlener (artt. 131*bis*, 189*quater* en 279*bis* Sv.).

AARD VAN DE BESLISSING	2014	2015	2016	2017	2018	2019	2020	2021	2022
Beslissingen voorafgaand aan de vatting									
1. Nietige klacht	0	0	0	0	0	0	0	0	0
2. Kennelijk ongegronde klacht	0	0	0	0	0	0	0	0	0
Tussenbeslissingen									
3. Schorsing methode	3	2	1	0	0	0	1	0	0

AARD VAN DE BESLISSING	2014	2015	2016	2017	2018	2019	2020	2021	2022
4. Bijkomende informatie van BIM-Commissie	0	0	0	0	0	0	0	0	0
5. Bijkomende informatie van inlichtingendienst	1	1	4	0	0	0	1	1	2
6. Onderzoeksopdracht Dienst Enquêtes[153]	54	48	60	35	52	52	24	33	40
7. Horen BIM-Commissieleden	0	2	0	0	0	0	0	0	0
8. Horen leden inlichtingendiensten	0	2	0	0	0	1	1	0	0
9. Beslissing m.b.t. geheim van onderzoek	0	0	0	0	0	0	0	0	0
10. Gevoelige informatie tijdens verhoor	0	0	0	0	0	0	0	0	0
Eindbeslissingen									
11. Stopzetting methode	3	3	6	9	4	11	10	5	9[154]
12. Gedeeltelijke stopzetting methode	10	13	4	6	6	4	0	3	3
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	0	4	11	0	0	0	0	0	0

153 Het Comité verzoekt de Dienst Enquêtes I om een bijkomende onderzoeksopdracht uit te voeren en/of mondeling de betrokken inlichtingendienst of de BIM-Commissie te contacteren.

154 In twee beslissingen heeft het Comité zich geschraagd achter de beslissing van de BIM-Commissie die geen eensluidend advies verschafte over een ontwerp van beslissing om een uitzonderlijke methode aan te wenden. Strikt genomen beslisten het Comité niet tot de stopzetting van de methode aangezien de betrokken inlichtingendienst de methode uiteindelijk niet had gemachtigd.

AARD VAN DE BESLISSING	2014	2015	2016	2017	2018	2019	2020	2021	2022
14. Onbevoegd	0	0	0	0	0	0	0	0	0
15. Wettige toelating/Geen stopzetting methode/ Ongegrond	4	6	2	1	1	0	0	1	2
Prejudicieel advies									
16. Prejudicieel advies	0	0	0	0	0	0	0	0	0

II.1.3.2. DE RECHTSPRAAK

Hieronder wordt de essentie weergegeven van de beslissingen die het Vast Comité I in 2022 nam binnen zijn jurisdictionele controle op de aanwending van de bijzondere inlichtingenmethoden. De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk worden opgenomen.

Foto's van een afgesloten plaats

Bij het nalezen van een observatierapport naar aanleiding van een gewone methode, bleek dat er foto's waren genomen van de tuin van de betrokkene en dat er op basis van artikel 18/4 W.I&V dus een specifieke methode had moeten worden aangevraagd. Het betrof immers '*een woning met tuin die afgesloten is met een niet doorzichtige omheining*'. '*Enkele gemaakte foto's tonen aanwezige voorwerpen in de tuin die boven de omheining uitsteken*', maar '*[d]eze voorwerpen zijn zichtbaar vanop de openbare weg, zonder hiervoor kunstgrepen te moeten uitvoeren*'. Het Comité stelt dat het '*est incontestable que l'observation effectuée ne pouvait l'être que sur la base d'une BIM prise en vertu de l'article 18/4 §2 L.R&S, ce qui ne fut aucunement le cas, par défaut même de mise en œuvre d'une quelconque procédure BIM*'[155]. De methode was dan ook niet wettig (2021/11081).

[155] '*het onbetwistbaar* is *dat de uitgevoerde observatie slechts had mogen uitgevoerd worden op basis van een BIM in uitvoering van artikel 18/4 §2 WI&V hetgeen geenszins gebeurde; er was zelfs geen sprake van de uitvoering van welkdanige BIM-procedure dan ook*'(vrije vertaling)

Een materiële vergissing

Een inlichtingendienst wenste in *real time* de lokalisatiegegevens te bekomen van een target aan de hand van zijn gsm-nummer (2022/11294). Bij het lanceren van deze specifieke methode werd echter een foutief document aan de BIM-Commissie gezonden. Het betrof '*een niet-finale versie*' die nog '*ettelijke fouten*' bevatte '*met betrekking tot de gevraagde periode en de gevraagde gegevens*'. Wanneer de inlichtingendienst dit opmerkt, zet ze de methode stop. De BIM-Commissie ging over tot de schorsing en het Vast Comité I stelde daaropvolgend vast dat de wettelijke voorschriften niet waren nageleefd.

Bijzondere methoden in bijstand van de noodhulp naar aanleiding van grote overstromingen

Naar aanleiding van de enorme overstromingen die ons land in juli 2021 teisterden, besliste de militaire inlichtingendienst om bij hoogdringendheid over te gaan tot de inzet van de specifieke methode bedoeld in artikel 18/3, § 3 en de uitzonderlijke methode bedoeld in artikel 18/11, § 1 W.I&V. Ze wou immers de beelden van een satellietsysteem, waarvan zij de enige Belgische exploitant is, gebruiken in het kader van de hulpverlening. Daarbij werden uiteraard beelden gemaakt van zowel voor het publiek toegankelijke plaatsen als niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en van personen en voorwerpen die zich daar bevinden of gebeurtenissen die daar plaatsvinden. Het Comité vatte zich in deze zaken (2021/10787 en 2021/10788) en kwam op basis van volgende elementen tot de conclusie dat de gemachtigde specifieke en uitzonderlijke methoden wettig, subsidiair en proportioneel waren.

Vooreerst stelt het Comité vast dat plaatsen op basis van de betrokken wetsbepalingen het voorwerp konden uitmaken van een specifieke of uitzonderlijke methode, zonder hieraan enige ruimtelijke beperking te koppelen, indachtig de naleving van de principes inzake proportionaliteit.

De specifieke methode had betrekking op de observatie van niet voor het publiek toegankelijke plaatsen die niet aan het zicht onttrokken zijn. Artikel 3, 12°/1 W.I&V omschrijft het begrip "*niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is*" als *"elke plaats waartoe het publiek geen toegang heeft en die voor iedereen zichtbaar is vanaf de openbare weg zonder hulpmiddel of kunstgreep, met uitzondering van de binnenkant van gebouwen die niet voor het publiek toegankelijk zijn*". Onder dit begrip vallen zodoende aanhorigheden van woningen (bijv. tuinen aan het zicht onttrokken door een hoge haag). Het Comité stelde dat het satellietsysteem zou kunnen gekwalificeerd worden als technisch hulpmiddel zoals bedoeld in artikel 3, 12°/1 W.I&V. In voorliggend dossier was dit evenwel geenszins het geval aangezien de beelden hiertoe niet gedetailleerd genoeg waren.

Verder stelde het Comité dat artikel 18/4, §§1 en 2 W.I&V noch artikel 18/11, § 1, W.I&V nader bepalen op welke wijze een observatie moet plaatsvinden. Daarbij kwam dat de informatie-inwinning kaderde binnen de opdracht tot nationale hulpverlening die de minister van Defensie aan de Krijgsmacht had gegeven. Deze opdracht was gestoeld op diverse wettelijke bepalingen.[156] Het Comité stelde verder vast dat de inzet van de ADIV stoelde op de artikelen 11, §1, 1°, *in limine*, 13, eerste lid en 18/1, 2°, W.I&V en op artikel 35/1 van het koninklijk besluit van 2 december 2018 tot bepaling van de algemene structuur van het ministerie van Landsverdediging en tot vaststelling van de bevoegdheden van bepaalde autoriteiten. Het nemen van satellietfoto's door de ADIV kaderde dan ook binnen een concrete opdracht inzake het verlenen van inlichtingensteun aan een lopende binnenlandse militaire operatie. Ook aan de subsidiariteitsvereiste was voldaan aangezien zowel de gewone als de specifieke methoden ontoereikend waren om de nodige informatie te bekomen. Hetzelfde gold voor de proportionaliteiteis: mede gelet op de ernst en de grootte van de schade veroorzaakt door de overstromingen en op de potentiële schade die hieruit nog kon voortvloeien, was het Comité van oordeel dat de inzet van de methoden proportioneel was.

Een methode op een verkeerd nummer

Enkele maanden na de opstart van de specifieke methode waarbij bepaalde verkeersgegevens van het in- en uitgaande verkeer van een gsm worden opgespoord, stelt de betrokken inlichtingendienst vast dat het geviseerde nummer verkeerd was doorgegeven. De dienst stopte de methode en bewaarde de reeds gecollecteerde gegevens apart. De BIM-Commissie werd ingelicht en deze schorste de methode. Het Comité bevestigde de schording. De methode werd definitief stopgezet en de gecollecteerde gegevens moesten vernietigd worden (2021/11060).

Vragen bij de proportionaliteit van een ingezette methode

Een inlichtingendienst wenst te weten te komen of een van de gsm's die officieel toebehoren aan een familielid van het target, niet door hem gebruikt wordt. Zij wil dit doen door de verkeers- en lokalisatiegegevens van die toestellen te controleren voor een periode van twaalf maanden. De BIM-Commissie schorste de methode en zond het dossier door naar het Comité voor beslissing. Het Comité oordeelde dat de periode van twaalf maanden niet proportioneel was. Het stelde dat '*een*

[156] Art. 3, §1, 2°, b) van de Wet van 20 mei 1994 'betreffende de perioden en de standen van de militairen van het reservekader alsook betreffende de aanwending en de paraatstelling van de Krijgsmacht'; art. 186, vierde lid van de Wet van 8 februari 2007 'tot vaststelling van het statuut van de militairen en kandidaat-militairen van het actief kader van de Krijgsmacht'; art. 6/1, eerste lid, 1°, en 6/2 van het Koninklijk besluit van 6 juli 1994 'houdende bepaling van de vormen van operationele inzet, hulpverlening en militaire bijstand, en van de voorbereidingsactiviteiten met het oog op de aanwending van de Krijgsmacht.

periode van 2 maanden […] aangewezen lijkt'. Indien nodig kon deze periode achteraf verlengd worden, aldus het Comité (2022/11256).

De inzet van een methode buiten de limieten van de beslissing

Een inlichtingendienst besliste tot de observatie van een bepaald gebouw en dit gedurende zes maanden vanaf de notificatie van de beslissing aan de BIM-Commissie. Het ingezette cameradispositief bleef echter een paar dagen langer beelden maken. Het Comité stelde dan ook vast dat die beelden niet gedekt waren door de beslissing en dat ze niet mochten geëxploiteerd en moesten vernietigd worden (2022/10587).

Een materiële vergissing

Via een uitzonderlijke methode wou een inlichtingendienst te weten komen welke *apps* een target gebruikte en welke *sites* hij consulteerde met zijn gsm. Bij de uitvoering van de methode werd echter verkeerdelijk overgegaan tot de kennisname van de inhoud van gevoerde gesprekken. Van zodra de betrokken dienst deze vergissing opmerkte, greep ze in. De BIM-Commissie was genoodzaakt de methode te schorsen en vatte hierdoor het Comité die de kennisname van de inhoud onwettig verklaarde en het bevel gaf om de onrechtmatig verkregen gegevens te vernietigen (2022 /11419).

Een onvoldoende gedifferentieerde inzet van een specifieke methode

Een inlichtingendienst wil de telefoniegegevens bekomen van vele tientallen personen die door het OCAD waren opgelijst als beantwoordend aan een welbepaald dreigingscriterium. De inlichtingendienst beweert deze gegevens nodig te hebben om onder meer de informatie *'die ze over deze personen reeds heeft, aan te vullen. Deze gegevens, die een beeld geven van de contacten die de targets onderhouden, kunnen aantonen of de betrokkene nog een problematisch profiel vertonen en of ze eventueel bezig zijn met bedreigende activiteiten*.' Op basis van artikel 18/3, §4 W.I&V moet elke beslissing '*de feitelijke omstandigheden [weergeven] die de specifieke methode rechtvaardigen, de motivering inzake subsidiariteit en proportionaliteit, inbegrepen het verband tussen*' de personen en de geviseerde potentiële dreiging. In het concrete geval beperkte de motivering zich echter grotendeels tot de verwijzing naar de criteria om op dergelijke OCAD-lijst te komen, terwijl zo'n lijst dynamisch is. '*[Q]ue les prescrits de la Loi organique du 30 novembre 1998 […] imposent aux services d'individualiser toutes motivations dans le cadre de la mise en œuvre des méthodes spécifiques décidées (ou autres envisagées), ce tant au niveau du lien à effectuer entre la menace ciblée et l'individu concerné qu'au niveau de la subsidiarité*

et de la proportionnalité des mesures spécifiques décidées (ou autres envisagées).'[157] *Naast het feit dat* de beslissing geen individualisering bevatte en dus geen enkele bijzondere en concrete verduidelijking bracht over de betrokkenen, bleek dat bepaalde personen op een lijst stonden die op basis van een ander dreigingscriterium was opgesteld. Zich aansluitend bij het oordeel van de BIM-Commissie besloot het Comité als volgt: '*une insuffisance de justification voire un manque de contextualisation concernant la menace évoquée et une insuffisance de motivation concernant les liens à effectuer entre une telle menace potentielle et les personnes ciblées ainsi que concernant les éléments de proportionnalité*'[158] (dossier 2022/11532).

Een probleem met de proportionaliteit en de subsidiariteit

Wanneer een ambtenaar een klacht indient bij het Comité wordt een onderzoek opgestart. Daaruit bleek dat de betrokken dienst op aangeven van de werkgever een inlichtingenonderzoek was opgestart tegen de ambtenaar. Terecht, want er was mogelijk sprake van radicalisme in de zin van de Inlichtingenwet. Maar al snel bleek dat een meer diepgaand onderzoek niet langer proportioneel was. De inzet van een specifieke methode was op dat ogenblik dan ook niet meer te rechtvaardigen: '*il n'y avait pas de menace(s) imminente(s) nécessitant de procéder à quelconque enquête telle qu'effectuée et de mettre en œuvre les méthodes de recueil de données, l'une ordinaire et l'autre particulière - spécifique*'[159]. Het Comité stelde dat '*le principe de subsidiarité quant à la méthode particulière - spécifique - ainsi que sa finalité n'ont pas été respectés*'[160] aangezien bepaalde beweringen in de BIM-beslissing manifest verkeerd waren en geen grondslag vonden in eerdere informatie waarover de dienst beschikte. De methode werd dan ook onwettig verklaard (2019/8823).

Nog een materiële vergissing

De dag nadat een inlichtingendienst via een specifieke en een uitzonderlijke methode was overgegaan tot de kennisname en interceptie van de communicatie die verloopt via een bepaald gsm-toestel, stelt men vast dat een van de drie gevorderde

---

157 '*Dat de bepalingen van de organieke wet van 30 november 1998 vereisen dat de diensten alle motiveringen in het kader van de uitvoering van besliste (of andere voorgenomen) specifieke methoden individualiseren, en dit zowel op niveau van het verband tussen de geviseerde bedreiging en het betrokken individu, als op het niveau van de subsidiariteit en de proportionaliteit van de besliste (of andere voorgenomen) specifieke methoden.*' (vrije vertaling)

158 '*er is een onvoldoende rechtvaardiging en zelfs een gebrek aan contextualisering van de ingeroepen dreiging en een onvoldoende motivering met betrekking tot de banden tussen een dergelijke potentiele dreiging en de geviseerde personen evenals met betrekking tot de elementen van de proportionaliteit.*' (vrije vertaling)

159 '*er was (waren) geen imminente dreiging(en) die het noodzaakten om over te gaan tot enig onderzoek zoals uitgevoerd en om de gewone of de specifieke methode in zetten.' (vrije vertaling)*

160 '*het principe van de subsidiariteit met betrekking tot de specifieke methode noch zijn finaliteit werd gerespecteerd.*' (vrije vertaling)

operatoren zich op een verkeerd IMEI-nummer had gebaseerd. De fout wordt onmiddellijk rechtgezet, maar de gegevens van die eerste dag zijn natuurlijk niet gedekt door een mandaat. De BIM-Commissie schorst de methode wat dit aspect betreft. Het Comité bevestigt die onwettigheid. Er stelde zich echter een probleem met de vernietiging van de via de uitzonderlijke methode gecollecteerde gegevens. Deze waren immers opgenomen in één document zodat niet meer kon uitgemaakt worden welke provider welke data had aangeleverd. Daarom besloot het Comité het volgende: '*Qu'enfin et qu'en ce qui concerne les seules data, il appert, prima facie, qu'une discrimination ne pourrait être réalisée entre les data recueillies et transmises par les trois opérateurs, celles-ci étant reprises sur un document unique de synthèse sans possibilité d'identification des opérateurs les ayant recueillies. Il conviendrait, dès lors et en pareil cas, d'en interdire purement et simplement leur exploitation et de les faire détruire sans autre forme de procès (…).*'[161] (2022/11825 en 2022/11826).

II.2. DE INZET VAN EN HET TOEZICHT OP DE 'GEWONE METHODEN PLUS'

Oorspronkelijk waren de gewone inlichtingenmethoden slechts aan het reguliere toezicht van het Comité onderworpen. Sinds enkele jaren werden er in de Inlichtingenwet echter gewone methoden ingeschreven waarbij aan het Comité een bijzondere controleopdracht werd toevertrouwd en/of waarbij aan de betrokken inlichtingendienst een bijkomende informatieplicht werd opgelegd ten aanzien van het Comité (de zgn. 'gewone methoden plus'). De controle of de informatieplicht is voor elk van die methoden anders geregeld, en dit ondanks het pleidooi van het Comité om dit te uniformiseren.[162]

---

161 *'Dat ten slotte wat betreft de data alleen prima facie blijkt dat er geen onderscheid kon worden gemaakt tussen de ingewonnen data en deze overgezonden door de drie operatoren aangezien ze werden opgenomen in één synthesedocument dat niet de mogelijkheid biedt om te identificeren welke operator welke data collecteerde. Het is dan ook aangewezen in dergelijk geval om eenvoudigweg de exploitatie te verbieden van alle data en ze zondermeer te laten vernietigen'.* (vrije vertaling)

162 Deze opdeling blijkt voor sommige te theoretisch en houdt te weinig rekening met de realiteit. Zie bijv. W. VAN LAETHEM, 'Enkele reflecties over tien jaar BIM-controle door het Vast Comité I', in VANDERBORGHT, J. (ed.), *o.c.*, 70-72. Het Comité is eenzelfde mening toegedaan en haalde bij wijze van voorbeeld artikel 16/3 W.I&V (verzamelen en verwerken van passagiersgegevens) en 16/4 W.I&V (verzamelen en verwerken van politionele camerabeelden) aan. Hoewel beide onderzoeks-bevoegdheden als een gewone methode worden gekwalificeerd, is de inmenging in de privacy bij deze methoden vaak groter dan bij sommige specifieke en zelfs uitzonderlijke inlichtingenmethoden. Dit is zeker het geval bij het cameragebruik wanneer hierbij intelligente camera's of *software* worden gebruikt zoals ANPR. Zie VAST COMITÉ I, Advies nr. 001/VCI/2021 van 12 juli 2021 (Wijzigingen Inlichtingenwet), consulteerbaar op www.comiteri.be.

II.2.1. DE IDENTIFICATIE VAN DE ABONNEE OF DE GEWOONLIJKE GEBRUIKER VAN TELECOMMUNICATIEDIENST OF -MIDDEL (ART. 16/2 W.I&V)

De identificatie van de abonnee of de gewoonlijke gebruiker van een telecommunicatiedienst of -middel (bijv. gsm-nummer of IP-adres[163]) is een gewone methode wanneer dit gebeurt via een vordering aan de telecomoperator of -provider of via een rechtstreekse toegang tot hun klantenbestanden.[164] De regeling voorziet in een verplichting voor de inlichtingendiensten om een register bij te houden van alle gevorderde identificaties en van alle via rechtstreekse toegang verkregen identificaties.[165]

ADIV	Aantal t oelatingen 2021	Aantal toelatingen 2022
Identificatie van de 'abonnee of de gewoonlijke gebruiker' van telecommunicatie	420	601

VSSE	Aantal toelatingen 2021	Aantal toelatingen 2022
Identificatie van de 'abonnee of de gewoonlijke gebruiker' van telecommunicatie	4080	5310

Wat betreft deze methode voerde de wet geen specifieke controle in. Er werd slechts bepaald dat het Comité maandelijks in het bezit wordt gesteld van de lijst van de gevorderde identificaties en van de rechtstreekse toegang. Het Comité ontvangt echter alleen het aantal vorderingen. Het Comité nam zich wel voor om jaarlijks steekproefsgewijs een aantal vorderingen te controleren.[166] Deze controle gebeurt maandelijks. Het vereist soms aanvullende informatie van de diensten.

In 2022 veranderde deze regeling in die zin dat de VSSE en de ADIV ook kunnen overgaan tot de identificatie van de abonnee of de gewoonlijke gebruiker van een elektronische communicatiedienst via de medewerking van:

---

163 Vanaf 2022 wordt ook het aantal vorderingen opgesplitst in 'vorderingen IP' en 'vorderingen non-IP'.

164 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).

165 De in artikel 16/2, §1, laatste lid W.I&V gecreëerde mogelijkheid voor de inlichtingendiensten om dergelijke identificatiegegevens op te vragen via een rechtstreekse toegang tot de klantenbestanden van de telecomoperatoren en -providers kende tot op heden geen uitwerking.

166 VAST COMITÉ I, *Activiteitenverslag 2017*, 25 voetnoot 40. Hiermee werd een aanvang genomen in 2020. Het Comité besliste deze thematiek mee op te nemen in zijn in 2019 geopende *'toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten die recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld.'*

- de personen of instellingen bedoeld in artikel 5, § 1, eerste lid, 3° tot 22° van de Wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten en van de personen of instellingen die, binnen het Belgisch grondgebied, diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde betaalmiddelen in virtuele waarden worden uitgewisseld, op basis van de referentie van een elektronische banktransactie die voorafgaandelijk meegedeeld is door een operator of verstrekker van een communicatiedienst;
- andere rechtspersonen die de abonnee zijn van een operator of verstrekker zoals bedoeld in paragraaf 1 of die zich in naam en voor rekening van natuurlijke personen abonneren op een elektronische communicatiedienst, op basis van gegevens die voorafgaand meegedeeld zijn door een operator of verstrekker.

II.2.2. TOEGANG TOT PNR-GEGEVENS VAN BELPIU (ART. 16/3 W.I&V EN ART. 27 VAN DE WET VAN 25 DECEMBER 2016)

Begin 2017[167] werd de mogelijkheid ingebouwd voor de inlichtingendiensten om toegang te krijgen tot informatie die berust bij de Passagiersinformatie-eenheid (BELPIU) en dit bij wijze van 'gerichte opzoekingen'. De toegang kan alleen 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 2022 werd door het Comité geen dergelijke verboden uitgesproken.

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). In deze heeft het Comité geen bijzondere bevoegdheden.

ADIV	Aantal toelatingen 2021	Aantal toelatingen 2022
Gerichte opzoekingen PNR-gegevens	29	33[168]

167 Wet van 25 december 2016 (*BS* 25 januari 2017).

168 De cijfers uit het Jaarrapport NTTC (National Travel Targeting Center) 2022 (p. 17) wijken hier licht van af. Hierin is sprake dat "*moet worden opgemerkt dat de verschillende ADIV-afdelingen 34 keer gebruik hebben gemaakt van de BelPIU om historisch onderzoek te verrichten en dat de VSSE dezelfde methode 229 keer heeft gebruikt*".

VSSE	Aantal toelatingen 2021	Aantal toelatingen 2022
Gerichte opzoekingen PNR-gegevens	98	221

De inzet van de gerichte opzoekingen kent een gestage opgang, en dit vooral bij de VSSE. Het aantal toelatingen voor gerichte opzoekingen in de passagiersgegevens (PNR) (art. 16/3 W.I&V) werd meer dan verdubbeld (van 98 naar 221). Het nut van deze methode neemt ook gestaag toe, nu het aantal aangesloten luchtvaartmaatschappijen ook exponentieel is toegenomen.[169] [170]

II.2.3. GEBRUIK VAN POLITIONELE CAMERABEELDEN (ART. 16/4, §2 W.I&V)

De inlichtingendiensten kunnen onder strikte voorwaarden gebruik maken van politionele camerabeelden. Daarbij werden aan het Comité bijzondere controlemodaliteiten toegekend: een *a priori*-[171] en een *a posteriori*-controle.[172] [173] In 2022 werd een lichte toename vastgesteld.

---

169 BelPIU stelt ondertussen een dekkingsgraad van 100% te benaderen.

170 In hetzelfde Jaarrrapport NTCC 2022 (pag. 17) werd ook opgemerkt dat "*er een versterkte samenwerking is ontstaan tussen VSSE en ADIV in de context van de BelPIU. Concreet betekent dit dat een veelvoud van methodes is gedeeld gedurende het jaar. Bijgevolg kan het zijn dat de resultaten van de ene dienst ook geteld worden bij de statistieken van de andere dienst. We stellen daarbij vast dat alle cijfers stijgen, zowel wat de verzoeken van de diensten als wat de gegenereerde resultaten betreft. Zo leverde crossmatching met de databanken 2.617 resultaten (een resultaat wordt gegenereerd per reisbeweging en niet per passagier, waardoor één passagier bijvoorbeeld evenveel resultaten kan genereren als het aantal (aan België) gerelateerde) reizen in zijn boeking) op voor de ADIV en 3.015 voor de VSSE, terwijl de ADIV-criterialijsten 8.277 positieve hits opleverden en die van de VSSE 4.473, wat neerkomt op een verdubbeling van de resultaten ten opzichte van het voorgaande jaar*".

171 '*De beoordelingscriteria bedoeld in het eerste lid, 2°, worden voorafgaandelijk aan het Vast Comité I voorgeleg*d.'

172 *'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 inlichtingenonderzoek. In dit geval wordt een lijst van de gerichte toegangen eenmaal per maand aan het Vast Comité I doorgegeven. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.*' en '*Elke lijst aan de hand waarvan de correlatie bedoeld in het eerste lid, 1°, wordt uitgevoerd, wordt zo spoedig mogelijk doorgegeven aan het Vast Comité I. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.*'

173 Begin 2022 formuleerde het Vast Comité I in zijn hoedanigheid van Bevoegde Toezichthoudende Autoriteit hierover een beslissing: VAST COMITÉ I, DPA-beslissing n° VCI-DPA/2022/2 – Verwerkingsinstructie m.b.t. de door de inlichtingendiensten ingestelde retroactieve opvragingen van politionele camerabeelden gegrond op artikel 16/4, §2 W.I&V.

ADIV	Aantal toelatingen 2021	Aantal toelatingen 2022
Gebruik politionele camerabeelden[174]	15	24

VSSE	Aantal toelatingen 2021	Aantal toelatingen 2022
Gebruik politionele camerabeelden	46	55

II.2.4. VORDEREN VAN BEPAALDE FINANCIËLE GEGEVENS (ART. 16/6 W.I&V)

Sinds august 2022 kunnen de VSSE en de ADIV de medewerking vorderen van:
- de personen en instellingen bedoeld in artikel 5, paragraaf 1, 3° tot 22°, van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;
- de personen en instellingen die, binnen het Belgisch grondgebied, diensten beschikbaar stellen of aanbieden met betrekking tot virtuele waarden die toelaten dat gereglementeerde betaalmiddelen in virtuele waarden worden uitgewisseld;
- het centraal aanspreekpunt gehouden door de Nationale Bank van België overeenkomstig de Wet van 8 juli 2018 houdende organisatie van een centraal aanspreekpunt van bankrekeningen en financiële contracten en tot uitbreiding van de toegang tot het centraal bestand van berichten van beslag, delegatie, overdracht, collectieve schuldenregeling en protest.

Deze medewerking beperkt zich tot:
- het identificeren van de producten en diensten, waarvan de geviseerde persoon titularis, gevolmachtigde of de uiteindelijke gerechtigde is;
- het identificeren van de titularissen, de gevolmachtigden, of de uiteindelijke gerechtigden van de producten en diensten.

De vordering moet schriftelijk gebeuren door het diensthoofd of zijn gedelegeerde. De VSSE en de ADIV moeten een register bijhouden van alle gevorderde identificaties en ze moeten maandelijks een lijst van de gevorderde identificaties overmaken aan het Vast Comité I. Het Comité kreeg daarbij de bevoegdheid om het gebruik van de gegevens te verbieden indien ze verzameld werden in omstandigheden die niet aan de wettelijke bepalingen voldoen.

[174] Het toepassingsgebied van artikel 16/4 W.I&V (bijv. met betrekking tot de bevragingen van de Directie van de politionele informatie en de ICT-middelen (DRI) van de Federale politie) maakt het voorwerp uit van een juridische analyse (2021).

In 2022 werden door de ADIV 9 en door de VSSE 20 vorderingen gedaan.

II.3. DE NIEUWE ROL VAN HET COMITÉ BIJ BESCHERMINGS- EN ONDERSTEUNINGSMAATREGELEN

Het Comité kreeg bij Wet van 14 juli 2022[175] belangrijke taken in het kader van de beschermings- en ondersteuningsmaatregelen die een inlichtingendienst kan aanwenden bij de uitvoering van haar taken.

II.3.1. PLEGEN VAN MISDRIJVEN DOOR AGENTEN, MENSELIJKE BRONNEN EN PERSONEN DIE HUN MEDEWERKING VERLENEN (ART. 13/1, 13/1/1, 13/1/2 EN 13/4 W.I&V)

Inlichtingenagenten of menselijke bronnen kunnen onder strikte voorwaarden strafbare feiten plegen. Een van die voorwaarden vormt doorgaans de goedkeuring door de BIM-Commissie. Indien de Commissie de toestemming weigert, kan het betrokken diensthoofd het Comité vatten dat "*zo spoedig mogelijk al dan niet de toestemming [moet] geven om het strafbaar feit of de strafbare feiten te plegen*." Het Vast Comité I deelt zijn beslissing vervolgens mee aan het diensthoofd en aan de Commissie.

Indien deze Commissie echter had nagelaten binnen de voorziene termijn een beslissing te nemen, kan het diensthoofd alsnog het Comité vatten. Het Comité neemt dan zo spoedig mogelijk een beslissing. Het Comité is ook bestemmeling van alle in dit kader opgestelde documenten. Het wordt ook zo snel mogelijk geïnformeerd wanneer het diensthoofd zelf de maatregel beëindigt.

Indien het Vast Comité I een onwettigheid vaststelt, wordt het betrokken diensthoofd hiervan schriftelijk op de hoogte gesteld. Deze laatste beëindigt zo snel mogelijk de geplande of lopende maatregel en bevestigt vervolgens schriftelijk de beëindiging.

De raadsleden en de medewerkers van het Vast Comité I blijven vrij van straf wanneer zij hun toezicht uitoefenen binnen de toepassing van deze regels.

Deze methode werd in 2022 door de VSSE in vier dossiers aangewend. De ADIV heeft geen gebruik gemaakt van deze methode.

---

175 Wet van 14 juli 2022 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, *B.S.* 5 augustus 2022.

II.3.2. VALSE OF FICTIEVE NAAM OF HOEDANIGHEID (ART. 13/2 W.I&V)

Een agent kan, om veiligheidsredenen verbonden aan de bescherming van zijn persoon of van derden, gebruik maken van een valse of fictieve naam of hoedanigheid. Elk actief gebruik van een fictieve identiteit moet vermeld worden in een lijst die maandelijks overgemaakt wordt aan het Vast Comité I. Tevens dient elke aanmaak van officiële documenten ten bewijze van een fictieve identiteit of hoedanigheid ter kennis worden gebracht van het Comité. Deze regeling geldt sinds 2017. In 2022 werden de lijsten, zoals de wet het voorschrijft, maandelijks toegezonden aan het Vast Comité I.

II.3.3. DE OPRICHTING VAN EEN RECHTSPERSOON (ART. 13/3 W.I&V)

De inlichtingendiensten kunnen ter ondersteuning van hun operaties rechtspersonen oprichten en ten behoeve daarvan valse documenten (laten) vervaardigen en gebruiken. Elke inzet van een rechtspersoon buiten het geval voorzien in artikel 18/13, wordt vermeld in een lijst die maandelijks overgemaakt wordt aan het Vast Comité I. Deze regeling geldt ook sinds 2017.

In 2022 werden de lijsten, zoals de wet het voorschrijft, maandelijks toegezonden aan het Vast Comité I.

II.4. SPECIFIEKE CONTROLE INZAKE VORDERINGEN TOT BEWARING VAN TELECOMGEGEVENS

Het hoeft geen betoog dat identificatie-, verkeers- en lokalisatiegegevens een belangrijke rol spelen in het inlichtingenwerk. Onder meer hiervoor werd destijds in artikel 126 Wet electronische communicatie van 13 juni 2005 (WEC) de dataretentieplicht in het leven geroepen. Aanbieders van openbare telefoniediensten en operatoren van openbare elektronische communicatienetwerken werden hierdoor verplicht om deze gegevens gedurende twaalf maanden bij te houden. Maar met zijn arrest van 22 april 2021 vernietigde het Grondwettelijk Hof deze zogenaamde Dataretentiewet.[176] Het Hof oordeelde dat een algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie het recht schendt op eerbiediging van het privéleven en een inbreuk betekent op de bescherming van persoonsgegevens. Het bewaren van gegevens moet de uitzondering zijn;

176 Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *BS* 18 juli 2016.

alleen een gerichte bewaring die evenredig is met het nagestreefde doel, mag worden toegelaten.

De wetgever reageerde hierop met de Wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten.[177]Wat betreft de VSSE en de ADIV resulteerde dit vooreerst in de artikelen 13/6 en 13/7 W.I&V.

Artikel 13/6 W.I&V geeft de twee diensten de mogelijkheid om een operator van een elektronisch communicatienetwerk of een verstrekker van een elektronische communicatie-dienst te vorderen om over te gaan tot:

- de bewaring van de verkeers- en lokalisatiegegevens van elektronische communicatiemiddelen waarover hij beschikt op het tijdstip van de vordering;
- de bewaring van de verkeers- en lokalisatiegegevens die hij op basis van de vordering genereert en verwerkt.

Deze vordering moet schriftelijke gebeuren door het diensthoofd of zijn gedelegeerde en worden gemotiveerd. De vordering vermeldt de aard van de verkeers- en lokalisatiegegevens die moeten worden bewaard en de personen, groeperingen, geografische gebieden, communicatiemiddelen en/of gebruikswijze waarvan de verkeers- en lokalisatiegegevens moeten bewaard worden evenals de bewaartermijn. Deze bewaartermijn of de duur van de maatregel mag niet langer zijn dan zes maanden te rekenen vanaf de datum van de vordering, onverminderd de mogelijkheid tot verlenging. De inlichtingen- en veiligheidsdiensten moeten een register bijhouden van alle vorderingen. Elke beslissing tot vordering en de motivering ervan moet worden ter kennis gebracht van het Vast Comité I. Indien het Comité een onwettigheid vaststelt, maakt het een einde aan de vordering.

Op basis van artikel 13/7 W.I&V kan ook overgegaan worden tot een algemene en ongedifferentieerde bewaring van gegenereerde en verwerkte verkeers- en lokalisatiegegevens. Er moet echter sprake zijn van een reële en actuele of voorzienbare ernstige dreiging tegen de nationale veiligheid. De inzet van deze methode is aan strikte voorwaarden verbonden. Ze vereist ook een voorafgaand schriftelijk akkoord van de BIM-Commissie. Deze Commissie geeft onverwijld de vraag van het diensthoofd en haar eventueel akkoord door aan het Vast Comité I. De goedgekeurde vordering moet bevestigd worden bij koninklijk besluit. Wanneer de Commissie of het Vast Comité I een onwettigheid vaststelt, wordt een einde gemaakt aan de vordering niettegenstaande de bevestiging bij koninklijk besluit.

Van deze nieuwe mogelijkheden werd in 2022 nog geen gebruik gemaakt.

Tevens dient gewezen te worden op artikel 126/3, § 6 WEC en waarbij ook een rol werd toebedeeld aan het Comité bij de controle op de vaststelling van de geografische zones waarbinnen aan dataretentie kan worden gedaan. Zo zal het Comité de enige bestemmeling zijn van de lijst met de gebouwen bestemd voor rechtspersonen waarvan het economisch en/of wetenschappelijk potentieel beschermd

177 *B.S.* 8 augustus 2022.

moet worden. Deze lijst wordt jaarlijks door de VSSE en de ADIV opgesteld en op voorstel van de minister van Justitie en de minister van Defensie goedgekeurd door de Nationale Veiligheidsraad. De bijgewerkte lijst van de andere zones bedoeld in de paragrafen 3 tot 5 van artikel 126/3 WEC waar een gegevensbewaring verplicht is, wordt ter beschikking gesteld van het Controleorgaan op de politionele informatie (COC) en van het Vast Comité I, elk binnen het kader van zijn bevoegdheden. Het Controleorgaan op de politionele informatie en het Vast Comité I kunnen, elk binnen het kader van hun bevoegdheden, aanbevelingen doen met betrekking tot deze lijsten of het met redenen omklede bevel geven om bepaalde geografische zones van de lijst te schrappen. Deze regeling is nog niet in werking getreden.[178]

II.5. ALGEMENE VASTSTELLINGEN

In vergelijking met het voorgaande jaar 2022, stelt het Vast Comité I een aanzienlijke toename vast bij beide inlichtingendiensten van het aantal ingezette bijzondere inlichtingenmethoden. Als de COVID-periode al een factor was in de vertraging van de activiteiten, heeft de terugkeer naar een relatief normale gezondheidssituatie de operationalisering van de activiteiten van beide diensten zeker vergemakkelijkt. In 2022 zijn de statistieken dan ook weer analoog met deze die sinds 2018 werden geregistreerd.

Tijdens de gedachteuitwisseling met de diensten over deze stijgende tendens, kon het Vast Comité I vaststellen dat de toename van de activiteiten van de diensten ook samenvalt met hun capaciteitstoename, in het bijzonder ten gevolge van het einde van de opleiding van de agenten en hun effectieve invoegetreding binnen de VSSE. In dit verband wijzen zowel de ADIV als de VSSE erop dat een toename van de operationele capaciteit, zowel kwantitatief als kwalitatief, logischerwijs leidt tot een toename van het aantal dossiers en dus van het gebruik van inlichtingenmethoden, of het nu gaat om gewone, specifieke of uitzonderlijke methoden. Ook bepaalde kwesties, zoals de oorlog in Oekraïne of de inmenging in het Europees Parlement, hebben een bijzondere investering gevergd.

In verband met deze laatste vaststelling en onverminderd hetgeen wordt gesteld in de activiteitenverslagen van de diensten - waarnaar wordt verwezen – stelt het Vast Comité I vast dat na de periode van de terroristische aanslagen van 2015-2016, waarin bedreigingen in verband met extremisme en radicalisme veel middelen vroegen, een herschikking heeft plaatsgevonden in het gebruik van bijzondere inlichtingenmethoden ten behoeve van de strijd tegen spionage en inmenging.

Ten slotte maakt de invoering van een nieuwe methodologie binnen de VSSE het zeker mogelijk de onderzoeksprioriteiten doeltreffender te bepalen.

---

178 Deze regeling treedt in werking op de door de Koning bij een besluit vastgesteld na overleg in de Ministerraad bepaalde datum en uiterlijk op 1 januari 2027. In de praktijk, als de Koning niets beslist, zullen de inlichtingendiensten hun lijsten moeten opmaken uiterlijk op 1 januari 2026 (art. 45 Wet 20 juli 2022).

HOOFDSTUK III.

HET TOEZICHT OP BUITENLANDSE INTERCEPTIES, BEELDOPNAMEN EN IT-INTRUSIES

III.1. DE BEVOEGDHEDEN VAN DE ADIV EN DE CONTROLETAAK VAN HET VAST COMITE I[179]

Al in 2017 werd de bevoegdheid van de Algemene Dienst Inlichting en Veiligheid (ADIV) in het kader van de veiligheidsintercepties uitgebreid.[180] De intercepties konden sindsdien voor communicaties '*uitgezonden of ontvangen in het buitenland*'. Deze mogelijkheid geldt voor *quasi* alle opdrachten van de ADIV. Daarbij is het niet onbelangrijk te vermelden dat de opdrachtomschrijvingen zelf, ook werden verruimd. Tegelijkertijd voerde de wetgever twee andere methoden in, te weten de 'intrusie in een informaticasysteem' (art. 44/1 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (W.I&V)) en de 'opname van bewegende beelden' (art. 44/2 W.I&V). En ook de wijze waarop het Comité deze methoden kan controleren, werd gewijzigd.

De controle *voorafgaand* aan de intercepties, intrusies of beeldopnames gebeurt op basis van jaarlijks opgestelde lijsten.[181] Dit betekent dat er naast een jaarlijks interceptieplan, ook een intrusie- en beeldplan dient te worden opgesteld door de ADIV.[182] 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

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

180 Over de opeenvolgende wetswijzigingen inzake de interceptiebevoegdheid van de ADIV, zie VAST COMITÉ I, *Activiteitenverslag 2018*, 61 e.v.

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

182 In deze plannen stelt de ADIV een lijst op van '*organisaties of instellingen die het voorwerp zullen uitmaken van interceptie van hun communicaties, intrusies in hun informaticasystemen of opnames van vaste of bewegende beelden tijdens het komende jaar. Deze lijsten verantwoorden voor iedere organisatie of instelling de reden waarom zij het voorwerp is van een interceptie, intrusie of opname van vaste of bewegende beelden in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°, en vermelden de voorziene duur*' (art. 44/3 W.I&V).

delen aan de ADIV[183] die op zijn beurt de lijsten, voorzien van de toelating van de minister, overzendt aan het Vast Comité I.[184]

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

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

Wat kan het Vast Comité I nu ondernemen indien het een onregelmatigheid vaststelt? Artikel 44/4 W.I&V bepaalt dat het Comité, '*[o]ngeacht de andere bevoegdheden aan dit Comité toegekend op basis van de wet van 18 juli 1991, het recht [heeft] de aan de gang zijnde intercepties, intrusies of beeldopnames te doen stopzetten wanneer blijkt dat ze de wettelijke bepalingen of de [ministeriële] toelating niet respecteren. Het beveelt dat de gegevens die onwettig werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd, volgens de door de Koning te bepalen nadere regels*.' Ondanks de dringende aanbeveling van het Comité[185], werd evenwel nog steeds geen dergelijk interceptie-KB getroffen.[186] Het Comité beveelt dan ook opnieuw aan om dit zo spoedig mogelijk te doen.

183 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.

184 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.

185 VAST COMITÉ I, *Activiteitenverslag 2018*, 129.

186 Het Comité moet zijn beslissing alleszins omstandig motiveren en meedelen aan de minister en aan de ADIV.

III.2. HET IN 2022 VERRICHTE TOEZICHT

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

Het Vast Comité I ontving alle plannen aangaande intercepties, intrusies en beeldopnamen voor 2022 op 23 december 2021. Het Comité kon vaststellen dat de plannen voor 2022 voldeden aan alle wettelijke vereisten.

III.2.2. HET TOEZICHT TIJDENS DE INTERCEPTIE, INTRUSIE OF OPNAME

In 2022 heeft het Vast Comité I geen bezoek gebracht aan de installaties van waaruit de intercepties, intrusies of opnames gebeuren.

Deze verschillende controles zullen het voorwerp uitmaken van een actieplan voor 2023, en dit rekening houdende met de oprichting in oktober 2022 van de nieuwe Component Cyber Command onder commando van de ADIV.

Gegeven dat deze nieuwe component werd aangekondigd om een '*approche intégrée de la sécurité d'information et du renseignement*'[187] in de hele *cyberspace* mogelijk te maken, zal het Comité erover waken om zijn toezicht op de specifieke bepalingen uit de artikelen 44 tot 44/5 inbegrepen W.I&V aan te passen ingevolge deze belangrijke door de ADIV opgestarte reorganisatie.

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

In 2022 heeft het Comité vastgesteld de '*maandelijkse lijsten 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°*' te hebben ontvangen.

187 '*Een geïntegreerde aanpak van de informatieveiligheid en inlichtingen*' (vrije vertaling). J. MATRICHE, *Le Soir*, 18 oktober 2022 ('Cyberspace, le nouveau champ de bataille de l'armée belge').

HOOFDSTUK IV.

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

IV.1. INLEIDING

De Algemene Verordening Gegevensbescherming 2016/679 (AVG)[188] en de Richtlijn 2016/680 (Richtlijn)[189] regelen de wijze waarop publieke en private actoren dienen te handelen wanneer zij persoonsgegevens verzamelen, opslaan, bewaren en doorgeven. Beide Europese instrumenten gaven aanleiding tot enkele belangrijke wetswijzigingen op nationaal vlak: in december 2017 werd de Gegevensbeschermingsautoriteit (GBA)[190] opgericht en in juli 2018 werd een nieuwe Gegevensbeschermingswet (GBW) gestemd.[191] Deze wet wijzigde op zijn beurt de Toezichtwet van 18 juli 1991. Het Vast Comité I werd immers als gegevensbeschermingsautoriteit aangeduid voor verwerkingen van persoonsgegevens die kaderen binnen het domein van de 'nationale veiligheid'.

De rol van het Comité in deze staat omschreven in de Wet tot oprichting van de Gegevensbeschermingsautoriteit (GBA-Wet), in de Gegevensbeschermingswet (GBW) en in de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse (W.Toezicht).[192]

---

188 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.

189 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.

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

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

192 Hierover uitvoerig: VAST COMITÉ I, *Activiteitenverslag 2018*, 75-86.

Artikel 35 §3 W.Toezicht stelt dat het Vast Comité I '*jaarlijks verslag uit[brengt] bij de Kamer van volksvertegenwoordigers omtrent de gegeven adviezen in zijn hoedanigheid van gegevensbeschermingsautoriteit, omtrent de onderzoeken die werden uitgevoerd en de maatregelen die werden genomen in dezelfde hoedanigheid alsook omtrent haar samenwerking met de andere gegevensbeschermingsautoriteiten*'.

In dit hoofdstuk wordt aan die verplichting gevolg gegeven. Het betreft:

- de verificaties die het Comité – alleen of samen met het Controleorgaan voor politionele informatie (COC) of het Vast Comité P – verricht op verzoek van individuele burgers die gebruik wensen te maken van hun recht op onrechtstreekse toegang tot hun 'dossier' bij een van de door het Comité te controleren diensten;
- de juridische adviesverlening van het Comité in het kader van gegevensbescherming.

IV.2. DE BEHANDELING VAN INDIVIDUELE VERZOEKEN

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 het recht om onjuiste persoonsgegevens die op hem betrekking hebben, te laten verbeteren of verwijderen. Hij mag vragen om te laten verifiëren of de toepasselijke regels inzake gegevensbescherming werden nageleefd. Hij mag ook een klacht indienen wegens de eventuele niet-naleving van de regels inzake gegevensbescherming door een verwerkingsverantwoordelijke voor wie het Comité bevoegd is.[193]

Om ontvankelijk te zijn, moet het verzoek geschreven, gedateerd, ondertekend en met redenen omkleed zijn (art 51/2 W.Toezicht).[194] 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.

De onderstaande tabel bevat een overzicht van de in 2022 behandelde dossiers (open en/of afgesloten). De kolommen van de tabel verdelen de verzoeken naargelang het Vast Comité I exclusief bevoegd is dan wel samen met andere toezichthoudende autoriteiten.[195] Het is nuttig om weten dat in onderstaande tabel, een

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

194 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).

195 In de tabel zijn dus niet de hypothesen opgenomen waarin er kon worden samengewerkt met een andere toezichthoudende autoriteiten (bv. het COC) wanneer de bevoegdheden van elke toezichthoudende autoriteit duidelijk zijn onderscheiden.

enkele en zelfde klacht het voorwerp kan uitmaken van verschillende 'dossiers' en dit naargelang de betrokken diensten.[196]

Tabel 1. Behandeling van individuele verzoeken[197]

2022	Vast Comité I		Vaste Comités I en P	Vaste Comités I en P en het COC	Totaal
1. Dossiers geopend in 2022	23		4	0	27
2. Onontvankelijke verzoeken 2022	3		0	0	3
3. Ontvankelijke verzoeken 2022	20		4	0	24
	t. ADIV	17			
	t. VSSE	1			
	t. VSSE&ADIV	2			
4. Lopende dossiers in 2022	25[198]		6[199]	0	31
5. Afgesloten dossiers in 2022[200]	13[201]		2[202]	3[203]	18
6. Corrigerende maatregelen	4		0	0	4
7. Totaal behandelde verzoeken	38		8	3	49

196 Zo zal, bij wijze van voorbeeld, een klacht tegen het OCAD én de VSSE zowel worden opgenomen in de door de Vaste Comités P en I gemeenschappelijk behandelde dossiers voor wat betreft het OCAD-luik van het dossier als bij de dossiers die uitsluitend door het Vast Comité I worden behandeld voor wat betreft onderzoeksdaden met betrekking tot de VSSE.

197 De eerste regel geeft aan hoeveel dossiers er in 2022 werden geopend. Regels 2 en 3 verdelen de dossiers ingediend in 2022 naargelang de beslissing tot ontvankelijkheid of onontvankelijkheid. Voor wat betreft de dossiers dewelke alleen door het Vast Comité I worden behandeld, preciseert regel 3 nog de verdeling tussen de betrokken diensten voor wat betreft de ontvankelijke dossiers (ingediend in 2022). De regels 4 en 5 tonen de vooruitgang van de in 2022 behandelde dossiers aan (nog lopende of reeds afgesloten). Regel 6 ten slotte geeft het aantal dossiers aan waarin door het Comité corrigerende maatregelen werden opgelegd.

198 Waarvan twee dossier geopend in 2021.

199 Waarvan twee dossiers geopend in 2021.

200 In het verleden werd door het Vast Comité I een dossier als afgesloten beschouwd op het ogenblik dat kon worden vastgesteld dat de opgelegde corrigerende maatregelen werden uitgevoerd. In 2022 brachten uitwisselingen tussen het Comité en de inlichtingendiensten over in verschillende dossiers opgelegde corrigerende maatregelen aan het licht dat de uitvoering ervan vertraging kon oplopen. Vandaar dat vanaf heden een dossier als afgesloten wordt beschouwd van zodra de verzoeker op de hoogte werd gebracht van de conclusies van het Comité en dat de eventuele opgelegde corrigerende maatregelen per brief werden meegedeeld aan de betrokken inlichtingendienst(en). Bijgevolg zijn dubbeltellingen mogelijk tussen de cijfers van 2021 en 2022 (regel 6).

201 Waarvan één dossier geopend in 2019, één dossier geopend in 2020 en 6 dossiers geopend in 2021.

202 Waarvan één dossier geopend in 2020 en één dossier geopend in 2021.

203 Waarvan één dossier geopend in 2020.

In 93% van de verzoeken behandeld in 2022 beweren de betrokkenen[204] dat er sprake is van concrete inmenging in hun rechten en vrijheden als gevolg van, of minstens in verband met, een verwerking van gegevens door een verwerkingsverantwoordelijke die onder de bevoegdheid van het Vast Comité I valt. Van een dergelijke inmenging zou bijvoorbeeld sprake zijn in het kader van een procedure van nationaliteitsverklaring waarbij een inlichtingendienst informatie verstrekt aan het Openbaar Ministerie, wanneer de betrokkene beweert dat hij regelmatig door de politie wordt gecontroleerd, wanneer hij vaststelt dat hem de toegang tot een grondgebied werd geweigerd, wanneer gegevens van een inlichtingendienst werden gebruikt in strafrechtelijke procedures, enz.

Net als in 2021, diende het Comité in 2022 verschillende verzoeken te behandelen die waren ingediend in het kader van de aanvraag tot verkrijging van de nationaliteit of een verblijfstitel. Geconfronteerd met een negatief besluit op basis van door de Veiligheid van de Staat (VSSE), de Algemene Dienst Inlichting en Veiligheid (ADIV) en/of het Coördinatieorgaan voor de dreigingsanalyse (OCAD) verstrekte informatie, wenden verzoekers zich (onder meer) tot het Vast Comité I voor een controle van de verwerking van hun persoonsgegevens.

De resterende 7% aan verzoeken bestaat uit aanvragen tot indirecte uitoefening van rechten, zonder bijzondere precisering of concrete grief. Doorgaans vraagt de betrokkene zich af of gegevens over hem of haar worden verwerkt en of de verwerking in overeenstemming is met de toepasselijke regelgeving (indirecte toegang).

Die onevenwicht[205] hoeft niet te verbazen, daar het antwoord dat wordt gegeven aan de betrokkene die zijn rechten uitoefent geen informatie bevat over hoe het staat met de (eventuele) verwerking van zijn persoonsgegevens door de diensten waarvoor het Comité bevoegd is. Alleen wanneer de betrokkene het bestaan vermoedt of concreet de gevolgen ondergaat van een dergelijke gegevensverwerking, heeft hij of zij er belang bij zich tot het Vast Comité I te wenden opdat het de nodige verificaties zou verrichten, in de hoop een verbetering van de situatie te verkrijgen.

Het Vast Comité I legde als toezichthoudende autoriteit in 2022 ten aanzien van de inlichtingendiensten corrigerende maatregelen op in vier dossiers (art. 51/3 W.Toezicht). Afhankelijk van het dossier, kan dit inhouden dat wordt verzocht om rectificatie of schrapping van de persoonsgegevens, dat de beslissing van het Comité ter kennis wordt gebracht van de partners en/of de autoriteiten, of dat de beslissing binnen de betrokken dienst wordt verspreid.

---

204 Op te merken valt dat, in meerdere dossiers, dergelijke gevallen van inmenging niet alleen worden gemeld door de betrokkenen, maar door hen ook worden gestaafd en bewezen (bijv. door analysenota's te bezorgen waarover de betrokkenen beschikken in het kader van de procedures waarin deze nota's worden gebruikt door de publieke autoriteiten). In andere gevallen zijn die beweringen vermoedens die min of meer of helemaal niet worden gestaafd.

205 In 2021 was dit onevenwicht 85% versus 15%.

IV.3. ADVIESVERLENING

Het Comité kan in twee gevallen een advies uitbrengen '*over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin beleidslijnen van de bevoegde ministers worden geformuleerd*': wanneer de wet zijn advies vereist of op verzoek van de Kamer van volksvertegenwoordigers of van de bevoegde minister (artikel 33, lid 8 W. Toezicht). Dergelijk advies heeft specifiek betrekking op de problematiek van de gegevensverwerking en moet dus onderscheiden worden van de algemene adviesbevoegdheid die bijvoorbeeld ook betrekking kan hebben op de efficiëntie en de coördinatie (cf. Hoofdstuk VI. Adviezen). 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.
Het Comité heeft in 2022 in vier adviezen verleend in deze hoedanigheid:
- Advies 001/VCI/2022 van 20 april 2022 aangaande de 'maritieme veiligheid';
- Advies 002/VCI/2022 van 29 juni 2022 over de toegang tot de databank E-PV;
- Advies 003/VCI/2022 van 29 juni 2022 over de gegevensbescherming m.b.t. de Dienst Vreemdenlingenzaken en doorgifte van persoonsgegevens aan de VSSE en de ADIV;
- Advies 004/VCI/2022 van 29 juni 2022 over de screening van buitenlandse directe investeringen en de rol van de VSSE en de ADIV hierbinnen.

Al deze adviezen werden samengevat in Hoofdstuk VI van voorliggend activiteitenverslag en zijn integraal beschikbaar op de website van het Vast Comité I.[206]

[206] www.comiteri.be

IV.4. DE MELDING VAN EEN MOGELIJKE DATA BREACH

De door het Vast Comité I gecontroleerde diensten moeten een hele reeks gegevens ter beschikking houden of stellen van het Comité.[207] Zo moet de verwerkingsverantwoordelijke binnen de kortste termijn en indien mogelijk binnen de 72 uur nadat hij er kennis van heeft gekregen, melding maken van eender welke inbreuk op de beveiliging die aanleiding kan geven tot een hoog risico voor de rechten en vrijheden van natuurlijke personen (artt. 89, 122, 155 en 180 GBW).

In 2022 werd geen dergelijke inbreuken op de beveiliging *(data breaches)*[208] aan het Comité gemeld.

[207] Niet elke dienst moet alle hier vermelde gegevens bijhouden of ter beschikking stellen. Dit geldt bijvoorbeeld zeker wat betreft de BIM-Commissie die geen informatie moet meedelen aan het Vast Comité I.

[208] Onder 'inbreuk op de beveiliging' wordt verstaan: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens (art. 26, 11° GBW).

HOOFDSTUK V.

DE CONTROLE VAN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN

In 2016 werd door de ministers van Binnenlandse Zaken en Justitie de gemeenschappelijke gegevensbank '*foreign terrorist fighters*' opgericht. Deze gemeenschappelijke gegevensbank (GGB) werd in 2018 omgevormd: ze heet voortaan gemeenschappelijke gegevensbank '*terrorist fighters*' (GGB TF) en omvat naast de algemene categorie van de '*foreign terrorist fighters*' tevens een categorie van '*homegrown terrorist fighters*'. Daarnaast werd in 2018 ook een aparte gemeenschappelijke gegevensbank opgericht voor '*haatpropagandisten*' (GGB HP). Bij koninklijk besluit van eind 2019 werden nog twee bijkomende categoriën van personen in de GGB TF opgenomen, zijnde de 'potentieel gewelddadige extremisten' (PGE) en 'terrorisme-veroordeelden' (TV).

Artikel 44/11/3*quinquies*/2 WPA vertrouwt het toezicht op de verwerking van de in de GGB vervatte informatie en persoonsgegevens toe aan het Controleorgaan op de politionele informatie (COC) en aan het Vast Comité I.

Sinds het laatste verslag[209] van het COC en het Vast Comité I over dit onderwerp werden geen wijzigingen in de wet- of regelgeving opgetekend.

In februari 2022 ging een nieuwe versie van de GGB TF en HP in productie. Deze versie heeft een aanzienlijk gewijzigde *interface* alsook een aantal nieuwe functionaliteiten.

V.1. DE CONTROLEOPDRACHT EN HET VOORWERP VAN CONTROLE

Het COC en het Vast Comité I besloten voor het jaar 2022 hun gezamenlijk toezicht toe te spitsen op de follow-up van enkele eerdere aanbevelingen en op het gebruik van gemeenschappelijke databanken door de inlichtingen- en veiligheids-

[209] COC en VAST COMITÉ I, *Verslag betreffende de gezamenlijke controle van de gemeenschappelijke gegevensbanken terrorist fighters en haatpropagandisten door het Vast Comité I en het Controleorgaan op de politionele informatie*, 2020, 34 p. (Beperkte verspreiding (K.B. 20 maart 2000). Het verslag werd door de toezichthoudende autoriteiten goedgekeurd op 12 augustus 2021.

diensten. Tevens werd de opvolging van de aanbevelingen van het in 2021 uitgevoerde toezichtonderzoek naar de radicalisering van een lid van de Defensie[210] in de evaluatie opgenomen.

De betrokken diensten, zijnde de Federale Politie, de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV), werden per brief op de hoogte gebracht van deze controle. De diensten werden schriftelijk bevraagd en bij de Federale Politie werd een uittreksel van de logboekgegevens aangaande de verwerkingsactiviteiten uitgevoerd door de twee inlichtingen- en veiligheidsdiensten opgevraagd.

Het verslag is voorzien voor de eerste helft van 2023.

V.2. DE ADVIESOPDRACHT

De Wet op het politieambt (WPA) voorziet verder ook in de verplichting om een gemeenschappelijk advies van het Vast Comité I het COC in te winnen en dit naargelang verschillende hypotheses.

Zo moeten de ministers van Binnenlandse Zaken en Justitie, voorafgaand aan de oprichting van een gemeenschappelijke gegevensbank alsook van de verwerkingsmodaliteiten, waaronder deze met betrekking tot de registratie van de gegevens en van de verschillende categorieën en types van persoonsgegevens en informatie die verwerkt worden, hiervan aangifte doen bij het Vast Comité I en het COC. Deze dienen op hun beurt een gezamenlijk een advies uit te brengen (art.44/11/3*bis* §3 WPA). Daarnaast bepaalt, na advies van bovenvernoemde controleorganen, voor elke gemeenschappelijke gegevensbank een koninklijk besluit vastgesteld na overleg in de Ministerraad, de types van verwerkte persoonsgegevens, de regels op het gebied van de verantwoordelijkheden op het vlak van de bescherming van de persoonlijke levenssfeer van de organen, diensten, overheden en organismen die gegevens verwerken, de regels op het gebied van de veiligheid van de verwerkingen, de regels van het gebruik, de bewaring en de uitwissing van de gegevens (art.44/11/3*bis* §4 WPA). Verder kunnen bijkomende beheersregels van de gemeenschappelijke gegevensbanken worden bepaald door een koninklijk besluit vastgesteld na overleg in de Ministerraad, evenwel ook hier na advies van het Comité en het COC (art.44/11/3*bis* §8 WPA). Ten slotte strekt de adviesfunctie zich tevens uit tot elk ontwerp van koninklijk besluit tot instelling of wijziging van de toegang tot de gemeenschappelijke gegevensbanken (art.44/11/3*ter* §§2 tot 4 WPA).

Het Vast Comité I en het COC werden in 2022 niet om een dergelijk advies verzocht.

---

210 Toezichtonderzoek naar het opsporen en het opvolgen – door de twee inlichtingendiensten- van de radicalisering van een militair werkzaam bij Defensie, en anderzijds naar hun samenwerking met hun partnerdiensten, waaronder Defensie, onder meer wat betreft hun informatie-uitwisseling, 1 juli 2021 (www.comiteri.be).

HOOFDSTUK VI.
ADVIEZEN

Artikel 33 van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse (W.Toezicht) bepaalt dat het Comité '*enkel op verzoek van de Kamer van volksvertegenwoordigers of van de bevoegde minister advies [mag] uitbrengen over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin de beleidslijnen van de bevoegde ministers worden geformuleerd*.'

Daarnaast dient het Comité ook advies te verlenen 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 Controleorgaan op de politionele informatie (COC).

In 2022 werd het Comité zeven maal om advies verzocht.[211] Drie maal werd door de ministers rechtstreeks bij het Comité om advies verzocht: door de minister van Ambtenarenzaken over de klokkenluidersregeling voor de publieke sector (VI.5) en door de minister van Defensie over de screening van (kandidaat-)personeelsleden van Defensie (VI.6). Wat dat laatste advies betreft, werd, voor het eerst, door de minister ook om advies verzocht van de Voorzitter van het Beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. De minister van Binnenlandse Zaken verzocht de Vaste Comités I en P om advies inzake de Directie Integriteitsbeoordelingen voor Openbare Besturen (DIOB).[212]

In vier andere gevallen, kwam het verzoek om advies door het Vast Comité I via de Gegevensbeschermingsautoriteit (GBA) : door de minister van Justitie en van de Noordzee over een voorontwerp van wet inzake maritieme veiligheid (VI.1), door de staatssecretaris voor Asiel en Migratie aangaande de uitwisseling van persoonsgegevens door de Dienst Vreemdelingenzaken en de inlichtingendiensten (VI.3) en ten slotte twee maal door de minister van Economie en Werk over enerzijds de toegang tot de databank e-PV (VI.2) en anderzijds de screening van buitenlandse investeringen (VI.4).

---

211 Het Comité wordt steeds meer om advies gevraagd op basis van artikel 33 W.Toezicht; de hieraan geïnvesteerde tijd is bijgevolg dan ook opmerkelijk gestegen.

212 De federale Ministerraad keurde op 14 september 2022 het wetsontwerp *"betreffende de gemeentelijke bestuurlijke handhaving, instelling van gemeentelijk integriteitsonderzoek en houdende oprichting van een Directie Integriteitsbeoordeling voor Openbare Besturen"* goed, waarna de minister van Binnenlandse Zaken hieromtrent opnieuw om een advies vroeg. Er werd door de Vaste Comités P en I besloten te verwijzen naar een eerder geformuleerd advies (17 september 2020) hierover (cf. www.comiteri.be). Het advies werd niet hernomen in voorliggend hoofdstuk.

Alle adviezen, die hieronder werden opgenomen in chronologische volgorde, zijn intregraal consulteerbaar op de website van het Comité.[213]

VI.1. ADVIES OVER MARITIEME BEVEILIGING[214]

Eind februari 2022 bezorgde Gegevensbeschermingsautoriteit aan het Vast Comité I een verzoek tot advies van de minister van Justitie en van de Noordzee met betrekking tot het voorontwerp van wet tot wijziging van de Wet van 8 mei 2019 tot invoering van het Belgisch Scheepvaartwetboek.

Het voorontwerp stelde dat de samenstelling en de werking van de Nationale Autoriteit voor Maritieme Beveiliging (NAMB) wordt bepaald bij koninklijk besluit. De memorie van toelichting verduidelijkte evenwel dat *"(a)lvast de volgende diensten (…) deel (zullen) uitmaken van de NAMB: DG Scheepvaart, NCCN, OCAD, Federale Politie/Scheepvaartpolitie, Douane en Accijnzen, Defensie, ADIV en Staatsveiligheid"*. Het Comité stelde aldus vast dat de VSSE, de ADIV en het OCAD uitdrukkelijk vernoemd werden als NAMB-leden. Voor wat betreft de VSSE en de ADIV lag dit lidmaatschap in de lijn van gelijkaardige deelnames aan overlegplatformen belast met de beveiliging binnen het domein 'mobiliteit en vervoer', meer bepaald in de Nationale Autoriteit voor de Beveiliging van het Spoorwegvervoer[215] en het Nationaal Comité voor de Veiligheid der Burgerlijke Luchtvaart.[216] Het voorontwerp stelde dat de samenstelling en de werking van de Lokale Comités voor Maritieme Beveiliging (LCMB) eveneens bepaald zou worden door de Koning. Ook hier verduidelijkte de memorie van toelichting dat *"(e)en LCMB zal bestaan uit minstens vertegenwoordigers van de Federale Politie/Scheepvaartpolitie, Lokale Politie, Douane en Accijnzen, DG Scheepvaart, Defensie, ADIV en vertegenwoordigers van de regionale entiteiten die de havens of waterwegen exploiteren"*. Het was voor het Comité evenwel onduidelijk waarom de ADIV eveneens deel zou moeten uitmaken van dergelijke lokale comités.

Het Comité beveelde verder aan om het voorstel van artikel te schrappen waarin wordt bepaald dat *"De NAMB kan optreden als veiligheidsofficier voor het aanvragen van de veiligheidsmachtigingen bedoeld in het eerste lid."* Het Comité herinnerde de regering er immers aan dat de functie van 'veiligheidsofficier' zoals bedoeld in de Wet van 11 december 1998 (artikel 13, 1°) een fysiek persoon is. Binnen het aanvragen van veiligheidsmachtigingen oefent een dergelijke veiligheidsofficier de

213 www.comiteri.be

214 Advies nr. 001/VCI/2022 van 20 april 2022 over de maritieme veiligheid, 5 p.

215 *Cf.* artikel 4 van het koninklijk besluit van 26 januari 2006 tot oprichting van een nationale Autoriteit voor de beveiliging van het spoorwegvervoer en houdende diverse maatregelen voor de beveiliging van het intermodaal vervoer.

216 *Cf.* artikel 3 van het koninklijk besluit van 20 juli 1971 betreffende de oprichting van een nationaal comité voor de veiligheid der burgerlijke luchtvaart en van plaatselijke comités voor de veiligheid der luchthavens.

verbinding uit tussen de instantie waartoe hij/zij behoort en de Nationale Veiligheidsoverheid (NVO) die belast is met de afgifte van veiligheidsmachtigingen.

Het Comité bracht tevens in herinnering dat het digitaal ISPS[217]-platform dat gebruikt wordt voor *"de opslag, opvolging en goedkeuring van alle […] vermelde beveiligingsbeoordelingen"* en ook aangewend wordt voor *"het uitwisselen van informatie tussen de betrokken actoren"*, geen geclassificeerde gegevens afkomstig van de VSSE, de ADIV en het OCAD mag bevatten. Voor wat betreft het gebruik van dit platform voor *"het bijhouden van de lijst van leden van de NAMB"*, bracht het Comité de gevoelige aard van de naam van de leden van de VSSE, de ADIV en het OCAD onder de aandacht. Er werd geadviseerd om betrokken agenten louter te identificeren aan de hand van hun door hun dienst verstrekte identificatienummer.

Ten slotte belastte het voorontwerp de VSSE, de ADIV en het OCAD – als leden van de Nationale Autoriteit voor Maritieme Beveiliging – *"met het toezicht op de naleving van de ISPS-Verordening […]"* van het Scheepvaartwetboek *"en de desbetreffende uitvoeringsbesluiten"*. Het Comité adviseerde negatief om de VSSE, de ADIV en het OCAD te belasten met een dergelijke taakstelling. De VSSE en de ADIV zijn inlichtingen- en veiligheidsdiensten. Het OCAD is een orgaan voor de dreigingsanalyse. Een opdracht tot toezicht op de naleving van straf- en bestuurswetten en de opsporing van inbreuken is tegenstrijdig met hun huidige opdrachten. Eventuele inbreuken door betrokken diensten gedurende de uitoefening van hun inlichtingen- en veiligheidsopdrachten dienen logischerwijs wel aan het Openbaar Ministerie gemeld te worden op grond van de ambtelijke aangifteplicht bedoeld in artikel 29 Sv.

Ondertussen werd de Wet van 13 oktober 2022 tot wijziging van het Belgisch Scheepvaartwetboek betreffende de maritieme beveiliging gepubliceerd[218] en trad deze in werking op 1 januari 2023.

VI.2. ADVIES OVER DE TOEGANG TOT DE DATABANK E-PV

Het Vast Comité I werd in mei 2022 via de Gegevensbeschermingsautoriteit (GBA) door de minister van Economie en Werk om advies verzocht over het voorontwerp van wet tot wijziging van het Sociaal Strafwetboek (Soc.Sw.) met het oog op de oprichting van het eDossier-platform (hierna het wetsontwerp).[219] Het wetsontwerp voorzag, onder andere, in de toegang voor de VSSE en de ADIV tot de databank e-PV waarin de processen-verbaal tot vaststelling van inbreuken van sociale inspecteurs worden verzameld.

---

217 *International Ship and Port Facility Security.*
218 *B.S.* 26 oktober 2022.
219 Advies nr. 002/VCI/2022 van 29 juni 2022 over de toegang tot de databank e-PV, 10 p.

VI.2.1. LEGITIMATIE VAN EEN TOEGANGSRECHT

Het Comité onderschrijft de installatie van een toegangsrecht tot de databank e-PV voor zowel de VSSE, de ADIV en, binnen de hierna besproken aangelegenheden[220], de Federale Politie.[221] Het Comité is immers van oordeel dat een dergelijk toegangsrecht niet enkel van belang is binnen de uitvoering van veiligheidsverificaties (door de VSSE, de ADIV en de Federale Politie in opdracht van de NVO), maar eveneens een belangrijk instrument kan vormen binnen de uitvoering van de (andere) inlichtingen- en veiligheidsopdrachten van de VSSE en de ADIV.

VI.2.2. BIJZONDERE REGELING TOEGANGSRECHT INLICHTINGENDIENSTEN

In zijn advies begon het Comité met de herinnering aan artikel 14 W.I&V dat de informatiedoorstroming van de gerechtelijke en bestuurlijke overheden naar de VSSE en de ADIV regelt. Deze bepaling stelt immers dat: "*[m]et inachtneming van de geldende wetgeving kunnen de inlichtingen- en veiligheidsdiensten, overeenkomstig de door de Koning vastgelegde algemene nadere regels, toegang krijgen tot de gegevensbanken van de openbare sector die nuttig zijn voor de uitoefening van hun opdrachten*." (art. 14, laatste § W.I&V). Hierin stelt de wetgever verder dat, ingeval de VSSE en/of de ADIV over een toegangsrecht tot een publieke gegevensbank beschikt, door de Koning bepaalde bijzondere voorschriften indachtig gehouden dienen te worden.

Bij koninklijk besluit van 2 oktober 2019, werden deze bijzondere voorschriften nader bepaald.[222] Deze voorzien, onder meer, in het bijhouden in de schoot van de inlichtingen- en veiligheidsdiensten, van een register van personen die beschikken over een rechtstreekse toegang tot de gegevensbank in kwestie alsook de verwerkingen die worden uitgevoerd door de diensten. Deze regels zijn dan ook van toepassing voor een eventuele toegang van de ADIV en de VSSE tot de gegevensbank e-PV.

---

220 Het Comité beperkt zich tot de werking van de Classificatiewet, regelgeving waarin het door de wetgever werd aangewezen als bevoegde gegevensbeschermingsautoriteit.

221 Het Comité bracht hierbij in herinnering dat de behoefte tot een dergelijk toegangsrecht voor alle drie vernoemde diensten reeds bij koninklijk besluit werd bekrachtigd voor wat betreft de door de VSSE, de ADIV en de Federale politie gedane informatiegaring in het kader en ten dienste van de door de Nationale Veiligheidsoverheid (NVO) uitgevoerde veiligheidsverificaties - Artikel 3, laatste lid KB 8 mei 2018 *juncto* artikel 21 KB 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, de veiligheidsattesten en de veiligheidsadviezen.

222 Koninklijk besluit van 2 oktober 2019 tot wijziging van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst.

VI.2.3. ONTWORPEN ARTIKEL 100/10, § 5 SOC.SW.

De creatie van een toegangsrecht van de VSSE, de ADIV en, voor wat betreft het uitvoeren van veiligheidsverificaties, de Federale Politie, dient zich in te schakelen in het ontworpen artikel 100/10, §5 Soc.Sw. In zijn advies suggereerde het Comité om het ontwerp van artikel aan te vullen met een verwijzing naar de W.I&V opdat de toegang tot de in de databank e-PV opgenomen gegevens zou worden uitgebreid tot de inlichtingen- en veiligheidsdiensten.

Het Comité wees tevens op de memorie van toelichting bij artikel 17, 4° van het Wetsontwerp die de vervanging van artikel 100/10, §5 Soc.Sw. als volgt rechtvaardigt : *"Het gaat om het preciseren van de toegang tot de gegevens van de databank e-PV voor een wettige en proportionele verwerking in het licht van de passende finaliteit(en) en berustend op een wettelijke basis om in overeenstemming te zijn met de voorschriften van de reglementering betreffende de gegevensbescherming naargelang de categorieën van de verwerkte gegevens."*

Het Comité diende aldus vast te stellen dat de wetgever ervoor opteerde om de gegevensbeschermingsvoorschriften in hoofde van de VSSE en de ADIV niet te integreren in de Inlichtingenwet van 30 november 1998, doch wel in een apart hoofdstuk in de Gegevensbeschermingswet van 30 juli 2018 (hierna GBW).[223]

De artikelen 76 en 110 GBW stellen dat *"in het belang van de uitoefening van hun opdrachten"* de VSSE, de ADIV en, voor o.m. wat betreft (o.m.) de veiligheidsverificaties, de Federale Politie *"persoonsgegevens van alle aard (verwerken), inbegrepen die waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging of het lidmaatschap van een vakvereniging blijken, alsook genetische en biometrische gegevens, gezondheidsgegevens, 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."*

In tegenstelling tot de (opgeheven) Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens (*juncto* artikel 14 Classificatiewet), kunnen de betrokken diensten voortaan gezondheidsgegevens verwerken in het kader van veiligheidsverificaties en -onderzoeken. Het Comité wees er niettemin op dat dient dit te gebeuren met respect voor de wettelijke kwaliteitseisen waaraan elke verwerking van persoonsgegevens cumulatief moet voldoen (cf. artikelen 75 en 109 GBW).

---

223 De gegevensbeschermingsvoorschriften van toepassing gedurende de inlichtingen- en veiligheidsopdrachten van de VSSE en de ADIV opgesomd worden in de artikelen 72 tot 104 GBW (titel 3, ondertitel 1). Deze van toepassing gedurende het uitvoeren van veiligheidsverificaties vindt men terug in de artikelen 106 tot 137 GBW (titel 3, ondertitel 3).

VI.3. ADVIES OVER DE GEGEVENSBESCHERMING M.B.T. DE DIENST VREEMDELINGENZAKEN EN DOORGIFTE VAN PERSOONSGEGEVENS AAN VSSE EN ADIV

In juni 2022 werd via de Gegevensbeschermingsautoriteit (GBA) aan het Vast Comité I een verzoek tot advies overgemaakt van de Staatssecretaris voor Asiel en Migratie met betrekking tot het voorontwerp van wet betreffende de verwerkingen van persoonsgegevens door de Algemene Dienst Vreemdelingenzaken van de Federale Overheidsdienst Binnenlandse Zaken (DVZ).[224]

VI.3.1. DE DOORGIFTE VAN PERSOONSGEGEVENS VAN DE DVZ AAN DE VSSE EN/OF DE ADIV

Het Comité kon vaststellen dat het ontwerp een ruime opsomming bevatte van de categorieën van persoonsgegevens die door de Dienst Vreemdelingenzaken (DVZ) verwerkt kunnen worden. Krachtens het ontwerp mag de DVZ bedoelde gegevens overmaken aan de VSSE respectievelijk de ADIV. Een dergelijke doorgifte van persoonsgegevens dient te geschieden, *dixit* betrokken bepalingen, "*met het oog op a) de uitvoering van zijn wettelijke opdrachten*" – m.b.t. de opdrachten van de VSSE of de ADIV – en/of "*b) de evaluatie door de Dienst Vreemdelingenzaken van de dreiging voor de openbare orde en de nationale veiligheid*". De memorie van toelichting (pag. 66 en 67) bij deze bepalingen verduidelijkt: *"De uitwisseling van persoonsgegevens met de Staatsveiligheid stelt de Dienst Vreemdelingenzaken ook in staat om na te gaan of een vreemdeling mogelijk een gevaar vormt voor de openbare orde en/of de nationale veiligheid.*"

VI.3.2. DE MEDEDELING DOOR DE VSSE EN/OF DE ADIV AAN BUITENLANDSE INLICHTINGENDIENSTEN VAN GEGEVENS AFKOMSTIG VAN DE DVZ

In zijn advies bracht het Comité in herinnering dat de bij de VSSE en de ADIV beschikbare persoonsgegevens slechts onder beperkte voorwaarden mogen doorgegeven worden aan landen die geen lid zijn van de Europese Unie of aan internationale organisaties (cf. artikelen 126 en 127 Gegevensbeschermingswet[225]). Ook de persoonsgegevens verkregen van de Dienst Vreemdelingenzaken kunnen niet

224 Advies nr. 003/VCI/2022 van 29 juni 2022 over de gegevensbescherming m.b.t. de Dienst Vreemdelingenzaken en doorgifte van persoonsgegevens aan de VSSE en ADIV, 5 p.

225 Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (hierna: Gegevensbeschermingswet of GBW).

zonder meer worden doorgegeven aan derde landen en zijn onderhevig aan een restrictief regime.

Het wettelijk kader voor (inter)nationale samenwerking en uitwisseling van informatie wordt, daarnaast, eveneens gevormd door de artikelen 19, eerste lid en 20 §3 W.I&V. Artikel 19, eerste lid W.I&V regelt de algemene bevoegdheid tot mededeling en doorgifte van inlichtingen aan derde instanties.[226] De wetgever was in 1998 echter zelf de mening toebedeeld dat deze bepaling onvoldoende is. Daarom schrijft artikel 20 §3 W.I&V voor dat de Nationale Veiligheidsraad (NVR), onder meer, de internationale samenwerking en informatie-uitwisseling verder moet uitwerken.

Via de Richtlijn van 30 september 2016 heeft de Nationale Veiligheidsraad aan deze wettelijke plicht (deels) voldaan.[227] Deze NVR-richtlijn de modaliteiten regelt van de internationale doorgifte van persoonsgegevens door de VSSE en de ADIV.[228]

In het licht van de naleving van artikel 8.2 EVRM inzake het recht op eerbiediging voor de persoonlijke levenssfeer, stuurde het Comité aan om de basisprincipes van de Richtlijn van de Nationale Veiligheidsraad vast te leggen in een wet. Het Comité adviseerde bijgevolg om de installatie van artikel 11, §1, 32° en 33° van het wetsontwerp te koppelen aan een dergelijke uitwerking.

Vanuit zijn hoedanigheid van gegevensbeschermingsautoriteit binnen het nationale veiligheidsdomein, nodigde het Comité de regering en de beide inlichtingendiensten uit om werk te maken van het opstellen van een wetsontwerp om de huidige situatie te remediëren opdat de internationale informatie-uitwisseling door de inlichtingendiensten terug op een verdragsconforme wijze kan plaatsvinden.[229]

---

226 Artikel 19, eerste lid W.I&V: *"De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook aan de instanties en personen die het voorwerp zijn van een dreiging bedoeld in de artikelen 7 en 11"*.

227 De Richtlijn van 30 september 2016 van de Nationale Veiligheidsraad 'aangaande de relaties van de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichtingen en Veiligheid (ADIV) met buitenlandse inlichtingendiensten'.

228 Er werd geopteerd om deze NVR-richtlijn te classificeren (niveau Vertrouwelijk). Het Comité begrijpt niet waarom dit document dient geclassificeerd te worden. Het betrokken document bevat geen operationele gegevens, noch operationele methodologieën, noch andersoortige gevoelige gegevens. Te meer omdat de NVR-richtlijn een onderdeel vormt van het juridisch toetsingskader voor het internationaal handelen van de inlichtingen- en veiligheidsdiensten, zijn er volgens het Comité geen redenen om een dergelijk document blijvend te classificeren.

229 Het Comité bracht op 28 september 2020 over het Wetsvoorstel 'tot wijziging van de wet van 30 november 1998 houdende regeling van inlichtingen- en veiligheidsdiensten met het oog op het invoeren van wegingsnotities voor de samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten' (www.comiteri.be).

VI.4. ADVIES OVER DE SCREENING VAN BUITENLANDSE DIRECTE INVESTERINGEN EN ROL VAN DE VSSE EN DE ADIV HIERBINNEN

In juni 2022 werd het Vast Comité I via de Gegevensbeschermingsautoriteit (GBA) door de minister van Economie verzocht een advies te geven over het voorontwerp van wet houdende instemming met het Samenwerkingsakkoord van 1 juni 2022 tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen.[230] Het doel van het Samenwerkingsakkoord bestaat uit het vrijwaren van de nationale veiligheid, de openbare orde en de strategische belangen van de deelstaten die kaderen binnen hun materiële bevoegdheden en dit door middel van de screening van bepaalde buitenlandse directe investeringen.

Het ontwerp had meer in het bijzonder betrekking op verwerkingen van persoonsgegevens door de Veiligheid van de Staat (VSSE) en/of de Algemene Dienst Inlichting en Veiligheid (ADIV). Artikel 13 van het Samenwerkingsakkoord voorziet inderdaad dat de twee inlichtingen- en veiligheidsdiensten (naast andere openbare diensten) in het kader van de toetsings- en screeningsprocedures van buitenlandse investeerders om advies zullen worden gevraagd.[231]

In zijn advies merkte het Comité op dat noch de tekst van het Samenwerkingsakkoord zelf noch de door de adviesaanvrager bijgevoegde documenten enige duidelijkheid omvatte omtrent de aard en omvang van het door de VSSE/ADIV uit te voeren screeningsonderzoek dat voorafgaat aan het formuleren van een advies. Het Comité identificeerde meerdere vragen, waarvan de antwoorden de aard en omvang van het uiteindelijke screeningsonderzoek van de Interfederale Screeningscommissie zullen bepalen, en zodoende van de verstrekkendheid van de door de Belgische overheid uitgevoerde controle op bedoelde buitenlandse directe investeringen. Zoals bijvoorbeeld:

- Wordt enkel een databankverificatie van de inlichtingendiensten verwacht?
- Dienen de bij de inlichtingendiensten ter beschikking staande inlichtingen en persoonsgegevens te worden bijgewerkt en geactualiseerd wanneer ze in het licht van een beoordeling van een buitenlandse directe investering als onvoldoende worden beschouwd?

---

230 Advies nr. 004/VCI/2022 van 29 juni 2022 over de screening van buitenlandse directe investeringen en de rol van de VSSE en de ADIV hierbinnen, 6 p.

231 Zo dient er een advies gevraagd te worden aan de ADIV wanneer buitenlandse investeerders "*1° actief is/zijn in defensie-gerelateerde sectoren; 2° actief is/zijn in de sector goederen voor tweeerlei gebruik in de zin van artikel 2, lid 1, van Verordening (EG) nr. 428/2009 van de Raad van 5 mei 2009 tot instelling van een communautaire regeling voor controle op de uitvoer, de overbrenging, de tussenhandel en de doorvoer van producten voor tweeërlei gebruik; 3° kandida(a)t(en), inschrijver(s) of opdrachtnemer(s) is/zijn voor een opdracht geplaatst of te plaatsen door of in naam van de Belgisch Defensie of van de NAVO met inbegrip van toegang tot hun faciliteiten*". De VSSE dient om advies te worden gevraagd wanneer de investering betrekking heeft op de wettelijke opdrachten zoals bedoeld in artikel 7, 1° en 3°/1 in de Wet van 30 november 1998 houdende de regeling van de inlichtingen- en veiligheidsdiensten.

- Wordt een volwaardig terreinonderzoek van de inlichtingendiensten verwacht? Zo ja, welke onderzoeksdaden en -doelstellingen worden er dan *in concreto* verwacht?
- Ingeval een terreinonderzoek van de inlichtingendiensten wordt verwacht, welke natuurlijke personen van een buitenlandse onderneming moeten dan het voorwerp uitmaken van onderzoek (bijv. leden raad van bestuur, dagelijkse leiding, leden algemene vergadering, e.d.m.)?
- Op inhoudelijk vlak: Zijn de inlichtingendiensten verantwoordelijk voor bijvoorbeeld het detecteren van eventueel verdoken vennootschapsrechtelijke structuren? Moeten bijvoorbeeld ook de stakeholders worden gedetecteerd en onderzocht?
- Op procedureel vlak: Welke onderzoekshandelingen dienen de VSSE en/of de ADIV ter zake uit te voeren (bijv. informatie-uitwisseling met nationale partners zoals de fiscus, informatie-uitwisseling met buitenlandse partners zoals de inlichtingendiensten van andere EU-lidstaten, *social media intelligence*, e.d.m.)?

Het Comité adviseerde bijgevolg dat betrokken vragen het voorwerp diende uit te maken van parlementair debat.

Ten slotte stelde het Comité vast dat de in het Samenwerkingsakkoord uitgewerkte screeningprocedure grote overeenkomsten heeft met de bestaande procedures uitgewerkt in de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen. Een belangrijk verschil tussen beide procedures vormt wel het feit dat tegen een negatief advies van de NVO een beroep openstaat bij een speciaal hiertoe bevoegde administratief rechtscollege, zijnde het 'Beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen'. Het Comité stelde vast dat deze belangrijke procedurele waarborg ontbrak in voorliggend Samenwerkingsakkoord. De rechtsbescherming van de gescreende natuurlijke en/of rechtspersonen eist echter dat tussen beide procedures een gelijkwaardige rechtsbescherming wordt ingebouwd. Het Comité was de mening toegedaan dat, als natuurlijke beroepsinstantie voor screenings- en veiligheidsbetwistingen, het Beroepsorgaan de aangewezen instantie vormt voor een beroep tegen een negatief advies van de Interfederale Screeningscommissie.

Op 2 december 2022 keurde de Ministerraad in tweede lezing een voorontwerp van wet goed houdende instemming met het samenwerkingsakkoord van 1 juni 2022 tussen de Federale Staat en de deelgebieden tot het invoeren van een mechanisme voor de screening van buitenlandse directe investeringen. De tekst werd aangenomen in plenaire zitting van de Kamer van volksvertegenwoordigers op 9 februari 2023.

VI.5. ADVIES OVER DE KLOKKENLUIDERSREGELING VOOR DE PUBLIEKE SECTOR

Op verzoek van de minister van Ambtenarenzaken bracht het Vast Comité I in augustus 2022 een advies in met betrekking tot het voorontwerp van wet betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie.[232]

Indachtig de omschrijving van het begrip 'federale overheidsinstanties' (artikel 6, 1° en 2° van het ontwerp) vallen zowel de VSSE als de ADIV onder het toepassingsgebied van dit wetsontwerp. Het Comité beveelde ook precies aan te geven wat niet onder het toepassingsgebied valt.

Voor wat betreft de vernoemde diensten sluit het ontwerp activiteiten inzake *"de nationale veiligheid*" uit, terwijl het ontwerp evenwel daarnaast stelt dat *"(d)eze wet (…) geen afbreuk (doet) aan de bepalingen van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen*".

De memorie van toelichting van het voorontwerp verduidelijkte evenwel dat de toekomstige wet ook van toepassing zou worden inzake "*integriteitsschendingen begaan tijdens activiteiten in de uitvoering van de opdrachten van de inlichtingen- en veiligheidsdiensten*". Niettegenstaande het Comité ten volle het belang van de inrichting van een klokkenluidersregeling onderschrijft voor wat betreft integriteitsschendingen in de inlichtingendiensten, was het Comité evenwel van oordeel dat het in de praktijk onmogelijk zal zijn om een duidelijk onderscheid te maken tussen integriteitsschendingen begaan *buiten* de uitoefening van de opdrachten van deze diensten en integriteitsschendingen begaan *binnen* de uitoefening ervan.

Meer in het algemeen stelde het Comité vast dat de in het wetsontwerp voorgestelde procedures, beschermingsvoorwaarden en notificatieregelingen niet aangepast waren aan de specifieke aard en uitvoeringswijze van de activiteiten van een inlichtingendienst, en dit niet enkel wat betreft de opdrachtgerelateerde activiteiten (wat niet onder de werking van het wetsontwerp valt) maar eveneens wat betreft de zogenaamde secundaire, niet-opdrachtgerelateerde activiteiten (wat wél onder deze werking valt).

Onder meer het ontbreken van een cascadesysteem bij de melding van veronderstelde integriteitsschendingen in het ontworpen artikel 7, §1, eerste lid, 2° (meer bepaald eerst interne melding, daarna eventuele externe melding, en pas dan eventuele openbaarmaking) zal er daarenboven voor zorgen dat de bescherming van geclassificeerde informatie volgens het Comité in de praktijk niet gegarandeerd zal kunnen worden.

Het Comité benadrukte hierbij tot slot dat de onduidelijkheid rond het onderscheid tussen de twee regelingen ook niet ten goede komt voor de klokkenluider

232 Advies nr. 005/VCI/2022 van 30 augustus 2022 aangaande de klokkenluidersregeling voor de publieke sector, 7 p.

zelf. Een klokkenluider zal immer slechts kunnen genieten van de immuniteit bij een openbaarmaking ingeval hij/zij initieel heeft gekozen voor de juiste regeling (m.n. regeling in het voor advies overgemaakte wetsontwerp *vs.* regeling nationale veiligheid). Aan de hand van voorliggend wetsontwerp is dit niet duidelijk voor het Comité. Een dergelijke keuze kan alsdan bezwaarlijk worden verwacht van een melder.

Vandaar dat het Comité adviseerde om prioritair en met hoge spoed werk te maken van het opstellen van het reeds in de memorie van toelichting aangekondigde wetsontwerp dat het klokkerluidersstatuut regelt voor wat betreft integriteitsschendingen binnen het 'nationale veiligheid'-domein. Specifiek wat betreft voorliggend wetsontwerp adviseerde het Comité sterk om de inlichtingendiensten (meer bepaald de VSSE en de ADIV) en het OCAD uit het toepassingsgebied van het wetsontwerp te halen.

De Wet van 8 december 2022 regelt de meldkanalen en de bescherming van klokkenluiders in de publieke sector en verscheen in het Belgisch Staatsblad op 23 december 2022 en is van kracht sinds 2 januari 2023.[233]

VI.6. ADVIES OVER DE SCREENING VAN (KANDIDAAT-) PERSONEELSLEDEN DEFENSIE - ALGEMENE VERIFICATIEPROCEDURE EN BIJZONDER ADMINISTRATIEF CONTENTIEUX

Het Vast Comité I bracht, op verzoek van de minister van Defensie, een advies uit over een bundel regeringsamendementen bij het wetsontwerp houdende wijziging van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.[234] Het ontwerp van amendementen beoogde voornamelijk de invoering van de verplichting om de personeelsleden van Defensie te onderwerpen aan een veiligheidsverificatie.[235] Het verzoek om advies werd eind juli 2022 ingediend bij de Voorzitter van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen, tevens Voorzitter van het Vast Comité I.

---

233 Wet van 8 december 2022 betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie, *B.S.* 28 december 2022.

234 Advies nr. 001/VCI/VzBOR/2022 van 14 september 2022 over de screening van (kandidaat-) personeelsleden van Defensie, 30 p.

235 Het ontworpen artikel 22*sexies*/2 (amendement 4) stelt dat *"(t)enzij hij of zij houder is van een veiligheidsmachtiging, (…) elke burger of militair van het actief en reservekader die een functie of een betrekking bekleedt bij het ministerie van Landsverdediging, elke persoon die kandidaat is voor een dergelijke functie of betrekking, elke militair die gedetacheerd is vanuit het ministerie van Defensie, en elke burgerambtenaar van het ministerie van Defensie die tijdelijk ter beschikking is gesteld van een andere dienst, onderworpen (wordt) aan de veiligheidsverificatie bedoeld in artikel 22sexies (…)"*.

Het advies behandelt zowel kwesties in verband met de bevoegdheid van de Beroepsorgaan alsook in verband met de bevoegdheid van het Vast Comité I. Daarom werden in het advies, afhankelijk van de besproken elementen, de benamingen 'de voorzitter van het Beroepsorgaan' en het 'Vast Comité I' gehanteerd.[236]

Als een van de opmerkingen in het advies stelde de voorzitter van het Beroepsorgaan voor het ontwerp op een aantal punten te wijzigen om zaken te verduidelijken, zo onder meer wat betreft de reikwijdte van de verplichting om een veiligheidsverificatie uit te voeren, de veiligheidsadviezen waarover het college in de schoot van de ADIV een besluit zou moeten nemen, over de belangen die door het opleggen van een dergelijke veiligheidsverificatie moeten worden beschermd… Er werden ook tekstuele wijzigingen gevraagd met het oog op de naleving van artikel 109, 4° van de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (GBW) te garanderen, dat vereist dat de in het kader van een veiligheidsverificatie aangewende persoonsgegevens nauwkeurig en actueel zijn.

De voorzitter van het Beroepsorgaan stelde ook vast dat de invoering van een specifieke verificatieprocedure leidt tot een ongelijke behandeling tussen degenen die onderworpen zijn aan de bestaande algemene verificatieprocedure en degenen die onderworpen zijn aan de specifieke verificatieprocedure voor Defensie die de wijzigingen beogen in te voeren. De voorzitter van het Beroepsorgaan merkte op dat sommige verschillen in behandeling niet (voldoende) gerechtvaardigd waren, en deed daarom voorstellen om de twee procedures op bepaalde punten op elkaar af te stemmen.

De voorzitter van het Beroepsorgaan pleitte ook voor wijzigingen in de W.Beroepsorgaan teneinde de rechtspraak van het Grondwettelijk Hof, volgens welke het Beroepsorgaan een administratieve rechtsbank is met volle rechtsmacht en de veiligheidsadviezen van het Beroepsorgaan dwingend van aard zijn, wettelijk te verankeren. Er werden aanvullende opmerkingen gemaakt over de beroepsprocedure bij het Beroepsorgaan (met name de kwestie van de persoonlijke verschijning van de verzoekende partij op de zitting).

Het Vast Comité I maakte ook een aantal opmerkingen over de nieuwe strafbare feiten die het wetsvoorstel beoogt in te voeren en die betrekking hebben op het oneigenlijk gebruik van geclassificeerde informatie en de openbaarmaking daarvan.

Ten slotte wees het Comité op een legistiek probleem in de wijziging van de Inlichtingenwet en verzocht het om een rectificatie van artikel 4 van de Wet van 14 juli 2022 in het Belgisch Staatsblad.

Het wetsontwerp tot wijziging van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, -attesten en -adviezen werd aangenomen in de plenaire vergadering van de Kamer van volksvertegenwoordigers van 9 februari 2023.

---

236 Voor een overzicht van het geheel van de gefomuleerde opmerkingen, wordt verwezen naar het integrale advies dat beschikbaar is op de website van het Vast Comité I.

HOOFDSTUK VII.

DE OPSPORINGS- EN GERECHTELIJKE ONDERZOEKEN

De Dienst Enquêtes I van het Comité doet in opdracht van de gerechtelijke overheden ook onderzoeken naar leden van de inlichtingen- en veiligheidsdiensten en het Coördinatieorgaan voor de dreigingsanalyse (OCAD)[237] die verdacht worden van een misdaad en/of wanbedrijf. 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 (W.Toezicht).

Wanneer zij een opdracht van gerechtelijke politie vervullen, staan de leden en het hoofd 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 het hoofd van de Dienst Enquêtes I 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).

In 2022 voerde de Dienst Enquêtes I onderzoeksdaden uit in het kader van drie opsporingsonderzoeken, respectievelijk onder leiding van de substituut-procureur des Konings van Halle-Vilvoorde en de onderzoeksrechter van Brussel, van de substituut-procureur des Konings van Brussel en van het Federaal Parket. Er werden zestien processen-verbaal opgesteld. De beoogde strafbare feiten betroffen de 'schending van het beroepsgeheim' door een lid van een inlichtingendienst (de en-

[237] Wat betreft de leden van de andere 'ondersteunende diensten' van het OCAD geldt deze bepaling alleen ten aanzien van de verplichting om relevante inlichtingen aan het OCAD mee te delen (artt. 6 en 14 W.OCAD).

quêtedienst werd hierin bijgestaan door de Federale Gerechtelijke Politie), het 'niet of onzorgvuldig toepassen van de regelgeving omtrent veiligheidsmachtigingen' en ten slotte in het kader van een reeds eerder (2021) opgestart onderzoek naar aanleiding van een klacht van een lid van een inlichtingendienst 'wegens pesterijen'.

Naast processen-verbaal die werden opgesteld in het kader van bovenstaande opsporingsonderzoeken, werd een bijkomend proces-verbaal opgesteld naar aanleiding van een gerechtelijk onderzoek waarbij de Dienst Enquêtes I door de onderzoeksrechter van Nijvel in het kader van een huiszoeking om bijstand werd gevraagd. Ten slotte werd op basis van artikel 29 Sv. een proces-verbaal opgesteld en gericht aan de procureur des Konings te Brussel.

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 2022 geen meldingen in die zin.

HOOFDSTUK VIII.
EXPERTISE EN EXTERNE CONTACTEN

VIII.1. EXPERT OP DIVERSE FORA

Leden van het Vast Comité I en van zijn personeel werden in 2022 diverse malen als expert geconsulteerd door binnen- en buitenlandse publieke en private instellingen:

- De dienstdoend 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;
- Er werd door medewerkers van het Comité een boek gerealiseerd en verschillende artikelen gepleegd in wetenschappelijke en gevulgariseerde tijdschriften[238];
- De voorzitter van het Vast Comité I werd half mei 2022 door de *Faculté de Droit, de Science Politique et de Criminologie* van de Universiteit van Luik gevraagd om de onderzoeksmethodologie bij de aanpak van toezichtonderzoeken te komen toelichten aan de deelnemers van een opleiding in het kader van het *Certificat d'Université en Analyse du Renseignement*;
- Er vonden gedachtenuitwisselingen plaats met academici (Uppsala University, Zweden) over de rechtspraak van het Hof van Justitie van de Europese Unie;
- De dienstdoend griffier werd uitgenodigd om een uiteenzetting te geven over het juridisch kader van veiligheidsscreenings in België tijdens een studiedag georganiseerd door het Verbond van Belgische Ondernemingen (VBO);
- De chef van de Dienst Enquêtes werd ingeschakeld in een opleidingsmoment voor de rekruten bij de ADIV;

238 W. VAN LAETHEM, *Handboek Veiligheidsscreenings*, Politeia, Brussel, 2022, 177 p.; B. VERSCHAEVE, 'Het Incident Response Team van de Staatveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht', *Politie en Recht*, 1, 2022, 3-20; C. THOMAS, *BePolitix*, www.absp.be/blog ('La 'liste OCAM' ou l'ancrage de l'organe de coordination au sein du champ antiterroriste belge');

- Een medewerkster van het Vast Comité I presenteerde in maart 2022 de resultaten van haar doctoraat over het coördinatieorgaan en de organisatie van de strijd tegen terrorisme in België;[239]
- Eind mei nam het Comité deel aan de UNCTAD[240]-evaluatie '*Law Enforcement – Oversight of Counter-terrorism activities of Law Enforcement Bodies*';
- De dienstdoend griffier werd uitgenodigd in september om een uiteenzetting te geven over het juridisch kader van veiligheidsscreenings in België tijdens een studiedag achter gesloten deuren georganiseerd door de Universiteit van Antwerpen (*Security screenings in Europe: A Comparative Analysis*);
- Nog in september 2022 werd de dienstdoend griffier uitgenodigd door uitgeverij Politeia om zijn *Handboek Veiligheidscreenings*' te komen voorstellen (Provinciehuis Vlaams-Brabant, Leuven);
- Ten slotte nam in september 2022 een medewerkster deel aan de *Pan-European Conference on International Relations* georganiseerd door de *European International Studies Association* in Athene.[241]

VIII.2. SAMENWERKINGSPROTOCOL MET DE FEDERALE OMBUDSMANNEN

De Wet van 15 september 2013[242] duidt de Federale Ombudsmannen aan als centraal meldpunt voor veronderstelde integriteitsschendingen in de federale administratieve overheden. In september 2021 werd het 'Samenwerkingsprotocol van 7 oktober 2021 voor de relaties tussen de Federale Ombudsmannen en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van de Wet van 15 september 2013' afgesloten. Het protocol beoogt de samenwerkingsmodaliteiten te regelen tussen de Federale Ombudsmannen en het Comité wanneer een veronderstelde integriteitsschending in één van beide inlichtingendiensten wordt gesignaleerd bij de Ombudsman.

In voorkomend geval kan deze laatste aan het Vast Comité I vragen om een lid van de Dienst Enquêtes I aan te duiden om het Centrum voor Integriteit – een centraal meldpunt opgericht in de schoot van de Federale Ombudsmannen – bij te staan als deskundige bij de uitvoering van het onderzoek. Van deze mogelijkheid werd door de Federale Ombudsmannen in 2022 geen gebruik gemaakt. In het pro-

---

239 C. THOMAS, *Une menace possible et vraisemblable. Dire et faire la sécurité : l'Organe de Coordination pour l'Analyse de la Menace et la structuration du champ antiterroriste belge*, Bruxelles, UCLouvain – Saint-Louis Bruxelles, septembre 2021, 470 p.

240 https://unctad.org/about/evaluation.

241 De titel van haar bijdrage luidde: '*Looking beyond traditional intelligence services: CUTA and the fight against terrorism in Belgium*'.

242 Wet van 15 september 2013 betreffende de melding van een veronderstelde integriteitsschending in de federale administratieve overheden door haar personeelsleden, *BS* 14 oktober 2013.

tocol werden verder afspraken gemaakt over de onderzoeksmiddelen, het beroepsgeheim, de vertrouwelijkheid en de uitwisseling van *best practices*.

Wel verscheen op 23 december 2022 in het Belgisch Staatsblad de 'Wet van 8 december 2022 betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie'. Melders van integriteitsschendingen binnen de federale overheidsdiensten en de geïntegreerde politie genieten voortaan bescherming conform de Europese Klokkenluidersrichtlijn (richtlijn 2019/1937). Met deze wet heeft de federale wetgever de bepalingen omgezet in nationaal recht.[243]

Deze wet kent het Vast Comité I een nieuwe bevoegdheid toe: "*het externe meldingskanaal voor integriteitsschendingen begaan bij de Algemene Dienst Inlichting en Veiligheid of de Veiligheid van de Staat, wordt ingericht bij het Vast Comité I*".[244]

VIII.3. PARTNERSHIP MET HET FEDERAAL INSTITUUT MENSENRECHTEN

Middels een samenwerkingsprotocol kwamen alle deelnemende instanties (te weten alle sectorale instanties voor de bescherming en de bevordering van de rechten van de mens, waaronder het Vast Comité I) overeen om praktijken en methoden uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen. Er worden daartoe in de schoot van het Mensenrechtenplatform informele overlegvergaderingen georganiseerd, die sedert september 2022 worden gecoördineerd door het Federaal Instituut Mensenrechten.[245] Het Comité nam in 2022 niet actief deel aan het Mensenrechtenplatform.

VIII.4. EEN MULTINATIONAAL INITIATIEF INZAKE INTERNATIONALE INFORMATIE-UITWISSELING

De toegenomen internationale gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten brengt uitdagingen mee voor de nationale toezichtorganen. De toezichtorganen van (oorspronkelijk) vijf Europese landen (België, Denemarken, Nederland, Noorwegen en Zwitserland) overleggen daarom sinds enkele jaren om het hoofd te bieden aan die uitdagingen door werkwijzen te vinden om het risico op een hiaat in het toezicht te verkleinen *(International Overisght Working Group (IOWG))*.

---

243 Het toepassingsgebied betreft niet de nationale veiligheid.

244 Het meldingskanaal voor integriteitsschendingen begaan bij het OCAD wordt ingericht bij het Vast Comité P.

245 Sinds februari 2023 nemen de Federale Ombudsmannen het secretariaat van het Platform Mensenrechten voor hun rekening.

In maart 2022 werd een *face-to-face* staff meeting van de IOWG georganiseerd in Bern, en dit sinds het eerst na de aanvang van de sanitaire crisis. Na een korte voorstelling door de verschillende delegaties van de laatste ontwikkelingen binnen de respectievelijke instellingen, ging de aandacht vooral naar de toekomst voor en de doelstellingen van de IOWG, het online platform, de publicaties van de toezichtsorganen en het model van risico-analyse voorgesteld door de gastheren van het Zwitserse toezichtorgaan *Autorité de surveillance indépendante des activités de renseignement* (AS-Rens). In oktober 2022 werd een, niet bindend- '*Charter of the Intelligence Oversight Working Group*' ondertekend in Londen, waar ook de toetreding van de Zweedse toezichtsorganen[246] tot de IOWG formeel werd aangenomen.

VIII.5. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

In oktober 2022 werd in Londen de vierde *European Intelligence Oversight Conference* gehouden. Tijdens deze conferentie, georganiseerd door de *Investigatory Powers Commissioner's Office (IPCO*), werden panels georganiseerd rond thema's als '*Accountablility and Communication – reporting and sharing information with the public*', *'Co-operation across the oversight community in building technological competence*', *'Metrics of Privacy*', *'Saveguards of information from sensitive professions*', *'Sharing information between states'* en *'Development of European jurisprudence and the role of the Council of Europe*'.

De voorzitter van het Vast Comité I nam in juni in Berlijn ook deel aan de derde workshop van het *European Intelligence Oversight Network* (EION), met als thema *'the governance of intelligence services' use of commercially available data*' en, in november, aan het *International Intelligence Oversight Forum 2022* (IIOF) in Straatsburg, met als voornaamste topics artikel 11 van de Convente 108+ en de impact van het conflict in Oekraïne op het toezicht van inlichtingendiensten.

De komst in 2022 van de stagiaire van het Zwitsere *Autorité de surveillance indépendante des activités de renseignement (AS-Rens)* werd uiteindelijk uitgesteld.

Ten slotte ontving het Vast Comité I eind juni, een delegatie van de Griekse *Haute Autorité hellénique pour la sauvegarde de l'intimité des communications* (ADAE). In de loop van dit tweedaags werkbezoek gaf het Comité de Griekse delegatie toelichting bij het Belgische institutionele en veiligheidssysteem en de wettelijke opdrachten van het Vast Comité I aan de hand van een reeks presentaties, gevolgd door discussies en het delen van ervaringen. Bovendien ontving de Kamervoorzitster en voorzitster van de Begeleidingscommissie de Griekse delegatie, het Comité en verscheidene van zijn medewerkers voor een gedachtewisseling.

246 Te weten de *Swedisch Foreign Intelligence Inspectorate (Statens inspektion av försvarunderättelse-verksamhet (SIUN)* en de *Swedish Board of Inventions (Statens uppfinnarnämnd (SUN).*

HOOFDSTUK IX.

HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN[247]

Dit hoofdstuk omvat het in mei 2023 goedgekeurde activiteitenverslag van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen alsook een aantal opmerkingen en suggesties van de voorzitter van dit rechtscollege.

IX.1. HET ACTIVITEITENVERSLAG VAN HET BEROEPSORGAAN

IX 1.1. INLEIDING

Het Beroepsorgaan is in België het enige administratief rechtscollege dat bevoegd is voor geschillen die betrekking hebben op administratieve beslissingen in verschillende domeinen: veiligheidsmachtigingen, veiligheidsattesten en, tot slot, veiligheids-adviezen.

Daarnaast kan het Beroepsorgaan ook optreden als 'annulatierechter' tegen beslissingen van publieke of administratieve overheden om in een bepaalde sector, voor een bepaalde plaats of voor een bepaald evenement veiligheidsattesten of -adviezen aan te vragen.[248]

Het Beroepsorgaan is samengesteld uit de voorzitters van het Vast Comité I, het Vast Comité P en de Geschillenkamer van de Gegevensbeschermingsautoriteit. Als ze verhinderd zijn, kunnen de drie voorzitters worden vervangen door een effectief lid-raadsheer van de instelling waartoe de betrokken voorzitter behoort.

De voorzitter van het Vast Comité I neemt het voorzitterschap van het Beroepsorgaan waar. De functie van griffier wordt uitgeoefend door de griffier van het Vast Comité I; het personeel van de griffie is het door het Comité aangestelde

247 Dit activiteitenverslag voert artikel 13 uit van de Wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, waarin wordt bepaald dat het Beroepsorgaan een activiteitenverslag moet opstellen.

248 Voor meer informatie, zie VAST COMITÉ I, *Activiteitenverslag 2006*, 87-120 en VAST COMITÉ I, *Activiteitenverslag 2018*, 111-124.

personeel. De samenstelling van het Beroepsorgaan levert een multidisciplinaire bijdrage aan de beraadslaging betreffende elk dossier.

Op te merken valt dat de administratie en de opvolging van de beroepen integraal ten laste is van het Vast Comité I. Het Comité stelt immers alle personen en middelen ter beschikking die nodig zijn om de administratie, de briefwisseling, het houden van hoorzittingen en het opstellen van de beslissingen voor zijn rekening te nemen. Het gaat daarbij enerzijds om de terbeschikkingstelling van de voorzitter en zijn plaatsvervangende leden en de griffier, maar ook de juristen als '*toegevoegde griffiers*' en het administratief personeel die de griffie van dit administratief rechtscollege vormen. Anderzijds neemt het Vast Comité I in zijn begroting ook de kosten van de kantoren op zich als werkingskosten van het Beroepsorgaan.

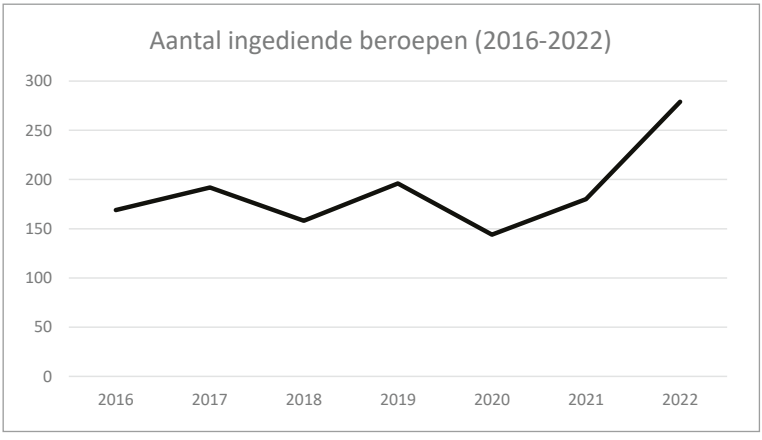
IX.1.2. GEDETAILLEERDE CIJFERS

In dit onderdeel worden de aard van de bestreden beslissingen, de hoedanigheid van de bevoegde overheden en de verzoekers, en de aard van de beslissingen van het Beroepsorgaan binnen de verschillende beroepsprocedures cijfermatig weergegeven. Om enige vergelijking mogelijk te maken, werden de cijfers van de zes vorige jaren eveneens opgenomen.

In 2022 werden 279 beroepen ingesteld, hetgeen een sterke stijging betekent ten opzichte van 2021 (180 beroepen) en 2020 (144 beroepen). Het Beroepsorgaan hield hoorzittingen à rato van minimaal twee per maand. In 2022 vonden er 41 hoorzittingen plaats waarvan vier hoorzittingen met leden van veiligheidsoverheden.[249]

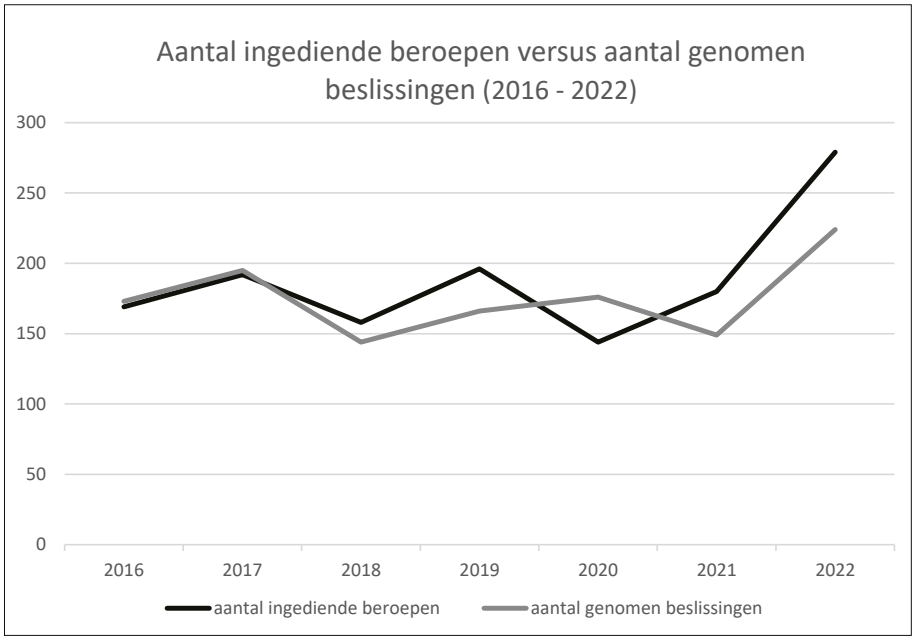
Er werden 224 definitieve beslissingen genomen.

Tabel 1. Aantal ingediende beroepen (2016-2022)



[249] 12 in het Nederlands en 29 in het Frans.

Tabel 2. Aantal ingediende beroepen versus aantal verleende beslissingen (2016-2022)

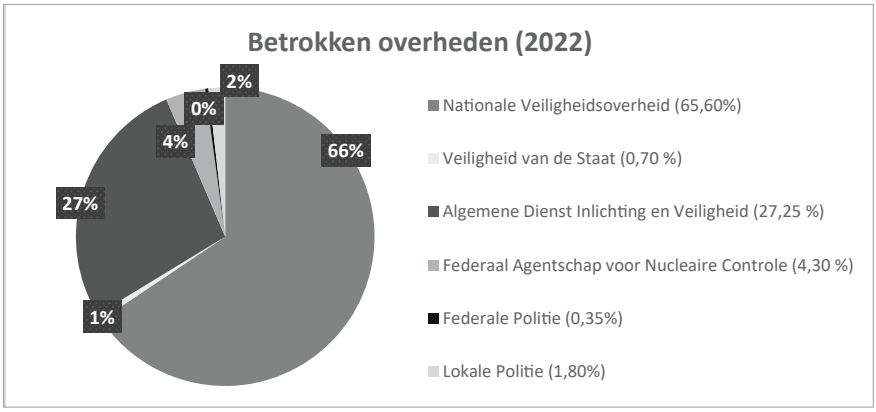


Tabel 3. Betrokken veiligheids- en verificatieoverheden[250] (2016-2022)

	2016	2017	2018	2019	2020	2021	2022
Nationale Veiligheidsoverheid	92	129	113	114	91	86	183
Staatsveiligheid	0	0	0	0	0	4	2
Algemene Dienst Inlichting en Veiligheid	68	53	32	61	41	84	76
Federaal Agentschap voor Nucleaire Controle	8	7	10	17	7	6	12
Federale politie	1	3	3	3	4	0	1
Lokale politie	0	0	0	1	1	0	5
TOTAAL	**169**	**192**	**158**	**196**	**144**	**180**	**279**

250 'Verificatieoverheden' zijn overheden bevoegd voor het afleveren van veiligheidsattesten en -adviezen, zoals bijvoorbeeld de Federale Politie en de Federaal Agentschap voor Nucleaire Controle.

Onderstaande grafiek toont de verdeling van de betrokken veiligheids- en verificatieoverheden in 2022.



Tabel 4. Aard van de bestreden beslissingen

	2016	2017	2018	2019	2020	2021	2022
Veiligheidsmachtigingen (Art. 12 e.v. W.C&VM)							
Vertrouwelijk	5	1	2	5	0	2	5
Geheim	38	33	31	39	27	50	64
Zeer geheim	7	6	3	7	5	8	14
Weigering	28	30	26	39	23	37	47
Intrekking	9	7	4	16	8	17	15
Weigering en intrekking	0	0	0	0	0	4	3
Machtiging voor beperkte duur	4	1	1	3	0	1	0
Machtiging voor een lager niveau	1	0	0	0	0	0	1
Geen beslissing binnen de termijn	7	2	5	0	0	1	17
Geen beslissing binnen de verlengde termijn	1	0	0	0	0	0	0
Andere					1[251]		
SUBTOTAAL VEILIGHEIDS-MACHTIGINGEN	**50**	**40**	**36**	**51**	**32**	**60**	**83**
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)							
Weigering	1	3	3	1	0	3	2
Intrekking	0	0	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	0	0	0	0	0

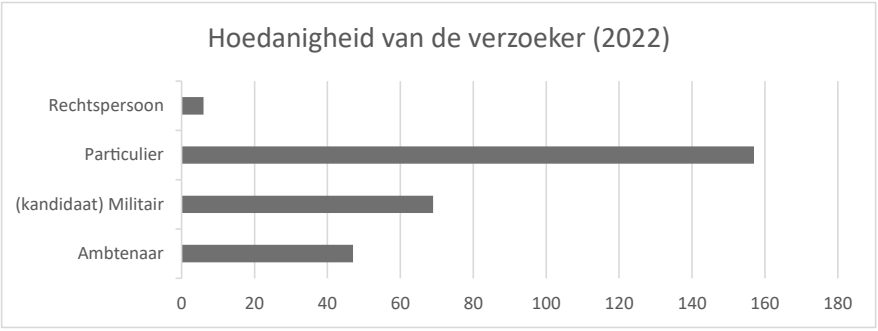
251 'Waarschuwing van de verzoeker'. Aan een persoon werd de veiligheidsmachtiging voor een periode van vijf jaar met een waarschuwing toegekend. De betrokkene heeft beroep ingesteld tegen deze waarschuwing.

	2016	2017	2018	2019	2020	2021	2022
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)							
Weigering	9	20	15	12	6	2	21
Intrekking	0	0	0	0	0	0	2
Geen beslissing binnen de termijn	0	0	0	0	0	1	2
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)							
Weigering	7	7	11	17	7	6	12
Intrekking	1	0	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	1	0	0	0	0
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)							
Negatief advies	101	122	92	115	99	108	157
Geen advies	0	0	0	0	0	0	0
Herroeping van positief advies	0	0	0	0	0	0	0
Normatieve rechtshandelingen van een administratieve overheid (Art. 12 W.Beroepsorgaan)							
Beslissing van een overheidsinstantie om veiligheidsattesten te eisen	0	0	0	0	0	0	0
Weigering van de NVO om verificaties voor veiligheidsattesten te verrichten	0	0	0	0	0	0	0
Beslissing van een administratieve overheid om veiligheidsadviezen te eisen	0	0	0	0	0	0	0
Weigering van de NVO om verificaties voor veiligheidsadviezen te verrichten	0	0	0	0	0	0	0
SUBTOTAAL ATTESTEN EN ADVIEZEN	**119**	**152**	**122**	**145**	**112**	**120**	**196**
TOTAAL BESTREDEN BESLISSINGEN	**169**	**192**	**158**	**196**	**144**	**180**	**279**

Tabel 5. Hoedanigheid van de verzoeker

	2016	2017	2018	2019	2020	2021	2022
Ambtenaar	2	4	5	4	8	16	47
(kandidaat) Militair	23	20	8	27	39	81	69
Particulier	139	164	140	163	95	80	157
Rechtspersoon	5	4	5	2	2	3	6

Onderstaande grafiek toont de verdeling volgens de 'hoedanigheid van de verzoeker' in 2022.



Tabel 6. Taal van de verzoeker

	2016	2017	2018	2019	2020	2021	2022
Franstalig	99	115	83	101	83	86	201[252]
Nederlandstalig	70	77	75	95	61	94	123[253]
Duitstalig	0	0	0	0	0	0	0
Anderstalig	0	0	0	0	0	0	0

252 181 Franstalige dossiers in 2022 et 20 Franstalige dossiers van de afgelopen jaren (maar behandeld in 2022).

253 98 Nederlandstalige dossiers in 2022 en 25 Nederlandstalige dossiers van de afgelopen jaren (maar behandeld in 2022).

Tabel 7. Handelingen van de griffie

	2016	2017	2018	2019	2020	2021	2022
Volledig dossier opvragen (1)	167	191	154	191	141	180	279
Vraag om bijkomende informatie (2) en herinneringen verstuurd naar de veiligheids- en verificatieoverheden (3)	23	36	12	39	41	45	146[254]

(1) Het Beroepsorgaan kan het gehele dossier opvragen bij de veiligheids- en verificatieoverheden. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan door de griffie.

(2) Het Beroepsorgaan beschikt over de mogelijkheid om tijdens de procedure aanvullende informatie die het nuttig acht, op te vragen. In de praktijk neemt de griffie de taak op zich om de overheden te vragen de dossiers te vervolledigen.

(3) Art. 6 van het KB Beroepsorgaan bepaalt de termijnen voor de aanlevering van de dossiers door de veiligheids- en verificatieoverheden. Die termijnen vangen aan wanneer de griffier een kopie van het beroep naar de betrokken veiligheids- of verificatieoverheid stuurt. Ze variëren naargelang de aard van de betwiste handeling. Zo moet de veiligheids- of verificatieoverheid haar dossier aanleveren binnen de 15 dagen voor veiligheidsmachtigingen, binnen de 5 dagen voor veiligheidsattesten en binnen de 10 dagen als het beroep betrekking heeft op een veiligheidsadvies. Wanneer die termijnen niet worden nageleefd, legt de griffie de nodige contacten. Deze gegevens worden geregistreerd vanaf 2019.

[254] Er werden 76 vragen om bijkomende informatie en 70 herinneringen verstuurd naar de veiligheids- en verificatieoverheden.

Tabel 8. Voorbereidende gerechtelijke handelingen van het Beroepsorgaan [255]

	2016	2017	2018	2019	2020	2021	2022
Horen van een lid van een overheidsinstantie (1)	10	0	1	6	1	4	12
Beslissing van de voorzitter (2)	0	0	0	0	0	0	0
Verwijderen van informatie uit het dossier door het Beroepsorgaan (3)	54	80	72	77	50	77	118
Beslissingen alvorens recht te doen (4)	/	/	/	9	9	19	28

(1) Het Beroepsorgaan kan beslissen om de leden van de inlichtingen- en politiediensten of van de veiligheids- of verificatieoverheden die aan het veiligheidsonderzoek of de veiligheidsverificatie hebben meegewerkt, te horen.
(2) De voorzitter van het Beroepsorgaan kan beslissen dat het lid van de inlichtingendienst bepaalde gegevens geheimhoudt tijdens zijn verhoor.
(3) Indien de betrokken inlichtingen- of politiedienst hierom verzoekt, kan de voorzitter van het Beroepsorgaan beslissen dat bepaalde informatie wordt verwijderd uit het dossier dat ter inzage aan de verzoeker zal worden voorgelegd.
(4) Het kan bijvoorbeeld gaan om de verdere opvraging van informatie over de context van een gerechtelijk dossier of de verschijning te bevelen van de diensten die het onderzoek of de veiligheidsverificatie hebben verricht. Deze gegevens worden geregistreerd vanaf 2019.

[255] De cijfers voor 'voorbereidende gerechtelijke handelingen' (tabel 6), 'wijze waarop de verzoeker zijn rechten van verdediging uitoefent' (tabel 7) of 'aard van de beslissingen van het Beroepsorgaan' (tabel 8) komen niet noodzakelijkerwijs overeen met het aantal ingediende verzoeken (zie tabellen 1 tot 4). Sommige dossiers werden bijvoorbeeld al opgestart in 2020, terwijl de beslissing pas viel in 2021.

Tabel 9. Wijze waarop de verzoeker zijn rechten van verdediging uitoefent

	2016	2017	2018	2019	2020	2021	2022
Inzage van het dossier door de verzoeker en/of zijn advocaat	87	105	69	96	96	97	136
Horen van de verzoeker (al dan niet bijgestaan door zijn advocaat)[256]	127	158	111	143	135	151	192

Tabel 10. Aard van de beslissingen van het Beroepsorgaan

	2016	2017	2018	2019	2020	2021	2022
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)							
Beroep onontvankelijk	0	3	0	1	1	0	2
Beroep zonder voorwerp	7	0	4	3	3	3	5
Beroep ongegrond	18	13	12	12	16	11	20
Beroep gegrond (volledige of gedeeltelijke toekenning)	24	24	12	25	14	17	31
Bijkomende onderzoeksdaden door de overheidsinstantie	2	0	1	1	2	1	1
Bijkomende termijn voor de overheidsinstantie	2	1	1	0	3	0	3
Verleent akte van afstand van beroep	0	0	3	2	2	11	2
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)							

256 De W.Beroepsorgaan regelt de bijstand door een advocaat tijdens de zitting, maar niet de vertegenwoordiging door die laatste. In bepaalde dossiers wordt de verzoeker (al dan niet bijgestaan door zijn advocaat) meermaals gehoord. In 56% van de gevallen werd de verzoeker bijgestaan door een advocaat.

	2016	2017	2018	2019	2020	2021	2022
Beroep onontvankelijk	0	1	0	0	0	0	0
Beroep zonder voorwerp	0	1	0	0	0	0	0
Beroep ongegrond	1	0	1	1	0	2	0
Beroep gegrond (toekenning)	1	1	0	3	0	2	1
Verleent akte van afstand van beroep	-	-	-	1	0	0	0
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)							
Beroep onontvankelijk	0	1	2	4	2	0	4
Beroep zonder voorwerp	0	1	0	0	0	0	1
Beroep ongegrond	2	12	2	4	4	1	6
Beroep gegrond (toekenning)	4	7	3	4	1	0	9
Verleent akte van afstand van beroep	0	1	2	0	0	0	2
Veiligheidsattesten voor nucleaire sector (art. 8*bis*, §2 W.C&VM)							
Beroep onontvankelijk	1	1	0	1	0	0	0
Beroep zonder voorwerp	1	0	1	0	0	0	1
Beroep ongegrond	0	1	1	5	2	2	6
Beroep gegrond (toekenning)	7	5	6	7	4	6	5
Verleent akte van afstand van beroep	-	-	2	0	0	0	0

	2016	2017	2018	2019	2020	2021	2022
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)							
Beroepsorgaan onbevoegd	0	20[257]	12	0	0	0	0
Beroep onontvankelijk	15	10	3	7	8	3	18
Beroep zonder voorwerp	0	1	3	1	6	4	11
Bevestiging van negatief advies	42	49	46	40	51	47	59
Omzetting in positief advies	46	41	27	43	52	34	37
Verleent akte van afstand van beroep	0	1	0	1	5	5	4
Beroep tegen normatieve rechtshandelingen van een administratieve overheid (art. 12 W.Beroepsorgaan)	0	0	0	0	0	0	0
TOTAAL	**173**	**195**	**144**	**166**	**176**	**149**	**228**

IX.2. OPMERKINGEN EN SUGGESTIES VAN DE VOORZITTER VAN HET BEROEPSORGAAN

1. Op 9 februari 2023 heeft de Kamer het wetsontwerp tot wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, -attesten en -adviezen aangenomen.[258]
   Na de inwerkingtreding van deze wet op 31 december 2023 zal de Veiligheid van de Staat de bevoegdheden van de Nationale Veiligheidsoverheid overnemen en voortaan bevoegd zijn voor de uitreiking, de wijziging, de schorsing en de intrekking van veiligheidsmachtigingen, uitgezonderd voor Defensie.

257 Het betreft *in casu* de beroepen ingediend tegen (negatieve) veiligheidsadviezen van de Nationale Veiligheidsoverheid met betrekking tot personeel van onderaannemers actief bij Europese instellingen. Het Beroepsorgaan had beslist dat er geen wettelijke basis was voor de adviezen van de Nationale Veiligheidsoverheid. Bijgevolg verklaarde het Beroepsorgaan zich onbevoegd om te oordelen over de al dan niet gegrondheid van de veiligheidsadviezen van de Nationale Veiligheidsoverheid.

258 Wetsontwerp tot wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *Parl. St.*, Kamer, 2022-2023, nr. 55-2443/009.

De Federale Politie krijgt dan weer een algemene bevoegdheid voor het uitreiken, wijzigen, schorsen en intrekken van veiligheidsadviezen.
Deze wijzigingen van veiligheidsoverheden zullen zeker gevolgen hebben voor de werking van de jurisdictie. De tijd zal het mogelijk maken de effecten hiervan te analyseren. In de volgende activiteitenverslagen kan ongetwijfeld een evaluatie worden gemaakt.

2. In 2022 moest het Beroepsorgaan zich in twee gevallen buigen over vragen in verband met veiligheidsonderzoeken in het kader van veiligheidsmachtigingen. Telkens stelde de burger problemen aan de orde met de rechtmatigheid van het door de inlichtingendiensten gevoerde onderhoud. Daarbij herinnerde het Beroepsorgaan eraan dat het aan de diensten was om het interview te laten paraferen door de aanvrager van een veiligheidsmachtiging en, indien de betrokkene niet een van de landstalen beheerste, zich door een tolk te laten bijstaan.

3. Het Beroepsorgaan heeft nota genomen van het voornemen van de regering om het beginsel van veiligheidsverificaties voor de toekenning van veiligheidsadviezen uit te breiden tot alle Defensiemedewerkers, en dit op vijfjaarlijkse basis.[259] Naast deze wetswijziging heeft de minister van Justitie ook andere wijzigingen aangekondigd voor de 16.000 mensen die in de havensector werken. Deze wijzigingen hebben gevolgen voor de toekomst van het Beroepsorgaan. Op geen enkel moment is in de ontwerpen op deze werklast ingegaan. Het is echter belangrijk dat de leden van de griffie in goede omstandigheden kunnen werken.

4. Het Beroepsorgaan stelt dat Kamer, verantwoordelijk voor zijn begroting via het Vast Comité I, nog geen rekening heeft gehouden met de ontwikkeling van het contentieux. Toen het Beroepsorgaan in december 2022 verzocht om een personeelsuitbreiding met twee eenheden (een secretaresse en een jurist), alleen al om de toename van de beroepen met 50% in 2022 op te vangen, stemde de Kamer ermee in een jurist in dienst te nemen. De administratieve werklast verandert voortdurend en de toename van het contentieux stelt dan ook problemen.

5. Maar ook het gebrek aan digitalisering van de jurisdictie, reeds eerder aan de Kamer gevraagd, vormt een toenemend probleem. Het wordt al jaren aan de kaak gesteld, maar zonder effect. Evenmin is gevolg gegeven aan het wetsvoorstel dat werd uitgewerkt om de procedure te vereenvoudigen en de toegang tot de rechter te verbeteren. Zo wordt de burger nog steeds geconfronteerd met

259 Zie het advies van het Comité hierover (VI.6. Screening van (kandidaat-)personeelsleden Defensie – Algemene verificatieprocedure en bijzonder administratief contentieux).

beroepstermijnen van acht dagen en omslachtige procedures die niet meer voldoen aan de moderne eisen voor toegang tot de rechter. Is het normaal dat particulieren en hun advocaten, die nu bij twee op de drie zaken betrokken zijn, hun dossier niet op afstand kunnen raadplegen?

6. Wij wijzen erop dat ons verzoek om in aanmerking te komen voor de vrijstelling van postfranchise door de Kamervoorzitster werd doorgegeven aan de bevoegde minister, maar evenwel zonder succes bleef. Het Beroepsorgaan blijft wettelijk verplicht al zijn correspondentie aangetekend te verzenden. De wet staat het niet toe e-mail te gebruiken. Dit resulteerde in 2022 in meer dan 15.000 euro portokosten.

Tot slot wil ik alle medewerkers van het Beroepsorgaan bedanken: de griffier, de toegevoegde griffiers, juristen, secretariaatsmedewerkers en alle mensen die ervoor zorgen dat rechtzoekenden hun beslissing zonder vertraging ontvangen. Ik wil de menselijke kwaliteiten en de beschikbaarheid van de griffie benadrukken, want als een rechtzoekende telefonisch of per e-mail contact opneemt met de griffie, wordt er echt naar hem of haar geluisterd en krijgt hij of zij een passend antwoord op zijn of haar vragen. De eenenveertig hoorzittingen in 2022 hadden niet kunnen plaatsvinden zonder de onmisbare hulp van onze collega-voorzitters en leden van het Vast Comité P en de Geschillenkamer van de Gegevensbeschermingsautoriteit. Ik dank ook raadslid Pieter-Alexander De Brock die de Nederlandstalige kamer van beroep heeft voorgezeten.

HOOFDSTUK X.

DE INTERNE WERKING VAN HET VAST COMITÉ I

X.1. SAMENSTELLING VAN HET VAST COMITÉ I

De samenstelling van het Comité bleef in 2022 ongewijzigd: Serge Lipszyc (F), eerste substituut arbeidsauditeur bij het arbeidsauditoraat van Luik bleef zijn opdracht als voorzitter vervullen. Pieter-Alexander De Brock (N) en Thibaut Vandamme (F), substituut procureur des Konings van het arrondissement Luxemburg oefenden het mandaat van lid uit.[260]

Wel werd door de Kamer een nieuwe griffier[261] benoemd, te weten Frédéric Givron (F), die op 26 april 2022 de eed aflegde.[262]

Nog in 2022, werd door de voorzitter van het Vast Comité I de voorzitster van de Kamer van volksvertegenwoordigers aangeschreven met verzoek om een personeelsuitbreiding. Een eerste brief van 8 juni 2022 werd door het Comité verstuurd in zijn hoedanigheid van Gegevensbeschermingsautoriteit. In een tweede schrijven d.d. 2 augustus 2022 werd verzocht om een personeelsversterking voor het Beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsadviezen en veiligheidsattesten. Niettegenstaande de door de Kamer geleverde inspanningen in het kader van de synergiën, dewelke door het Comité worden toegejuicht, achtte het Comité het noodzakelijk om een versterking aan te vragen.[263] Het Comité verkeert immers in de onmogelijkheid om alle wettelijke opdrachten uit te voeren en adequaat te reageren op de verschillende verzoeken van de Kamer. Op 15 december 2022

---

260 Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten - benoeming van de tweede plaatsvervanger van het Nederlandstalig lid – Filip Vanneste (*Hand.* Kamer 2021-22, 24 maart 2022, CRIV55PLEN171, 67).

261 Op 19 mei 20022 wordt Wouter De Ridder, voormalig griffier, in toepassing van artikel 20, tweede lid, van het Huishoudelijk Reglement van het Vast Comité I, de eretitel van zijn ambt toegekend ((*Hand.* Kamer 2021-22, 19 mei 2022, CRIV55PLEN181, 58.)

262 Benoeming van de griffier van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Parl. St. Kamer 2021-22, nr. 55K2597/001 en uitslag van de geheime stemming invasie *(Hand.* Kamer 2021-22, 24 maart 2022, CRIV55PLEN171, 75).

263 In dat kader werden twee vacatures gepubliceerd: de aanwerving voor onmiddellijke indiensttreding en de aanleg van een wervingsreserve voor een Franstalige statutaire secretaris/esse (m/v/x) (niv.B) (*B.S.* 6 september 2022) en de aanwerving, middels detachering, en de samenstelling van een wervingsreserve van Franstalige en Nederlandstalige commissarissen-auditoren (m/v/x) met specifieke kennis in het domein van de ICT/data voor de Dienst Enquêtes I (*B.S.* 12 juli 2022).

keurde de Commissie voor Comptabiliteit van de Kamer van volksvertegenwoordigers een uitbreiding van het personeelskader van het Vast Comité I goed. Van de zeven full time equivalenten (FTE's) door het Comité gevraagd, kon de Commissie instemmen met een uitbreiding van het kader van twee FTE's (een jurist(e) en een commissaris-auditeur) en dit vanaf 1 april 2023.[264]

X.2. HET 'RIBORN'-PROJECT

Begin 2022 lanceerde het Vast Comité I, met de steun van de FOD Beleid en Ondersteuning, een veranderingstraject dat erop gericht is de organisatie te verbeteren op basis van een gedeelde visie en overleg met de belangrijkste *stakeholders*[265] en dit in een 360°-visie.

Dit project, dat de naam 'RIborn' meekreeg, mobiliseerde het hele jaar door energie, getuige de vergaderingen die regelmatig werden gehouden. In de lokalen van de FOD Beleid en Ondersteuning werd in juni 2022 een *workshop* georganiseerd. Wat dit interne deel van het project betreft, heeft de FOD Beleid en Ondersteuning een samenvattend verslag van de raadpleging van de werknemers afgeleverd, waarin dertien verbeteringsdoelstellingen werden opgenomen. De Comitéleden, zijnde de voorzitter en raadsleden, hebben vervolgens in het laatste kwartaal van het jaar een oefening gehouden om deze verbeteringsdoelstellingen om te zetten in projecten of actieplannen en deze te prioriteren. De afronding van het project wordt voorzien in 2023.

Daarnaast wou het Vast Comité I zijn belangrijkste externe partners raadplegen om de samenwerking te verbeteren. Na een grondige bezinning op basis van nauwkeurige criteria (aard, belang en frequentie van de betrekkingen) werden twaalf *stakeholders* geselecteerd. In dit stadium heeft het projectteam in drie opeenvolgende golven negen *stakeholders*[266] benaderd.

---

264 Rekenhof, Grondwettelijk hof, Hoge Raad voor de Justitie, Vast comité van toezicht op de politiediensten, Vast comité van toezicht op de inlichtingen- en veiligheidsdiensten, Federale ombudsmannen, Gegevensbeschermingsautoriteit, Benoemingscommissies voor het notariaat, BIM-Commissie, Controleorgaan op de politionele informatie, Federale Deontologische Commissie, Centrale Toezichtsraad voor het Gevangeniswezen, Mensenrechteninstituut - Werkzaamheden van de werkgroepen in het kader van het synergieproject - Rekeningen van het begrotingsjaar 2021 - Begrotingsaanpassingen van het begrotingsjaar 2022 - Begrotingsvoorstellen voor het begrotingsjaar 2023, *Parl. St.*, Kamer 2022-2023, nr. 55/3050/001, p. 70 en volgende. Het budget werd gevalideerd in de plenaire zitting van de Kamer van volksvertegenwoordigers op 22 december 2022.

265 *'Samenwerkingsovereenkomst. Opstellen van een nieuwe organisatie-gedragen visie en actieplan voor het Vast Comité van Toezicht op de Inlichtingen- en veiligheidsdiensten'* (10 januari 2022).

266 De VSSE, de ADIV, het OCAD, de BIM-Commissie, de NVO, het Vast Comité P, het COC, de GBA, het College van Procureurs-generaal, de minister van Justitie, de minister van Defensie, de Kamervoorzitster en voorzitster van de Begeleidingscommissie van de Vaste Comités P en I.

X.3. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE

De samenstelling van de Bijzondere commissie belast met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de veiligheids- en inlichtingendiensten (de Begeleidingscommissie) kende in 2022 enkele wijzigingen. Maakten als stemgerechtigde leden deel uit van de commissie: Peter Buysrogge (N-VA), Yngvild Ingels (N-VA), Julie Chanson/Gilles Vanden Burre (Ecolo-Groen), Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Denis Ducarme (MR), Servais Verherstraeten (CD&V), Nabil Boukili (PVDA-PTB), Tim Vandenput (Open Vld) en Bert Moyaers (Vooruit). Kamervoorzitster Eliane Tillieux (PS) neemt het voorzitterschap van de commissie waar. Georges Dallemagne (Les Engagés) neemt deel als niet-stemgerechtigd lid.

In de loop van 2022 vonden vier vergaderingen achter gesloten deuren plaats. Tijdens deze commissievergaderingen werden diverse door het Vast Comité I afgesloten toezichtonderzoeken besproken. De Commissie boog zich ook over het interne functioneren van het Vast Comité I.

Tijdens haar vergadering van 8 juni 2022 werd het algemeen *Activiteitenverslag 2021* besproken.[267] Een aantal thema's weerhielden de bijzondere aandacht van de Voorzitster en de Kamerleden, zoals de opvolging van de in het kader van de parlementaire onderzoekscommissie 'Terroristische Aanslagen' geformuleerde aanbevelingen, de opvolging van politieke mandatarissen, de screening van militairen, de opvolging van voor terrorisme veroordeelde gedetineerden of nog, de veiligheid van de Staat. De Commissie nam als eindconclusie "*akte van het activiteitenverslag 2021 van het Vast Comité I en verleent haar goedkeuring aan de aanbevelingen van het Vast Comité I*".[268]

X.4. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITÉ P

Artikel 52 W.Toezicht voorziet dat minstens twee maal per jaar gemeenschappelijke vergaderingen dient plaats te vinden tussen het Vast Comité I en het Vast Comité P. Gezien de afwezigheid van gemeenschappelijke toezichtonderzoeken, vond slechts één gemeenschappelijke vergadering plaats op 12 oktober 2022.

---

267 De Commissie verwijst daartoe naar artikel 66*bis*, §3, 1°W.Toezicht, zoals gewijzigd bij de wet van 6 januari 2014 tot wijziging van diverse wetten tot hervorming der instellingen (*BS* 31 januari 2014).

268 *Parl. St.* Kamer 2020-21, nr. 55K2745/001, 30 juni 2022 (Activiteitenverslag 2021 van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, Verslag namens de Bijzondere commissie belat met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten).

In 2021 hadden beide Comités aan hun enquêtediensten de opdracht gegeven om werkprocessen voor te bereiden voor de afhandeling van gemeenschappelijke klachten en toezichtonderzoeken. In 2022 kon de finalisering van de gemeenschappelijke procedure voor de afhandeling van klachten worden opgetekend. Het tweede werkproces (aangaande de behandeling van gemeenschappelijke onderzoeken), is nog in ontwikkeling.

Ook blijft het Vast Comité P zijn steun verlenen in het kader van de raadpleging door de Dienst Enquêtes I van de Algemene Nationale Gegevensbank (ANG), in het bijzonder via de noodzakelijke informatiedoorstroming naar aanleiding van technische *updates* en de punctuele coaching van een referentiepersoon wanneer dit nodig mocht blijken.[269] [270]

X.5. DE *DATA PROTECTION OFFICER* OP HET COMITÉ

Sinds mei 2018 stelde het Comité een *Data Protection Officer* (DPO) of functionaris voor gegevensbescherming aan voor de verwerkingen van persoonsgegevens in het kader van de 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 (algemene verordening gegevensbescherming) of AVG, en de 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 betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad. De DPO oefent vanuit de Kamer van volksvertegenwoordigers deze functie ook uit voor een aantal andere dotatiegerechtigde instellingen.

Afgelopen jaar lag naast de wettelijke voorgeschreven taken zoals het informeren en sensibiliseren van het personeel over gegevensbescherming, de focus op adviesverlening van een aantal verwerkingen van persoonsgegevens in het kader van

---

269 De aanwerving, in juni 2021, van een commissaris-auditor met een gerechtelijk profiel en ervaring in het beheer van politie-informatie heeft de capaciteit en de interne competenties aangaande het gebruik van de ANG in de schoot van de Dienst Enquêtes I versterkt.

270 In oktober 2017 ondertekende het Vast Comité I een protocolakkoord met de Federale Politie aangaande de toepassing van het Koninklijk Besluit van 30 oktober 2015 betreffende de rechtstreekse toegang van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten en de Dienst Enquêtes ervan tot de gegevens en de informatie van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt (BS 20 november 2015).

personeelsbeheer en -administratie.[271] De bedoeling is om ook de persoonsleden nog gerichter te informeren over de verwerkingen van hun persoonsgegevens door het Vast Comité I als verwerkingsverantwoordelijke.

X.6. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Het 'budget 2022' van het Vast Comité I werd vastgelegd op 5,215 miljoen euro, wat identiek was aan het budget van 2021.[272]

De financieringsbronnen van het budget werden door de Kamer van volksvertegenwoordigers[273] als volgt toegewezen: 74,93 % dotatiebudget en 21,53 % boni van 2020 en 3,54% boni (hypothetisch) van 2021.

De uitvoering van het budget 2021 leverde een budgettaire bonus op van 1,616 miljoen euro, te weten het vastgestelde verschil tussen de inkomsten en de samengestelde uitgaven.

Het budget is traditiegetrouw gebaseerd op verschillende financieringsbronnen en de enige nieuwe bijdrage in termen van eigen beheer, staat ingeschreven in de dotatie van de algemene uitgavenbegroting van de Staat. Tot 2017 was deze dotatie onvoldoende om de reële uitgaven van het Comité te dekken, wat een structureel verlies als gevolg met zich meebracht. De tendens om zoveel mogelijk artikel 57, lid 1, W.Toezicht toe te passen hetwelke vermeldt dat de kredieten die noodzakelijk zijn voor de werking dienen te worden uitgetrokken op de begroting van de dotaties, laat heden ten dage het Comité toe zijn activiteiten te financieren.

Het aanzienlijk boekhoudkundig overschot is vooral te wijten aan het tijdsverloop tussen de goedkeuring van de begroting en met name de daadwerkelijke indiensttreding van het personeel als gevolg van de langdurige aanwervingsprocedures en het verkrijgen van de vereiste veiligheidsmachtigingen. Dit leverde, samen met de bevriezing van het budget voor het digitaliseringsproject (zie hierboven), waartoe de Kamer heeft besloten, een aanzienlijke boni op.

---

271 De functionaris voor gegevensbescherming verleende een intern advies inzake camerabewaking waarbij een register werd opgesteld en de aangifte werd geformaliseerd naar aanleiding van de zgn. 'nieuwe Camerawet' (Wet van 30 juli 2018 tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's met het oog op het verbeteren van de samenhang van de tekst en de overeenstemming ervan met de Algemene Verordening Gegevensbescherming (AVG), BS 31 augustus 2018).

272 *Hand.* Kamer 2020-21, CRIV55PLEN154, 17.

273 *Parl. St.* Kamer 2020-21, 55K01676/001, 30-34.

X.7. IMPLEMENTATIE VAN DE AANBEVELINGEN VAN DE AUDIT VAN HET REKENHOF

Op verzoek van de Commissie van de Comptabiliteit van de Kamer van volksvertegenwoordigers startte het Rekenhof al in december 2017 samen met Ernst and Young een onderzoek naar de dotatiegerechtigde instellingen. Het auditverslag, daterend van eind maart 2018, formuleerde aanbevelingen voor de 'opdrachten' van de negen bij de audit betrokken dotatiegerechtigde instellingen, waaronder het Vast Comité I.[274]

In april 2021 werd in de schoot van de Commissie voor de Comptabiliteit een akkoord bereikt over de synergiën die tussen de betrokken instellingen op gang moeten worden gebracht. Het gaat onder meer om de oprichting van een gemeenschappelijk dienstencentrum. Verder werd besloten het statuut en de salarisschalen van het personeel van de betrokken instellingen te harmoniseren en het wagenpark van de instellingen te rationaliseren.

De werkzaamheden werden in de loop van 2022 verdergezet, voornamelijk met een wetsvoorstel aangaande de harmonisering van de statuten. Het Comité organiseerde interne vergaderingen om zijn medewerkers hieromtrent te informeren, en, in de mate van het mogelijke, een antwoord te bieden op hun vragen en bedenkingen.

In het kader van de mogelijke verhuis van de BIM-Commissie in een gedeelte van de kantoren van het Vast Comité I, werd aan de Kamer een raming van de kosten die een dergelijke verhuis met zich zou meebrengen, bezorgd.

X.8. VORMING

In het belang van zijn organisatie, moedigt het Vast Comité I zijn leden en medewerkers aan om algemene (informatica, management…) of sectoreigen opleidingen en conferenties te volgen.

In 2022 namen een of meerdere personeelsleden van het Vast Comité I deel aan de in de tabel hieronder opgenomen studiedagen of opleidingen.

274 *Parl. St.* Kamer 2018-19, 54K3418/003.

DATUM	TITEL	ORGANISATOR	PLAATS
26-27 januari 2022	Intelligence, surveillance & oversight: tracing connections & contestations	GUARDINT	On line
Maart – april 2022	Opleiding vertrouwenspersoon (N)	IDEWE	Leuven
12 mei 2022	Fusion Conference: La communication polarisante en tant que vecteur de radicalisation	Egmont Instituut en het Orgaan voor de Coördinatie van de Analyse van de Dreiging (OCAD)	Brussel
19 mei 2022	Extreme Right: what are the risks for Belgium?	Royal Higher Institute for Defense	Brussel
Mei – juni 2022	Opleiding vertrouwenspersoon (F)	Securex	Brussel
14 juni 2022	Public Security Exhibition 2022	British Embassy Brussels & ADS Group	Brussel
1-4 september 2022	Pan-European Conference on International Relations	European International Studies Association	Athens
5-9 september 2022	Formation de rappel pour les réservistes de la Défense	School voor Inlichting en Veiligheid	Heverlee
5 oktober 2022	Wapengebruik en schietoefeningen	Defensie	Leopoldsburg
10 oktober 2022	Wapengebruik en schietoefeningen	Defensie	Brussel
28 oktober 2022	Rétention des données	Groupe de Recherche en matière Pénale et Criminelle (GREPEC) de l'Université Saint-Louis à Bruxelles & Vrije Universiteit Brussel	Brussel
September – december 2022	Hogere Studies Veiligheid en Defensie (4e cyclus)	Koninklijk Hoger Instituut voor Defensie	Brussel
September – december 2022	Opleiding IT	VSSE	Brussel
November – december 2022	Opleiding IT	VSSE	Brussel
5 december 2022	Fusion Conference: Vijf jaar LIVC-R. Good practices, lessen en uitdagingen	Egmont Instituut en het Orgaan voor de Coördinatie van de Analyse van de Dreiging (OCAD)	Brussel

In oktober 2022 lichtte een medewerkster van het Comité tijdens een interne presentatie de resultaten van haar doctoraat over het OCAD en de organisatie van de strijd tegen terrorisme, toe.

HOOFDSTUK XI.
AANBEVELINGEN

Op basis van de in 2022 afgesloten toezichtonderzoeken, controles en inspecties formuleert het Vast Comité I onderstaande aanbevelingen. Zij hebben zowel betrekking op op de coördinatie en de efficiëntie van de inlichtingendiensten, het Coördinatieorgaan voor de dreigingsanalyse (OCAD) en de ondersteunende diensten als op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I.[275]

XI.1. AANBEVELINGEN IN VERBAND MET DE COÖRDINATIE EN DE EFFICIËNTIE VAN DE INLICHTINGENDIENSTEN, HET OCAD EN DE ONDERSTEUNENDE DIENSTEN

XI.1.1. HET VERSTERKEN VAN DE UITWISSELING VAN INFORMATIE TUSSEN DE VSSE EN DE GEVANGENISSEN[276]

Het Comité verzoekt de minister van Justitie om regelmatig informatiesessies te organiseren binnen elke penitentiaire inrichting om erop toe te zien dat alle gevangenissen worden gesensibiliseerd voor het belang van informatie-uitwisseling met de VSSE.

XI.1.2. INVESTEREN IN RELATIES MET DE SOCIOPREVENTIEVE ACTOREN

Het Comité beveelt de VSSE aan om een actieplan uit te werken met als doel te investeren in haar relaties met de sociopreventieve actoren[277], niet alleen om informatie te verzamelen, maar om elk gevoel van wantrouwen te ondervangen, en

---

275 In 2022 werden geen aanbevelingen geformuleerd die specifiek betrekking hadden op de bescherming van de rechten die de Grondwet ende wet aan personen verlenen.

276 De aanbevelingen opgenomen in de punten XI.2.1. tot en met XI.2.8. zijn ontleend aan het toezichtonderzoek naar de opvolging van vrijgelaten terro-veroordeelden door de VSSE (zie Hoofdstuk I.1.).

277 Het betreft *in casu* leerkrachten, CLB-medewerkers, welzijns- en geozndheidsmedewerkers, VDAB-consulenten, jeugdwerkers…

dit door een bredere denkoefening te organiseren rond het fenomeen van radicalisering in de gevangenis en de psychosociale drijfveren ervan.

XI.1.3. OPERATIONALISERING EN EVALUATIE VAN HET PILOOTPROJECT VEILIGHEIDSCOÖRDINATOREN IN GEVANGENISSEN

Het proefproject van het Directoraat-generaal Penitentiaire Inrichtingen (DG EPI) in verband met veiligheidscoördinatoren[278], dat in december 2021 werd gelanceerd, kan pas op middellange termijn worden geëvalueerd. Hoewel dit volgens het Comité een veelbelovend project is, moet er een evaluatie worden gemaakt van enerzijds de verenigbaarheid van een dergelijke functie met de managementtaken en anderzijds van de nadere regels voor samenwerking met de VSSE. Het Comité moedigt daarom het overleg tussen de VSSE en het DG EPI aan met betrekking tot de operationalisering van de opdrachten en de opleiding van deze veiligheidscoordinatoren. Het Comité vraagt aan de minister van Justitie om in de eerste helft van 2024 een evaluatieverslag aan het Comité te bezorgen met betrekking tot het proefproject.

XI.1.4. DE REALISATIE VAN HET (NIEUW) PROTOCOLAKKOORD TUSSEN DE VSSE EN HET DG EPI[279]

Het Comité vraagt aan de minister van Justitie om in het protocolakkoord tussen de VSSE en het DG EPI toelichting te verschaffen bij de concrete samenwerking tussen de VSSE en de veiligheidscoördinatoren en alle maatregelen te nemen die nodig zijn om het protocol, waarover de besprekingen al lopen sinds 2016, af te werken tegen eind 2022.

XI.1.5. VOORZICHTIGHEID INZAKE GEGEVENSUITWISSELING MET BUITENLANDSE PARTNERS

Het Comité nodigt de VSSE uit om de nodige voorzichtigheid aan de dag te leggen bij de uitwisseling met sommige buitenlandse partners van de lijst van gedetineerden die voorkomen in de Gemeenschappelijke Gegevensbank *Terrorist Fighters*

---

278 Het gaat om personen van de DG EPI die het aanspreekpunt zijn voor de Veiligheid van de Staat, en tegelijkertijd instaan voor een betere risicotaxatie.

279 In haar voorwoord refereert de Administrateur-generaal a.i. naar een ondertussen getekend akkoord met DG EPI *"dat onder meer de inhoudelijke en wettelijke bepalingen regelt in de informatiedoorstroming tussen beide diensten"*. In VSSE, *Intelligence report 2021-2022* (www.vsse.be).

(GGB TF) en aan het eind van hun straf komen. Bovendien roept het Comité op tot grotere bedachtzaamheid wat betreft de inachtneming van het recht om te worden vergeten voor gedetineerden die hun straf hebben uitgezeten en volgens de Belgische diensten niet langer een bedreiging vormen. Het Comité wijst er ook nog op dat het opvragen van lijsten van de GGB is onderworpen aan strikte en cumulatieve wetsbepalingen.[280]

XI.1.6. EEN NAUWERE SAMENWERKING TUSSEN DE ADIV EN DE VSSE VAN WEGENS TERRORIMSE VEROORDEELDE EN/OF GERADICALISEERDE (EX-) GEDETINEERDEN

Het Comité vestigt de aandacht van de ADIV op de zeer restrictieve interpretatie door deze dienst van zijn bevoegdheid in de opvolging van wegens terrorisme veroordeelde en/of geradicaliseerde (ex-)gedetineerden. Het Comité beveelt aan om de bestaande contacten met de VSSE binnen het platform CT te behouden en verder te versterken met als doel te garanderen dat het – in de eerste plaats theoretische – actieterrein van de ADIV niets uitsluit in het kader van de opvolging van (ex-)terro- en/of geradicaliseerde gedetineerden.

XI.1.7. TOEGANG VAN DE ADIV TOT SIDIS SUITE

Het Comité vraagt aan de ministers van Defensie en Justitie om een koninklijk besluit aan te nemen om de toegang van de ADIV tot SIDIS Suite effectief te maken. Het Comité beveelt aan de ADIV aan om vervolgens interne procedures uit te werken betreffende de toegang tot deze software en de nadere regels voor het gebruik ervan.

XI.1.8. WETENSCHAPPELIJKE ONDERZOEKEN ONDERSTEUNEN AANGAANDE TERRORISTISCHE RECIDIVE

De omvang en factoren van terroristische recidive blijven vaag. Het Comité moedigt de minister van Justitie ertoe aan om projecten van wetenschappelijk onderzoek over deze materie te ondersteunen om een beter beeld te krijgen van het fenomeen van recidive bij individuen die zijn veroordeeld wegens terrorisme. De resultaten van dergelijk onderzoek moeten met de inlichtingendiensten worden

[280] Zie VAST COMITÉ I, *Activiteitenverslag 2018*, 94 ('VI.2.4. Over de informatie aan de burgemeesters en de doorgifte van (uittreksels) van informatiekaarten of van lijsten aan derde instanties') en VAST COMITÉ I, *Activiteitenverslag 2019*, 86-87 ('VI.2.2.6. Doorgifte van lijsten').

gedeeld, waardoor zij hun strategie en middelen zullen kunnen aanpassen in functie van de reële behoeften.

XI.1.9. BELEIDSRICHTLIJNEN OVER BUITENLANDSE ACTIVITEITEN[281]

Het Comité benadrukt dat elke inzet van extra inlichtingencapaciteit in het buitenland zorgvuldig moet worden overwogen, gezien de vele risico's die hieraan verbonden zijn. Zo houdt het verzamelen van inlichtingen in het buitenland risico's in voor de internationale betrekkingen van België. Het is derhalve passend dat de kosten-batenoefening van een eventuele inlichtingenoperatie in het buitenland door de regering wordt geëvalueerd en beoordeeld. Aangezien in dit geval de bevoegdheden van meerdere ministers worden aangesproken, beveelt het Vast Comité I aan dat de Nationale Veiligheidsraad zich over deze kwestie buigt en dat deze raad bepaalt hoe de inlichtingenactiviteiten in het buitenland en de gevolgen daarvan voor de internationale betrekkingen dienen te worden gecoördineerd.

XI.1.10. VERMIJDEN VAN DOUBERLING BIJ INTERNATIONALE ACTIVITEITEN

Het Comité beveelt aan om de ontwikkeling van eventuele activiteiten in het buitenland, waar mogelijk, te integreren in een globale aanpak met de ADIV, en dit om interferenties en doublering van activiteiten te vermijden.

XI.1.11. SYNERGIE EN COMPLEMENTARITEIT IN DE UITBOUW VAN EEN NETWERK VAN VERBINDINGSOFFICIEREN

Het Vast Comité I herhaalt dat het de inzet van verbindingsofficieren - zowel op operationeel niveau als wat betreft het diplomatieke type - als een duidelijke meerwaarde beschouwt. De uitbouw van een dergelijk netwerk verdient de nodige aandacht van de VSSE. De inzet van dergelijke verbindingsofficieren moet evenwel gebeuren in een context van complementariteit en synergie met nationale partners, *in casu* de ADIV en de Federale Politie.[282]

---

281 De aanbevelingen opgenomen in de punten XI.2.9. tot en met XI.2.11. zijn ontleend aan het toezichtonderzoek naar de buitenlandse inlichtingencapaciteiten van de VSSE (zie Hoofdstuk I.2.).

282 Zie in die zin het in september 2020 door de Federale Politie en de VSSE ondertekende protocolakkoord dat de samenwerking regelt tussen de Veiligheid van de Staat en de verbindingsofficieren van de Belgische politie in het buitenland.

XI.1.12. EEN TASKFORCE EN EEN NATIONAAL PLAN VOOR DIGITALE VEILIGHEID[283]

Om haar informatiepositie ten aanzien van digitale bedreigingen, en daarmee de preventie van en reactie op deze bedreigingen, te verbeteren, verzoekt het Vast Comité I de Regering om binnen zes maanden een alomvattende en geïntegreerde nationale *taskforce* op te richten naar het model van andere *taskforces* die reeds voor crisissituaties zijn opgericht. Dit kan een specifiek strategisch en politiek orgaan zijn dat aanbevelingen zal opstellen om digitale bedreigingen doeltreffend te voorkomen en te bestrijden. Deze *taskforce* zal ook verantwoordelijk zijn voor het opstellen van een Nationaal Plan voor Digitale Veiligheid, naar het model van andere nationale veiligheidsplannen.

XI.1.13. REGELMATIGE RISICOANALYSES OVER HET GEBRUIK VAN *REMOTE INFECTION TECHNOLOGIES*

Het Vast Comité I is van oordeel dat zowel de inlichtingen- als de veiligheidsdiensten meer aandacht moeten besteden aan de bedreigingen die de nieuwe technologische mogelijkheden kunnen inhouden op het gebied van informatiegaring en economische en politieke spionage, zelfs indien deze risico's afkomstig zijn van landen waarmee zij strategische betrekkingen onderhouden. In dit verband beveelt het Comité aan dat de twee inlichtingendiensten regelmatig risicoanalyses uitvoeren, met bijzondere aandacht voor de risico's die verbonden zijn aan de aanwezigheid van talrijke internationale instellingen op het Belgische grondgebied.

XI.1.14. HET ONTWIKKELING VAN EIGEN EN GEMEENSCHAPPELIJKE *TOOLS* VOOR DE VSSE EN DE ADIV

Met het oog op een betere coördinatie en efficiëntie moeten de twee Belgische inlichtingen- en veiligheidsdiensten hun technische/technologische capaciteiten zoals *Remote Infection Technologies* bundelen. Het Vast Comité I verzoekt de ministers van Justitie en van Defensie te investeren in de ontwikkeling van hun eigen instrumenten. Het Comité beveelt aan om in geval van inschakeling van partners een versterkte controle op wettigheid en subsidiariteit te organiseren.

---

283 De aanbevelingen opgenomen in de punten XI.2.12. tot en met XI.2.15. zijn ontleend aan het toezichtonderzoek naar het gebruik van de Pegasus-software (zie Hoofdstuk I.5.).

XI.2. AANBEVELINGEN IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

XI.2.1. DE CONTROLECAPACITEIT VAN HET VAST COMITÉ I[284]

Het Vast Comité I beveelt aan zijn capaciteiten aan te passen aan de versterking van de personeelscapaciteit van de inlichtingendiensten, zodat het al zijn wettelijke taken kan vervullen, hetgeen thans niet meer het geval is.

[284] Zie onder meer Hoofdstuk 'I.5. De onthullingen over het gebruik van de Pegasus-software'.

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 2022 TOT 31 DECEMBER 2022)

Wet van 9 december 2021 houdende instemming met de overeenkomst tussen het Koninkrijk België en het Koninkrijk Spanje inzake de uitwisseling en wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 15 oktober 2015, *BS* 21 februari 2022

Wet van 9 december 2021 houdende instemming met de overeenkomst tussen het Koninkrijk België en Hongarije inzake de uitwisseling en wederzijdse bescherming van geclassificeerde informatie, gedaan te Boedapest op 21 september 2015, *BS* 4 maart 2022

Wet van 9 december 2021 houdende instemming met de overeenkomst tussen het Koninkrijk België en de Republiek Finland inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Helsinki op 20 juli 2016, *BS* 22 maart 2022

Wet van 26 mei 2016 houdende instemming met het samenwerkingsverdrag tussen de regering van het Koninkrijk België en de regering van het Koninkrijk Marokko inzake de bestrijding van de georganiseerde criminaliteit en het terrorisme, opgemaakt te Brussel op 18 februari 2014, *BS* 20 mai 2022

Wet van 14 juli 2022 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, *BS* 5 augustus 2022

Wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, *BS* 5 augustus 2022

Wet van 20 juli 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, *BS* 8 augustus 2022

Wet van 20 juli 2022 tot wijziging van de wet van 23 mei 2017 houdende de militaire programmering van investeringen voor de periode 2016- 2030, *BS* 2 september 2022

Wet van 11 september 2022 tot invoering van een algemene declassificatieregeling van de geclassificeerde stukken (nieuw opschrift), *BS* 27 september 2022

Wet van 31 mei 2022 tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging, *BS* 19 oktober 2022

Wet van 13 oktober 2022 tot wijziging van het Belgisch Scheepvaartwetboek betreffende de maritieme beveiliging, *BS* 26 oktober 2022

Wet van 25 april 2022 tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, wat de verplichting voor de Dienst Enquêtes van het Comité P betreft om in het geval van een strafonderzoek de bevoegde tuchtrechtelijke overheid in te lichten over het bestaan van een mogelijke tuchtrechtelijke fout, *BS* 28 november 2022

Wet van 8 december 2022 betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie, *BS* 23 december 2022

Wet van 26 december 2022 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2023, *BS* 30 december 2022

K.B. van 14 maart 2022 betreffende de postdiensten, *BS* 18 maart 2022

K.B. van 29 maart 2022 tot wijziging van het koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid, *BS* 7 avril 2022

K.B. van 29 maart 2022 tot wijziging van het koninklijk besluit van 13 december 2006 houdende het statuut van de ambtenaren van de buitendiensten van de Veiligheid van de Staat, *BS 27* avril 2022

K.B. van 14 juni 2022 tot wijziging van het ministerieel besluit van 29 juli 1987 houdende oprichting van de basisoverlegcomités voor de Federale Overheidsdienst Justitie en aanduiding van hun voorzitters en tot opheffing van het ministerieel besluit van 24 oktober 2014 houdende samenstelling van het Basisoverlegcomité van het Belgisch Staatsblad, *BS 25* juillet 2022

K.B. van 16 oktober 2022 tot uitvoering van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, en tot wijziging van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, *BS* 24 oktober 2022

K.B. van 30 juli 2022 besluit van betreffende de toekenning van een toelage betreffende de bestrijding van terrorisme en extremisme in het kader van de implementatie van een lokaal beleid voor veiligheid en preventie voor het jaar 2022, *BS* 24 oktober 2022

K.B. van 30 juli 2022 besluit betreffende de toekenning van een toelage in het kader van de implementatie van een lokaal beleid voor veiligheid en preventie voor het jaar 2022, *BS* 24 oktober 2022

K.B. van 2 oktober 2022 tot wijziging van het koninklijk besluit van 4 juli 2014 tot vaststelling van het statuut van bepaalde burgerlijke ambtenaren van het stafdepartement inlichtingen en veiligheid van de Krijgsmacht, *BS* 29 november 2022

M.B. van 16 juni 2022 tot bepaling van de voorgeschreven uitrusting van de agenten van de Veiligheid van de Staat en tot vaststelling van bijzondere bepalingen betreffende het voorhanden hebben, het dragen en het bewaren van de bewapening, *BS* 19 oktober 2022

Uittreksel uit arrest nr. 158/2021 van 18 november 2021, rolnummer 6672, in zake: het beroep tot vernietiging van de wet van 1 september 2016 'tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst', ingesteld door P. Van Assche en anderen, *BS* 17 februari 2022

Veiligheid van de Staat - tijdelijke aanwijzing - bij ministerieel besluit van 18 mei 2022 wordt mevrouw Francisca BOSTYN, adviseur-generaal bij de Federale Overheidsdienst Justitie, vast benoemd in de klasse A4, tijdelijk aangeduid om de functie van administrateur-generaal van de Veiligheid van de Staat uit te oefenen, met ingang van 2 mei 2022, *BS* 27 mei 2022

Activiteitenverslag 2021 van het Vast Comité van Toezicht op de inlichtingenen veiligheidsdiensten, *BS* 30 juni 2022

Aanwerving bij wijze van detachering en samenstelling van een wervingsreserve van Franstalige en Nederlandstalige Commissarissen- auditors met een bijzondere kennis van ICT/Data (m/v/x) voor de Dienst Enquêtes van het Vast Comité I, *BS* 12 juli 2022

Bericht voorgeschreven bij artikel 3*quater* van het besluit van de Regent van 23 augustus 1948 tot regeling van de rechtspleging voor de afdeling bestuursrechtspraak van de Raad van State. De vzw Syndicaat van de Belgische Politie 'Sypol.be' heeft de nietigverklaring gevorderd van het koninklijk besluit van 29 maart 2022 tot wijziging van het koninklijk besluit van 13 december 2006 houdende het statuut van de ambtenaren van de buitendiensten van de Veiligheid van de Staat, *BS* 10 augustus 2022

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten - aanwerving voor onmiddellijke indiensttreding en samenstelling van een wervingsreserve van een Franstalige statutaire secretaris/secretaresse (m/v/x), (niv. B), *BS* 6 september 2022

Uittreksel uit arrest nr. 33/2022 van 10 maart 2022, Rolnummer 7330. In zake: het beroep tot gedeeltelijke vernietiging van de wet van 22 mei 2019 'tot wijziging van diverse bepalingen wat het politionele informatiebeheer betreft', ingesteld door de vzw 'Ligue des droits humains', *BS* 18 november 2022

Vergelijkende selecties, voorafgaande proeven in de vergelijkende selecties, resultaten van de vergelijkende selecties van:

Nederlandstalige Data officers (m/v/x) (niveau B) voor de Veiligheid van de Staat - selectienummer: ANG21452, *BS* 13 januari 2022

Franstalige Data officers (m/v/x) (niveau B) voor de Veiligheid van de Staat - selectienummer: AFG21328, *BS* 13 januari 2022

Nederlandstalige Surveillance officers (m/v/x) (niveau B) voor de Veiligheid van de Staat - selectienummer: ANG21457, *BS* 17 13 januari 2022

Nederlandstalige Technical officers (m/v/x) (niveau B) voor de Veiligheid van de Staat. - selectienummer: ANG21458, *BS* 13 januari 2022

Franstalige Surveillance officers (m/v/x) (niveau B) voor de Veiligheid van de Staat - selectienummer: AFG21332, *BS* 17 13 januari 2022

Franstalige Technical officers (m/v/x) (niveau B) voor de Veiligheid van de Staat - selectienummer: AFG21333, *BS* 17 13 januari 2022

Nederlandstalige Analisten veiligheidsmachtiging (m/v/x) (niveau A1) voor het Ministerie van Defensie - selectienummer: ANG22016, *BS* 18 januari 2022

Franstalige ICT-experts voor het Cyberdefense Laboratory (m/v/x) (niveau B) voor het Ministerie van Defensie. - selectienummer: AFG22133, *BS* 2 mei 2022

Resultaat van de vergelijkende selectie van Franstalige Technical Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat - selectienummer: AFG21333, *BS* 15 juin 2022

Resultaat van de vergelijkende selectie van Nederlandstalige Data Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat - selectie-nummer: ANG21452, *BS* 15 juin 2022

Franstalige Support Officers (m/v/x) (niveau C) voor Velligheid van de Staat - selectie-nummer: AFG22248, *BS* 29 augustus 2022

Franstalige Masters (m/v/x) (niveau A1) voor Velligheid van de Staat - selectienummer: AFG22249, *BS* 29 augustus 2022

Nederlandstalige Support Officers (m/v/x) (niveau C) voor Velligheid van de Saat - selectienummer: ANG22350, *BS* 29 augustus 2022

Nederlandstalige Masters (m/v/x) (niveau A1) voor Velligheid van de Saat - selectie-nummer: ANG22351, *BS* 29 augustus 2022

Nederlandstalige Bachelors (m/v/x) (niveau B) voor Velligheid van de Saat - selectienummer: ANG22386, *BS* 19 september 2022

Franstalige Bachelors (m/v/x) (niveau B) voor Velligheid van de Staat - selectienummer: AFG22268, *BS* 19 september 2022

Franstalige Psychologen (m/v/x) (niveau A1) voor de Veiligheid van de Staat - selectienummer: AFG22337, *BS* 28 oktober 2022
Resultaat van de vergelijkende selectie van Franstalige Masters (m/v/x) (niveau A1) voor de Veiligheid van de Staat - selectienummer: AFG22249, *BS* 9 november 2022
Resultaat van de vergelijkende selectie van Nederlandstalige Masters (m/v/x) (niveau A1) voor de Veiligheid van de Staat - selectienummer: ANG22351, *BS* 9 november 2022
Resultaat van de vergelijkende selectie van Franstalige Bachelors (m/v/x) (niveau B) voor de Veiligheid van de Staat - selectienummer: AFG22268, *BS* 16 november 2022
Resultaat van de vergelijkende selectie van Nederlandstalige Bachelors (m/v/x) (niveau B) voor de Veiligheid van de Staat - selectienummer: ANG22386, *BS* 16 november 2022

BIJLAGE B.
OVERZICHT VAN DE BELANGRIJKSTE WETSVOORSTELLEN, WETSONTWERPEN, RESOLUTIES, ORDE MOTIES EN PARLEMENTAIRE BESPREKINGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2022 TOT 31 DECEMBER 2022)

Senaat

Verzoek tot het opstellen van een informatieverslag ter bestrijding van de inmenging door buitenlandse mogendheden met het oog op het ondermijnen van de democratische rechtsstaat, *Parl. St.* Senaat 2021-22, nr. 7- 344/1 en *Hand*. Kamer 2021-22, 29 april 2022, nr. 7-28, 15
Voorstel van resolutie met betrekking tot een meldingsplicht voor universiteiten en bedrijven die samenwerken met autoritaire regimes in risicosectoren, *Parl. St.* Senaat 2021-22, nr. 7-373/1

Kamer van volksvertegenwoordigers

Wetsvoorstel tot invoering van een algemene declassificatieregeling voor geclassificeerde stukken, Parl. St. Kamer 2021-22, nr. 55K0732/003
Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten - benoeming van de tweede plaatsvervanger van het Nederlandstalig lid - ingediende kandidaturen, *Hand*. Kamer 2021-22, 13 januari 2022, CRIV55PLEN157, 86
Wetsvoorstel tot wijziging van de wet van 29 juli 1934 waarbij de private milities verboden worden wat het verbod van ondemocratische groeperingen betreft, wetsvoorstel tot strafbaarstelling van het behoren tot of het samenwerken met een groepering die discriminatie of segregatie voorstaat, wetsvoorstel tot wijziging van de wet van 29 juli 1934 waarbij de private milities verboden worden, teneinde het in die wet vervatte verbod uit te breiden tot de verenigingen die aanzetten tot haat, discriminatie of geweld, en teneinde de ontbinding van die verenigingen door de uitvoerende macht mogelijk te maken, Parl. St. Kamer 2021-22, nr. 55K0943/003
Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, wat de verplichting voor de Dienst Enquêtes van het Comité P betreft om in het geval van een gerechtelijk onderzoek de bevoegde tuchtrechtelijke overheid in te lichten over het bestaan van een mogelijke tuchtrechtelijke fout, Parl. St. Kamer 2021-22, nr. 55K1985/005

Wetsontwerp tot invoering van bijkomende beveiligingsmaatregelen voor de verstrekking van mobiele 5G- diensten, Parl. St. Kamer 2021-22, nr. 55K2317/008

Wetsontwerp houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, Parl. St. Kamer 2021-22, nr. 55K2443/001

Wetsontwerp tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging, Parl. St. Kamer 2021-22, nrs. 55K2495/001 tot 55K2495/010

Wetsontwerp houdende instemming met de Overeenkomst tussen de Regering van het Koninkrijk België en de Regering van de Italiaanse Republiek inzake de uitwisseling en wederzijdse bescherming van geclassificeerde informatie, gedaan te Rome op 31 januari 2017, Parl. St. Kamer 2021-22, nr. 55K2555/001

Wetsvoorstel tot wijziging van het Strafwetboek wat de terbeschikkingstelling van de strafuitvoeringsrechtbank betreft, Parl. St. Kamer 2021-22, nr. 55K2571/001

Wetsontwerp betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten, Parl. St. Kamer 2021-22, nrs. 55K2572/001 tot 55K2572/007 en algemene bespreking (*Hand.* Kamer 2021-22, 7 juli 2022, CRIV55PLEN192, 44)

Voorstel van resolutie tot een versterkte aanpak van extremistische groeperingen, Parl. St. Kamer 2021-22, nr. 55K2585/001

Benoeming van de griffier van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Parl. St. Kamer 2021-22, nr. 55K2597/001 en uitslag van de geheime stemming invasie *(Hand.* Kamer 2021-22, 24 maart 2022, CRIV55PLEN171, 75)

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten - benoeming van de tweede plaatsvervanger van het Nederlandstalig lid (*Hand.* Kamer 2021-22, 24 maart 2022, CRIV55PLEN171, 67)

Wetsvoorstel tot wijziging van diverse wetten, wat de afbakening van het misdrijf van aanzetten tot haat betreft, Parl. St. Kamer 2021-22, nr. 55K2606/001

Voorstel van resolutie waarin wordt gevraagd om het Belgische defensiebudget tegen 2030 op 2% van het bruto binnenlands product te brengen, Parl. St. Kamer 2021-22, nr. 55K2619/001

Wetsvoorstel tot wijziging van de wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren wat de verplichting van het gebruik van unidirectionele netwerken betreft, Parl. St. Kamer 2021-22, nrs. 55K2635/001

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten - eretitel (*Hand.* Kamer 2021-22, 19 mai 2022, CRIV55PLEN181, 58)

Wetsontwerp inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit, Parl. St. Kamer 2021-22, nrs. 55K2693/001 en algemene bespreking (*Hand.* Kamer 2021-22, 14 juli 2022, CRIV55PLEN195, 23)

Wetsontwerp tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, Parl. St. Kamer 2021-22, nr. 55K2706/001 en algemene bespreking (*Hand.* Kamer 2021-22, 7 juli 2022, CRIV55PLEN192, 53)

Wetsontwerp tot wijziging van het Belgisch Scheepvaartwetboek betreffende de maritieme beveiliging, Parl. St. Kamer 2021-22, nr. 55K2734/001

Wetsontwerp tot wijziging van de wet van 23 mei 2017 houdende de militaire programmering van investeringen voor de periode 2016-2030, Parl. St. Kamer 2021-22, nrs. 55K2737/001, 55K2737/003 en 55K2737/004, algemene bespreking (*Hand.* Kamer 2021-22, 13 juli 2022, CRIV55PLEN194, 22) en aangehouden amendement (*Hand.* Kamer 2021-22, 14 juli 2022, CRIV55PLEN195, 68)

Wetsvoorstel tot invoering van een algemene declassificatieregeling voor geclassificeerde stukken, Parl. St. Kamer 2021-22, nrs. 55K2739/001 tot 55K2739/006, algemene bespreking (*Hand.* Kamer 2021-22, 19 juli 2022, CRIV55PLEN196, 22), aangehouden amendementen en artikelen (*Hand.* Kamer 2021-22, 20 juli 2022, CRIV55PLEN201, 51) en geheel van het wetsvoorstel (*Hand.* Kamer 2021-22, 20 juli 2022, CRIV55PLEN201, 52)

Activiteitenverslag 2021 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Parl. St. Kamer 2021-22, nr. 55K2745/001

Voorstel van resolutie betreffende de bevordering van een performanter cybersecuritybeleid ter ondersteuning van onze bedrijven en organisaties in de strijd tegen cybercrime, Parl. St. Kamer 2021-22, nr. 55K2771/001

Wetsontwerp houdende instemming met de volgende internationale akten: 1) de overeenkomst tussen het Koninkrijk België en de Republiek India inzake wederzijdse rechtshulp in strafzaken, gedaan te Brussel op 16 september 2021, en 2) de overeenkomst tussen het Koninkrijk België en de Verenigde Arabische Emiraten inzake wederzijdse rechtshulp in strafzaken, gedaan te Abu Dhabi op 9 december 2021, en 3) het verdrag tussen het Koninkrijk België en de Verenigde Arabische Emiraten inzake uitlevering, gedaan te Abu Dhabi op 9 december 2021, en 4) het verdrag tussen het Koninkrijk België en de Islamitische Republiek Iran inzake overbrenging van gevonniste personen, gedaan te Brussel op 11 maart 2022, en 5) het protocol van 22 november 2017 ter amendering van het aanvullend protocol bij de conventie inzake de overbrenging van gevonniste personen, ondertekend op 7 april 2022 te Straatsburg (2784/1-4) (*Hand.* Kamer 2021-22, 19 juli 2022, CRIV55PLEN197, 1) en (*Hand.* Kamer 2021-22, 20 juli 2022, CRIV55PLEN201, 48)

Wetsontwerp tot wijziging van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit, Parl. St. Kamer 2021-22, nr. 55K2793/001

Wetsontwerp houdende instemming met de overeenkomst tussen het Koninkrijk België en het Koninkrijk der Nederlanden inzake de uitwisseling en wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 5 november 2019, Parl. St. Kamer 2021-22, nr. 55K2796/001

Wetsontwerp houdende instemming met de overeenkomst tussen de regering van het Koninkrijk België en de regering van het Verenigd Koninkrijk van Groot-Brittannië en Noord-Ierland betreffende de bescherming van geclassificeerde informatie, gedaan te Brussel op 1 december 2020, Parl. St. Kamer 2021-22, nr. 55K2797/001

Wetsvoorstel tot wijziging van de wet van 4 juli 1989 betreffende de beperking en de controle van de verkiezingsuitgaven voor de verkiezing van de Kamer van volksvertegenwoordigers, de financiering en de open boekhouding van de politieke partijen teneinde de buitenlandse financiering van politieke partijen te verbieden, Parl. St. Kamer 2021-22, nr. 55K2905/001

Wetsontwerp betreffende de meldingskanalen en de bescherming van de melders van integriteitsschendingen in de federale overheidsinstanties en bij de geïntegreerde politie, Parl. St. Kamer 2021-22, nr. 55K2952/001

Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, teneinde het Comité P te belasten met het uitvoeren van een jaarlijkse steekproef van klachten en aangiften, Parl. St. Kamer 2021-22, nr. 55K2963/001

Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op de politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, teneinde de meldingsplicht van misdaden of wanbedrijven gepleegd door een collega uit te breiden tot gevallen van overlijdens, ernstige kwetsuren en schietincidenten, Parl. St. Kamer 2021-22, nr. 55K2964/001

Voorstel van resolutie betreffende het efficiënt en effectief bestrijden van de buitenlandse beïnvloeding en de ondermijning van onze democratie, Parl. St. Kamer 2022-23, 55K3045/001

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, BIM-Commissie, Controleorgaan op de politionele informatie, Federale Deontologische Commissie, Centrale Toezichtsraad voor het Gevangeniswezen, Mensenrechteninstituut - werkzaamheden van de werkgroepen in het kader van het synergieproject - rekeningen van het begrotingsjaar 2021 - begrotingsaanpassingen van het begrotingsjaar 2022 - begrotingsvoorstellen voor het begrotingsjaar 2023, Parl. St. Kamer 2022-23, 55K3050/001 tot 55K3050/003 en (*Hand.* Kamer 2022- 23, 22 december 2022, CRIV55PLEN226, 44)

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 2022 TOT 31 DECEMBER 2022)

Senaat

Schriftelijke vraag van R. Daems aan de minister van Justitie over de 'veiligheidsdiensten - specifieke methode - uitzonderlijke methode - kabelinterceptie - snapshots - datatap - verzameling - toestemming - privacy - cijfers en tendensen' (Senaat 2021-22, 30 maart 2022, Vr. nr. 7-1542)

Schriftelijke vraag van R. Daems aan de minister van Defensie over de 'veiligheidsdiensten - specifieke methode - uitzonderlijke methode - kabelinterceptie - snapshots - datatap - verzameling - toestemming - privacy - cijfers en tendensen' (Senaat 2021-22, 30 maart 2022, Vr. nr. 7-1543)

Schriftelijke vraag van R. Daems aan de minister van Binnenlandse Zaken over de 'veiligheidsdiensten - specifieke methode - uitzonderlijke methode - kabelinterceptie - snapshots - datatap - verzameling - toestemming - privacy - cijfers en tendensen' (Senaat 2021-22, 30 maart 2022, Vr. nr. 7-1544)

Schriftelijke vraag van E. Ampe aan de minister van Justitie over de 'oorlog in Oekraïne - antivirussoftware 'Kasparsky' - mogelijke veiligheidsrisico's - buitenlandse actoren - hacking - aanpak binnen de overheids- en veiligheidsdiensten - maatregelen' (Senaat 2021-22, 5 april 2022, Vr. nr. 7-1570)

Schriftelijke vraag van E. Ampe aan de minister van Defensie over de 'oorlog in Oekraïne - antivirussoftware 'Kasparsky' - mogelijke veiligheidsrisico's - buitenlandse actoren - hacking - aanpak binnen de overheids- en veiligheidsdiensten - maatregelen' (Senaat 2021-22, 5 april 2022, Vr. nr. 7-1571)

Schriftelijke vraag van E. Ampe aan de minister van Binnenlandse Zaken over de 'oorlog in Oekraïne - antivirussoftware 'Kasparsky' - mogelijke veiligheidsrisico's - buitenlandse actoren - hacking - aanpak binnen de overheids- en veiligheidsdiensten - maatregelen' (Senaat 2021-22, 5 april 2022, Vr. nr. 7-1572)

Schriftelijke vraag van S. Coenegrachts aan de minister van Justitie over de 'oorlog in Oekraine - russisch- orthodoxe kerken - bedreigingen - cijfers en tendensen - Staatsveiligheid - maatregelen' (Senaat 2021-22, 5 april 2022, Vr. nr. 7-1581)

Schriftelijke vraag van S. Coenegrachts aan de minister van Binnenlandse Zaken over de 'oorlog in Oekraïne - russisch- orthodoxe kerken - bedreigingen - cijfers en tendensen - Staatsveiligheid - maatregelen' (Senaat 2021-22, 5 april 2022, Vr. nr. 7-1582)

Schriftelijke vraag van R. Daems aan de minister van Defensie over de 'Citrix - ernstige kwetsbaarheid - veiligheidsrisico's - hacking - servers en computers - ondernemingen - overheids- en veiligheidsdiensten - beveiliging - richtlijnen - maatregelen' (Senaat 2021-22, 5 mei 2022, Vr. nr. 7-1600)

Schriftelijke vraag van L. Gahouchi aan de minister van Justitie over de 'Nationaal mensenrechteninstituut - interfederale benadering - samenwerkingsovereenkomst - stand van zaken - functie van de agent van de regering bij het Europees Hof voor de Rechten van de Mens - coördinatie - personeelsformatie - A-status - aanvraag tot accreditering' (Senaat 2021-22, 11 mei 2022, Vr. nr. 7-1617)

Schriftelijke vraag E. Ampe aan de minister van Binnenlandse Zaken over de 'camera's - china - spionage - buitenlandse actoren - privacy - cijfers en tendensen' (Senaat 2021-22, 2 juni 2022, Vr. nr. 7-1646)

Schriftelijke vraag E. Ampe aan de minister van Justitie over 'cyberaanvallen - statelijke actoren - privacy - cybersecurity - cijfers en tendensen' (Senaat 2021-22, 2 juni 2022, Vr. nr. 7-1651)

Schriftelijke vraag E. Ampe aan de staatssecretaris voor Digitalisering over de 'cyberaanvallen - statelijke actoren - privacy - cybersecurity - cijfers en tendensen' (Senaat 2021-22, 2 juni 2022, Vr. nr. 7-1653)

Schriftelijke vraag van T. Ongena aan de minister van Defensie over 'defensie - instant-messaging applicaties - gebruik - veiligheidsrisico's - hacking - statelijke actoren - cijfers en tendensen - mogelijke verbod -andere maatregelen' (Senaat 2021-22, 2 juni 2022, Vr. nr. 7-1668)

Kamer van volksvertegenwoordigers

Samengevoegde vragen van Ph. Pivin en G. Dallemagne aan de minister van Justitie over 'de beschikking van de ondernemingsrechtbank betreffende het Executief van de Moslims van België' (*Hand.* Kamer 2021-22, 12 januari 2022, CRIV55COM652, 58, Vr. nrs. 23785C en 23837C)

Vraag van M. Freilich aan de minister van Binnenlandse Zaken over de 'aanpak dark web' (*Vr. en Ant*. Kamer 2021-22, 13 januari 2022, QRVA74, 316, Vr. nr. 961)

Vraag van O. Depoortere aan de minister van Binnenlandse Zaken over de 'Vast Comité van Toezicht op de politiediensten - jaarverslag 2020' (*Vr. en Ant*. Kamer 2021-22, 13 januari 2022, QRVA74, 330, Vr. nr. 966)

Vraag van Th. Francken aan de staatssecretaris voor Asiel en Migratie over de 'veiligheidscheck operatie Afghanistan' (*Vr. en Ant*. Kamer 2021-22, 13 januari 2022, QRVA74, 406, Vr. nr. 437)

Vraag van S. Loones aan de minister van Justitie over 'de aanslagen van 2017 in Spanje' (*Hand.* Kamer 2021-22, 19 januari 2022, CRIV55COM663, 41, Vr. nr. 23908C)

Vraag van Y. Ingels aan de minister van Justitie over 'Belgian secure communications' (*Vr. en Ant*. Kamer 2021-22, 24 januari 2022, QRVA75, 241, Vr. nr. 897)

Samengevoegde vragen van P. Prévot en M. Freilich aan de Staatssecretaris voor Digitalisering over 'de gevaren van de Log4Shell- kwetsbaarheid' (*Hand.* Kamer 2021-22, 25 januari 2022, CRIV55COM666, 23, Vr. nrs. 23387C en 24275C)

Samengevoegde vragen van G. Defossé, A. Ponthier, Ch. Lacroix, A. Flahaut en P. Buysrogge aan de minister van Defensie over 'de cyberaanval op de website van Defensie' (*Hand.* Kamer 2021-22, 26 januari 2022, CRIV55COM671, 20, Vr. nrs. 23607C, 23612C, 23634C, 24318C en 24502C)

Actualiteitsdebat en toegevoegde vragen van F. Demon, V. Matz, T. Vandenput, B. Moyaers, H. Rigot en S. Goethals aan de minister Binnenlandse Zaken over 'de betoging van 23 januari' (*Hand.* Kamer 2021-22, 26 januari 2022, CRIV55COM676, 19, Vr. nrs. 24423C, 24450C, 24457C, 24490C, 24495C, en 24514C)

Samengevoegde vragen van K. Metsu, E. Gilissen, M. Freilich en S. Cogolati aan de minister van Justitie over 'het risico op cybersurveillance via bewakingsapparatuur van de merken Dahua en Hikvision' (*Hand.* Kamer 2021-22, 26 januari 2022, CRIV55COM677, 1, Vr. nrs. 23995C, 24232C, 24363C en 24454C)

Vraag van P. Buysrogge aan de minister van Justitie over de 'gewelddadig links-extremisme in België en Brussel' (*Hand.* Kamer 2021-22, 26 januari 2022, CRIV55COM677, 24, Vr. nr. 24477C)

Vraag van J. Pillen aan de minister van Buitenlandse Zaken over de 'algemeen veiligheidsakkoord tussen België, Bulgarije en andere landen' (*Vr. en Ant.* Kamer 2021-22, 31 januari 2022, QRVA76, 110, Vr. nr. 575)

Vraag van S. Cogolati aan de minister van Justitie over het 'risico op censuur en cyberspionage bij het gebruik van smartphones van Huawei, Xiaomi en OnePlus' (*Vr. en Ant.* Kamer 2021-22, 31 januari 2022, QRVA76, 251, Vr. nr. 909)

Vraag van G. Dallemagne aan de minister van Justitie over de 'jaarrapport van de Veiligheid van de Staat inzake vluchtelingen' (*Vr. en Ant.* Kamer 2021-22, 31 januari 2022, QRVA76, 268, Vr. nr. 951)

Vraag van G. Dallemagne aan de minister van Justitie over de 'verslag van de Veiligheid van de Staat over de moslimbroeders' (*Vr. en Ant.* Kamer 2021-22, 31 januari 2022, QRVA76, 271, Vr. nr. 953)

Vraag van S. Cogolati aan de minister van Defensie over de 'camerabewakingssystemen in onze militaire bases in België en in het buitenland' (*Vr. en Ant.* Kamer 2021-22, 31 januari 2022, QRVA76, 282, Vr. nr. 382)

Vraag van M. Freilich aan de minister van Defensie over 'defensie - cyberaanval' (*Vr. en Ant.* Kamer 2021-22, 31 januari 2022, QRVA76, 285, Vr. nr. 388)

Samengevoegde vragen van N. Boukili en F. De Smet aan de Staatssecretaris voor Asiel en Migratie over 'de intrekking van de verblijfsvergunning van de heer Toujgani' (*Hand.* Kamer 2021-22, 1 februari 2022, CRIV55COM681, 1, Vr. nrs. 24124C en 24129C)

Samengevoegde vragen van D. Safai en D. Van Langenhove aan de Staatssecretaris voor Asiel en Migratie over 'de procedureslag van Abdallah Ouahbour' (*Hand.* Kamer 2021-22, 1 februari 2022, CRIV55COM681, 30, Vr. nrs. 24601C, 24691C en 24649C)

Samengevoegde vragen van F. Demon en M.-Ch. Marghem aan de minister van Justitie over 'de vervolging van de relschoppers na de coronabetogingen' (*Hand.* Kamer 2021-22, 2 februari 2022, CRIV55COM683, 48, Vr. nrs. 24641C en 24774C)

Gedachtewisseling en toegevoegde vragen van Th. Francken, P. Buysrogge, A. Ponthier, M. Vindevoghel, R. Hedebouw en N. Boukili aan de minister van Defensie over 'de strategische visie' (*Hand.* Kamer 2021-22, 9 februari 2022, CRIV55COM688, 1, Vr. nrs. 24329C, 24330C, 24376C, 24506C, 24680C en 24681C)

Samengevoegde vragen van S. Cogolati, K. Metsu en J. Pillen aan de minister van Defensie over 'de bewakingscamerasystemen op onze militaire bases in België en in het buitenland' (*Hand.* Kamer 2021-22, 9 februari 2022, CRIV55COM688, 46, Vr. nrs. 24270C, 24589C, 24755C en 25092C)

Vraag van S. Matheï aan de minister van Defensie over de 'militair transport met humanitair karakter' (*Vr. en Ant.* Kamer 2021-22, 11 februari 2022, QRVA77, 305, Vr. nr. 399)

Samengevoegde vraag en interpellatie van T. Vandenput en K. Metsu aan de minister van Binnenlandse Zaken over 'Hikvision' (*Hand.* Kamer 2021-22, 15 februari 2022, CRIV-55COM698, 19, Vr. nrs. 24602C en 24642C)

Samengevoegde vraag en interpellatie van K. Metsu aan de minister van Binnenlandse Zaken over 'de beleidsnota 2022 en de aanbevelingen van de POC 'Terro" (*Hand.* Kamer 2021-22, 15 februari 2022, CRIV55COM698, 23, Vr. nrs. 24562C en 246I)

Vraag van D. Van Langenhove aan de Staatssecretaris voor Asiel en Migratie over 'het verblijf in België van de terroristen van de Groupe Islamique Combattant Marocain' (*Hand.* Kamer 2021-22, 16 februari 2022, CRIV55COM702, 17, Vr. nr. 25060C)

Interpellatie van M. Dillen aan de minister van Justitie over 'het digitaal transformatieplan' (*Hand.* Kamer 2021-22, 16 februari 2022, CRIV55COM703, 25, Vr. nr. 261I)

Vraag van P. Buysrogge aan de minister van Binnenlandse Zaken over 'de aanwezigheid van extremisten bij betogingen' (*Hand.* Kamer 2021-22, 23 februari 2022, CRIV55COM709, 1, Vr. nr. 25043C)

Vraag van S De Wit aan de minister van Justitie over 'de vernietigde dataretentiewet' (*Hand.* Kamer 2021-22, 23 februari 2022, CRIV55COM710, 20, Vr. nr. 25422C)

Samengevoegde vragen van Ph. Pivin, G. Dallemagne en S. Rohonyi aan de minister van Justitie over 'het Executief van de Moslims van België' (*Hand.* Kamer 2021-22, 23 februari 2022, CRIV55COM710, 22, Vr. nr. 25441C, 25583C en 25585C)

Vraag van M. Freilich aan de minister van Buitenlandse Zaken over het 'advies BOIC omtrent cyberveiligheid bij de Winterspelen' (*Vr. en Ant.* Kamer 2021-22, 25 februari 2022, QRVA78, 119, Vr. nr. 602)

Vraag van O. Depoortere aan de minister van Justitie over de 'Comité I - verloning' (*Vr. en Ant.* Kamer 2021-22, 25 februari 2022, QRVA78, 243, Vr. nr. 1004)

Vraag van N. Boukili aan de minister van Justitie over de 'gebruik van de Pegasus-software' (*Vr. en Ant.* Kamer 2021-22, 25 februari 2022, QRVA78, 251, Vr. nr. 1013)

Vraag van M. Freilich aan de minister van Justitie over de 'Chinese economische spionage' (*Vr. en Ant.* Kamer 2021-22, 25 februari 2022, QRVA78, 255, Vr. nr. 1022)

Vraag van A. Ponthier aan de minister van Defensie over 'de goedgekeurde overheidsopdrachten voor Defensie - ACOS-IS' (*Vr. en Ant.* Kamer 2021-22, 25 februari 2022, QRVA78, 262, Vr. nr. 408)

Vraag van A. Ponthier aan de minister van Defensie over 'de geplande Belgische inzet in het kader van de strijd tegen IS' (*Vr. en Ant.* Kamer 2021-22, 25 februari 2022, QRVA78, 264, Vr. nr. 410)

Gedachtewisseling en toegevoegde vragen van S. Cogolati, S. De Vuyst, E. Gilissen, N. Boukili, F. De Smet, A. Van Bossuyt, G. Dallemagne, A. Ponthier, W. De Vriendt, J. Pillen, E. Van Hoof, Th. Francken, K. Verduyckt, G. Defossé, S, Creyelman, T. Roggeman, S. Moutquin, E. Platteau, H. Rigot en G. Daems aan de eerste minister, de minister van Buitenlandse Zaken, de minister van Binnenlandse Zaken, de minister van Defensie en de Staatssecretaris voor Asiel en Migratie over 'de Oekraïne-crisis, de ondersteuning van de Belgische regering en de opvang van de Oekraïense vluchtelingen' (*Hand.* Kamer 2021-22, 2 maart 2022, CRIV55COM712, 1, Vr. nrs. 24261C, 24323C, 25171C, 25262C, 25726C, 24664C, 24721C, 24916C, 25259C, 25263C, 25490C, 25596C, 25696C, 25704C, 25706C, 25707C, 25709C, 25694C, 24663C, 25109C, 25598C, 25693C, 25700C, 25703C, 25705C, 25708C, 25722C, 25725C, 25648C, 25651C, 25690C, 25691C, 25692C, 25699C, 25701C, 25702C, 25711C, 25719C, 25721C, 25723C, 25727C en 25724C)

Vraag van R. D'Amico de minister van Ambtenarenzaken over 'Ericsson en de onthullingen van het Internationaal Consortium van Onderzoeksjournalisten' (*Hand.* Kamer 2021-22, 9 maart 2022, CRIV55COM716, 22, Vr. nr. 25843C)

Vraag van O. Depoortere aan de minister van Binnenlandse Zaken over 'het veiligheidsniveau, de risicoanalyse en de verhoogde bewaking van potentiële doelwitten in België' (*Hand.* Kamer 2021-22, 9 maart 2022, CRIV55COM716, 35, Vr. nr. 25747C)

Vraag van M.-Ch. Marghem aan de minister van Justitie over 'het vertrek van vrijwilligers naar Oekraïne' (*Hand.* Kamer 2021-22, 9 maart 2022, CRIV55COM717, 32, Vr. nr. 25865C)

Vraag van W. De Vriendt aan de minister van Buitenlandse Zaken over de 'Noordoost- Syrië - aanval van IS' (*Vr. en Ant.* Kamer 2021-22, 10 maart 2022, QRVA79, 155, Vr. nr. 606)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over de 'nieuwe technologieen - opvolging' (*Vr. en Ant.* Kamer 2021-22, 10 maart 2022, QRVA79, 378, Vr. nr. 1078)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over de 'begroting 2022 - aanpak gewelddadig extremisme' (*Vr. en Ant.* Kamer 2021-22, 10 maart 2022, QRVA79, 386, Vr. nr. 1081)

Gedachtewisseling en toegevoegde vragen van K. Metsu, R. Van Lommel, M. Freilich, A. Van Bossuyt, D. Van Langenhove, S. Cogolati, W.r De Vriendt, B. Segers, F. De Smet, D. Safai en Th. Francken aan de eerste minister over 'de nationale veiligheidsstrategie' (*Hand.* Kamer 2021-22, 16 maart 2022, CRIV55COM721, 1, Vr. nrs. 25758C, 25765C, 25786C, 25811C, 25799C, 25991C, 26001C, 26015C, 26026C, 26067C, 26117C, 26134C en 26151C)

Vraag van A. Flahaut aan de eerste minister over 'de deelname van Belgische burgers aan de gewapende strijd Oekraïne na de Russische invasie' (*Hand.* Kamer 2021-22, 16 maart 2022, CRIV55COM729, 14, Vr. nrs. 25981C)

Vraag van O. Depoortere aan de minister van Justitie over de 'VSSE - verloning' (*Vr. en Ant.* Kamer 2021-22, 18 maart 2022, QRVA80, 235, Vr. nr. 1005)

Vraag van E. Burton aan de minister van Justitie over 'OCAD - ontsnapping van Belgische terroristen in Syrië' (*Vr. en Ant.* Kamer 2021-22, 18 maart 2022, QRVA80, 250, Vr. nr. 1049)

Vraag van E. Burton aan de minister van Defensie over 'Afghanistan - geheime missie voor de evacuatie van burgers' (*Vr. en Ant.* Kamer 2021-22, 18 maart 2022, QRVA80, 278, Vr. nr. 421)

Vraag van A. Laaouej aan de minister van Binnenlandse Zaken over 'de bedreigingen aan het adres van moskeeën in de aanloop naar de ramadan' (*Hand.* Kamer 2021-22, 24 maart 2022, CRIV55PLEN171, 25, Vr. nr. 2421P)

Vraag van T. Vandenput aan de minister van Binnenlandse Zaken over het 'OCAD - databank - update' (*Vr. en Ant.* Kamer 2021-22, 28 maart 2022, QRVA81, 269, Vr. nr. 1110)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'dood van de leider van IS' (*Vr. en Ant.* Kamer 2021-22, 28 maart 2022, QR25VA81, 276, Vr. nr. 1115)

Actualiteitsdebat over Oekraïne en toegevoegde vragen van A Van Bossuyt, A. Ponthier, M. De Maegd, W. De Vriendt, S. Cogolati, S. De Vuyst, N. Boukili, F. De Smet, S. Rohonyi en S. Moutquin aan de minister van Buitenlandse Zaken over 'het aftreden van Jens Stoltenberg' (*Hand.* Kamer 2021-22, 29 maart 2022, CRIV55COM743, 1, Vr. nrs. 24926C, 25027C, 25742C, 25751C, 25769C, 25770C, 25806C, 25847C, 25861C, 26006C, 26016C, 26194C, 26196C, 26602C, 26604C, 26610C, 26615C, 26598C, 26613C et 26626C)

Samengevoegde vragen van G. Defossé en E. Van Hoof aan de minister van Defensie over 'de financiering van de Rwandese troepen in Mozambique' (*Hand.* Kamer 2021-22, 29 maart 2022, CRIV55COM743, 60, Vr. nrs. 25039C, 25184C, 25688C en 25899C)

Actualiteitsdebat en toegevoegde vragen van B. Segers, D. Safai, M.-Ch. Marghem, J. Chanson, K. Aouasti, V. Van Peel, Fr. De Smet en G. Daems aan de minister van Binnenlandse Zaken over 'Oekraïne' (*Hand.* Kamer 2021-22, 30 maart 2022, CRIV55COM746, 1, Vr. nrs. 26027C, 26133C, 26141C, 26283C, 26622C, 26624C, 26636C, 26667C en 55026712C)

Vraag van A. Ponthier aan de minister van Defensie over 'de plannen voor de cybercomponent en de rekrutering van personeel' (*Hand.* Kamer 2021-22, 30 maart 2022, CRIV55COM748, 21, Vr. nr. 24791C)

Vraag van J.-M. Delizée aan de minister van Justitie over 'het archief van de koloniale veiligheid' (*Hand.* Kamer 2021-22, 30 maart 2022, CRIV55COM751, 7, Vr. nr. 26463C)

Samengevoegde vragen van D. Ducarme en S. Rohonyi aan de minister van Justitie over 'de Moslimbroeders en de bedreiging die zij mogelijk vormen in België' (*Hand.* Kamer 2021-22, 30 maart 2022, CRIV55COM751, 14, Vr. nrs. 26663C en 26668C)

Vraag van S. Loones aan de minister van Justitie over de 'screening buitenlandse investeringen, overnames en participaties' (*Vr. en Ant.* Kamer 2021-22, 5 april 2022, QRVA82, 159, Vr. nr. 1054)

Vraag van S. Matheï aan de minister van Defensie over de 'cyberdefensiecomponent' (*Vr. en Ant.* Kamer 2021-22, 5 april 2022, QRVA82, 227, Vr. nr. 406)

Vraag van S. Matheï aan de minister van Binnenlandse Zaken over de 'desinformatiecampagnes - veiligheidsdienst' (*Vr. en Ant.* Kamer 2021-22, 5 april 2022, QRVA82, 292, Vr. nr. 1152)

Vraag van O. Depoortere aan de minister van Binnenlandse Zaken over de 'potentiële doelwitten in België - veiligheidsniveau, risicoanalyse en verhoogde bewaking' (*Vr. en Ant.* Kamer 2021-22, 21 april 2022, QRVA83, 378, Vr. nr. 1162)

Samengevoegde vragen van O. Depoortere en N. Boukili aan de minister van Binnenlandse Zaken over 'het gebruik van de Pegasussoftware' (*Hand.* Kamer 2021-22, 27 april 2022, CRIV55COM767, 28, Vr. nrs. 27060C en 27170C)

Samengevoegde vragen van M. De Maegd en G. Dallemagne aan de minister van Justitie over 'de bekladding v.h. monument ter herdenking v.d. Armeense genocide en de strijd tegen het radicalisme' (*Hand.* Kamer 2021-22, 28 april 2022, CRIV55COM176, 10, Vr. nrs. 2485P en 2488P)

Vraag van S. Verherstraeten aan de minister van Defensie over de 'transfer van wapens naar Oekraïne' (*Vr. en Ant.* Kamer 2021-22, 2 mai 2022, QRVA84, 295, Vr. nr. 446)

Vraag van K. Metsu aan de minister van Justitie, over de 'buitenlandse inmenging in de Belgische islam' (*Vr. en Ant.* Kamer 2021-22, 11 mai 2022, QRVA85, 225., Vr. nr. 1168)

Samengevoegde vragen van B. Pas, K. Metsu en E. Platteau aan de minister van Justitie over 'de repatriëring van IS-gangsters' (*Hand.* Kamer 2021-22, 19 mai 2022, CRIV55PLEN181, 2, Vr. nrs. 2544P, 2551P en 2565P)

Vraag van S. Creyelman aan de minister van Defensie over de 'cyberactiviteit tegen ons land sinds de Russische inval in Oekraïne' (*Vr. en Ant.* Kamer 2021-22, 25 mai 2022, QRVA86, 69, Vr. nr. 193)

Vraag van T. Van Grieken aan de minister van Justitie over 'de erkenning van moskeeën' (*Vr. en Ant.* Kamer 2021-22, 25 mai 2022, QRVA86, 238, Vr. nr. 1139)

Vraag van G. Defossé aan de minister van Defensie over de 'veiligheidsverificatie van militairen' (*Vr. en Ant.* Kamer 2021-22, 25 mai 2022, QRVA86, 294., Vr. nr. 464)

Actualiteitsdebat en toegevoegde vragen van M. Freilich, A. Ponthier, G. Dallemagne en K. Verduyckt aan de minister van Defensie over 'de door de ADIV en defensie aangeschafte hardware van Huawei' (*Hand.* Kamer 2021-22, 1 juni 2022, CRIV55COM802, 10, Vr. nrs. 26849C, 26870C, 26871C, 27247C en 28265C)

Gedachtewisseling over de opvolging van de aanbevelingen van de onderzoekscommissie 'terroristische aanslagen' en toegevoegde vragen van K Van Vaerenbergh, N. Boukili, O. Vajda, Ph. Pivin, M. Dillen, N. Boukili, G. Dallemagne, S. Rohonyi, M.-C. Leroy, K. Aouasti en K. Metsu aan de minister van Justitie over 'de opvolging v.d. aanbevelingen v.d. onderzoekscommissie aanslagen m.b.t. de Staatsveiligheid' (*Hand.* Kamer 2021-22, 3 juni 2022, CRIV55COM806, 1, Vr. nrs.28307C, 28321C, 28329C, 28335C, 28338C, 28340C, 28341C, 28345C, 28346C, 28347C, 28348C, 28349C, 28350C, 28351C, 28352C,

28353C, 28354C, 28355C, 28356C, 28357C, 28358C, 28359C, 28360C, 28361C, 28362C, 28363C, 28364C, 28365C, 28368C, 55028369C, 28370C, 28371C, 28372C, 28374C, 28375C, 28376C, 28377C, 28378C, 28386C, 28387C, 28388C, 28390C, 28393C, 28397C, 28389C, 28391C, 28392C, 28394C, 28398C, 28399C, 28400C, 28402C, 28410C, 28411C, 28412C, 28413C, 28418C, 28421C, 28441C, 28443C, 28448C en 28449C)

Vraag van S. Creyelman aan de minister van Defensie over 'de bijkomende investeringen in Defensie' (*Vr. en Ant.* Kamer 2021-22, 9 juni 2022, QRVA87, 239, Vr. nr. 461)

Vraag van S. Creyelman aan de minister van Defensie over de 'veiligheidsmaatregelen inzake extremisme bij Defensie' (*Vr. en Ant.* Kamer 2021-22, 9 juni 2022, QRVA87, 240, Vr. nr. 465)

Vraag van E. Burton aan de minister van Binnenlandse Zaken over de 'Belgen die naar Oekraïne vertrokken zijn om te vechten' (*Vr. en Ant.* Kamer 2021-22, 9 juni 2022, QRVA87, 265, Vr. nr. 1242)

Samengevoegde vragen van M. Freilich aan de eerste minister over 'de cyberrisico's' (*Hand.* Kamer 2021-22, 14 juni 2022, CRIV55COM815, 6, Vr. nrs. 26784C en 28450C)

Vraag van T. Vandenput aan de minister van Binnenlandse Zaken over 'veiligheidsscreenings voor gevoelige jobs' (*Hand.* Kamer 2021-22, 15 juni 2022, CRIV55COM818, 15, Vr. nr. 28264C)

Vraag van O. Depoortere aan de minister van Binnenlandse Zaken over 'het gebruik van wifi-routers of producten van Huawei bij Binnenlandse Zaken' (*Hand.* Kamer 2021-22, 15 juni 2022, CRIV55COM818, 27, Vr. nr. 28409C)

Vraag van D. Senesael aan de minister van Binnenlandse Zaken over 'motorbendes' (*Hand.* Kamer 2021-22, 15 juni 2022, CRIV55COM818, 32, Vr. nr. 28579C)

Gedachtewisseling over de opvolging van de aanbevelingen van de onderzoekscommissie 'Terroristische aanslagen' en toegevoegde vragen van O. Vajda, Ph. Pivin, D. Ducarme en G. Dallemagne aan de minister van Binnenlandse Zaken over 'de follow-up van de aanbevelingen na de aanslagen en de aanbevelingen op het stuk van de wetgeving' (*Hand.* Kamer 2021-22, 21 juni 2022, CRIV55COM824, 1, Vr. nrs. 28330C, 28337C, 28643C, 28645C, 28646C, 28647C, 28798C, 28800C, 28802C, 28803C, 28979C, 28980C, 28981C en 28982C)

Vraag van N. Boukili aan de minister van Ambtenarenzaken over 'een mogelijk moratorium op de uitrol van het 5G-netwerk van Ericsson' (*Hand.* Kamer 2021-22, 22 juni 2022, CRIV55COM830, 1, Vr. nr. 27264C)

Samengevoegde vragen van B. Pas en K. Metsu aan de eerste minister over 'de repatriëring van IS-gangsters' (*Hand.* Kamer 2021-22, 23 juni 2022, CRIV55PLEN190, 6, Vr. nrs. 2671P en 2694P)

Vraag van M. Dillen aan de minister van Justitie over 'de veiligheidscoördinatoren voor de gevangenissen' (Hand. Kamer 2021-22, 22 juni 2022, CRIV55COM841, 7, Vr. nr.29079C)

Vraag van K. Jadin aan de minister van Justitie over 'integriteitscontrole voor personeel' (*Vr. en Ant.* Kamer 2021-22, 27 juin 2022, QRVA88, 297, Vr. nr. 1237)

Vraag van E. Burton aan de minister van Defensie over 'Belgische militairen die naar Oekraine vertrokken zijn' (*Vr. en Ant.* Kamer 2021-22, 27 juin 2022, QRVA88, 343, Vr. nr. 477)

Vraag van S. Creyelman aan de minister van Defensie over 'de investeringen van de militaire programmeringswet inzake cyber en command' (*Vr. en Ant.* Kamer 2021-22, 27 juin 2022, QRVA88, 359, Vr. nr. 497)

Vraag van O. Depoortere aan de minister van Binnenlandse Zaken over 'gecoördineerde bestrijding van cyber-security en cybercriminaliteit' (*Vr. en Ant.* Kamer 2021-22, 27 juin 2022, QRVA88, 384, Vr. nr. 1270)

Vraag van M. Freilich aan de minister van Binnenlandse Zaken over 'Joodse gemeenschap - veiligheidsvoorzieningen' (*Vr. en Ant*. Kamer 2021-22, 27 juin 2022, QRVA88, 393, Vr. nr. 1279)

Vraag van K. Metsu aan de staatssecretaris voor Asiel en Migratie over 'infodoorstroming Fedasil' (*Vr. en Ant*. Kamer 2021-22, 27 juin 2022, QRVA88, 480, Vr. nr. 599)

Vraag van M. Dillen aan de minister van Justitie over 'de toegang tot de gegevensbank SIDIS Suite door ADIV' (*Hand.* Kamer 2021-22, 29 juni 2022, CRIV55COM841, 5, Vr. nr. 29078C)

Vraag van P. De Roover aan de minister van Justitie over 'het beleid van de regering ten aanzien van terroristen in hechtenis' (*Hand.* Kamer 2021-22, 30 juni 2022, CRIV55PLEN191, 7, Vr. nr. 2704P)

Vraag van K. Metsu, S. Goethals en P. Buysrogge aan de eerste minister over 'de verduidelijking van de Nationale Veiligheidsstrategie' (*Hand.* Kamer 2021-22, 5 juli 2022, CRIV55COM844, 7, Vr. nrs. 27325C, 27326C, 27327C, 27328C, 27775C, 27950C et 28091C)

Vraag van P. Buysrogge aan de minister van Defensie over 'de veiligheidsverificaties door de ADIV' (*Hand.* Kamer 2021-22, 13 juli 2022, CRIV55COM859, 1, Vr. nr. 28866C) '

Vraag van T. Roggeman aan de staatssecretaris voor Digitalisering over de 'nieuw gebouw Staatsveiligheid' (*Vr. en Ant*. Kamer 2021-22, 14 juillet 2022, QRVA89, 86, Vr. nr. 338)

Vraag van M. Dillen aan de minister van Justitie over de 'budget VSSE - verhogingen' (*Vr. en Ant*. Kamer 2021-22, 14 juillet 2022, QRVA89, 307, Vr. nr. 1244)

Vraag van E. Platteau aan de minister van Binnenlandse Zaken over 'terrorist fighters en haatpropagandisten - gemeenschappelijke gegevensbank' (*Vr. en Ant*. Kamer 2021-22, 14 juillet 2022, QRVA89, 425, Vr. nr. 1324)

Vraag van M. Freilich aan de minister van Justitie over de 'hoog risico vendoren' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 260, Vr. nr. 1233)

Vraag van M. Dillen aan de minister van Justitie over de 'wegwerken van deficits en versterken van de inlichtingenen veiligheidsdiensten' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 265, Vr. nr. 1247)

Vraag van M. Dillen aan de minister van Justitie over de 'VSSE - verbeteren rekrutering en aandacht voor personeelsbeleid' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 271, Vr. nr. 1255)

Vraag van C. Taquin aan de minister van Justitie over de 'monitoring van en toezicht op sektarische organisaties' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 279, Vr. nr. 1277)

Vraag van M. Freilich aan de minister van Justitie over 'TikTok' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 280, Vr. nr. 1282)

Vraag van B. Pas aan de minister van Justitie over 'repatriëring Syriëgangsters' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 282, Vr. nr. 1288)

Vraag van A. Van Bossuyt aan de minister van Justitie over de 'spionage door China' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 284, Vr. nr. 1291)

Vraag van G. Dallemagne aan de minister van Defensie over 'Defensie - cyberaanval' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 304, Vr. nr. 505)

Vraag van S. Cogolati aan de minister van Binnenlandse Zaken over 'FANC - erkenning van een buitenlandse veiligheidsmachtiging' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 351, Vr. nr. 1339)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'het Brusselse kanaalplan en LIVC's' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 377, Vr. nr. 1357)

Vraag van V. Scourneau aan de minister van Binnenlandse Zaken over de 'veiligheid van gevoelige functies - screening' (*Vr. en Ant*. Kamer 2021-22, 11 augustus 2022, QRVA90, 392, Vr. nr. 1369)

Vraag van K. Aouasti aan de minister van Justitie over 'motorbendes' (*Vr. en Ant*. Kamer 2021-22, 9 september 2022, QRVA91, 275, Vr. nr. 1280)

Vraag van M. Dillen aan de minister van Justitie over het 'ontwerp protocolakkoord tussen VSSE en DG EPI' (*Vr. en Ant*. Kamer 2021-22, 9 september 2022, QRVA91, 284, Vr. nr. 1296)

Vraag van E. Burton aan de minister van Defensie over 'clandestien drugslab in Kleine-Brogel' (*Vr. en Ant*. Kamer 2021-22, 9 september 2022, QRVA91, 320, Vr. nr. 529)

Samengevoegde vragen van K. Metsu en B. Pas aan de minister van Binnenlandse Zaken over 'de kosten van de repatriëring van IS-terroristen voor het departement Binnenlandse Zaken' (*Hand.* Kamer 2021-22, 21 september 2022, CRIV55COM881, 23, Vr. nrs. 55029655C en 55030088C)

Samengevoegde vragen van N. Boukili, A. Laaouej en J. Chanson aan de minister van Binnenlandse Zaken over 'het festival Frontnacht en het rapport van het OCAD' (*Hand.* Kamer 2021-22, 21 september 2022, CRIV55COM881, 44, Vr. nrs. 55029719C, 55029724C en 55029748C)

Vraag van K. Aouasti aan de minister van Binnenlandse Zaken over 'het dreigingsniveau' (*Hand.* Kamer 2021-22, 21 september 2022, CRIV55COM881, 64, Vr. nr. 55029926C)

Samengevoegde vragen van D. Senesael aan de minister van Binnenlandse Zaken over 'het activiteitenverslag 2021 van het OCAD' (*Hand.* Kamer 2021-22, 21 september 2022, CRIV55COM881, 54, Vr. nrs. 29731C en 29868C)

Vraag van M. Dillen aan de minister van Justitie over 'geradicaliseerde gedetineerden - opvolging bij strafeinde - recidive' (*Vr. en Ant*. Kamer 2021- 22, 28 september 2022, QRVA92, 233, Vr. nr. 1254)

Vraag van S. Cogolati aan de minister van Buitenlandse Zaken over de 'NVO - veiligheidsverificaties in nucleaire inrichtingen' (*Vr. en Ant*. Kamer 2021-22, 28 september 2022, QRVA92, 311, Vr. nr. 22)

Samengevoegde vragen van M. Prévot, K. Gabriëls, Ph. Pivin, N. Boukili en K. Aouasti aan de eerste minister over 'het veiligheidsbeleid van de regering in het licht van de dreiging van drugsdealers en terroristen' (*Hand.* Kamer 2021-22, 29 september 2022, CRIV55PLEN203, 1, Vr. nrs. 55002833P, 55002834P, 55002840P, 55002838P en 55002839P)

Vraag van M. Dillen aan de minister van Justitie over de 'informatiesessies informatie- uitwisseling met de VSSE' (*Vr. en Ant*. Kamer 2021-22, 30 september 2022, QRVA93, 56, Vr. nr. 1295)

Vraag van C. Taquin aan de minister van Binnenlandse Zaken over de 'sektarische bewegingen - aantal klachten' (*Vr. en Ant*. Kamer 2021-22, 30 september 2022, QRVA93, 154, Vr. nr. 1405)

Vraag van S. Cogolati aan de minister van Binnenlandse Zaken over de 'beveiliging van de Belgische kerncentrales in het licht van de terreurdreiging' (*Vr. en Ant*. Kamer 2021-22, 30 september 2022, QRVA93, 213, Vr. nr. 1445)

Vraag van A. Flahaut aan de minister van Buitenlandse Zaken over de 'NVO' (*Vr. en Ant*. Kamer 2021-22, 30 september 2022, QRVA93, 231, Vr. nr. 12)

Samengevoegde vragen van G. Dallemagne en O. Vajda aan de minister van Binnenlandse Zaken over 'de directie van het OCAD' (*Hand.* Kamer 2021-22, 5 oktober 2022, CRIV55COM894, 44, Vr. nrs. 55030712C, 55030744C en 55030882C)

Samengevoegde vragen van Ph. Pivin, S. Rohonyi en O. Vajda aan de minister van Justitie over 'de uitspraak van de rechtbank van eerste aanleg met betrekking tot de top van het EMB' (*Hand.* Kamer 2021-22, 5 oktober 2022, CRIV55COM895, 48, Vr. nrs. 55029965C, 55030162C en 55030674C)

Vraag van S. Creyelman aan de minister van Defensie over de 'aantrekken geschikte profielen voor de cybercomponent' (*Vr. en Ant*. Kamer 2021-22, 9 oktober 2022, QRVA94, 383, Vr. nr. nr. 534)

Actualiteitsdebat over cyberaanvallen en toegevoegde vragen van M. Freilich, B. Moyaers, B. Pas, D. Senesael en G. Dallemagne aan de eerste minister over 'de toewijzing van cyberaanvallen aan Chinese hackersgroepen' (*Hand.* Kamer 2022-23, 18 oktober 2022, CRIV55COM899, 1, Vr. nrs.55029671C, 55029676C, 55029765C, 55029827C, 55030228C, 55030235C en 55030714C)

Vraag van Y. Ingels aan de minister van Binnenlandse Zaken over 'de begrotingstabellen in navolging van de SOTU 2022 en de NVO' (*Hand.* Kamer 2022-23, 19 oktober 2022, CRIV55COM907, 47, Vr. nr. 55031319C)

Vraag van M. Dillen aan de minister van Justitie over de 'radicalisering gedetineerden in de gevangenis' (*Vr. en Ant.* Kamer 2022-23, 19 oktober 2022, QRVA95, 152, Vr. nr. 1297)

Vraag van P. Buysrogge aan de minister van Justitie over de 'VSSE - infrastructuur' (*Vr. en Ant.* Kamer 2022-23, 19 oktober 2022, QRVA95, 152, Vr. nr. 1358)

Vraag van K. Metsu aan de minister van Justitie over de 'justitiële aspecten terrorismebestrijding' (*Vr. en Ant.* Kamer 2022-23, 19 oktober 2022, QRVA95, 157, Vr. nr. 1364)

Vraag van D. Safai aan de minister van Justitie over de 'uitzetting Marokkaanse haatprediker Abdallah Ouahbour' (*Vr. en Ant.* Kamer 2022-23, 19 oktober 2022, QRVA95, 161, Vr. nr. 1387)

Vraag van S. Cogolati aan de minister van Justitie over de 'Chinese academische en industriele spionage' (*Vr. en Ant.* Kamer 2022-23, 19 oktober 2022, QRVA95, 178, Vr. nr. 1401)

Vraag van A. Laaouej aan de minister van Justitie over 'Frontnacht' (*Vr. en Ant.* Kamer 2022-23, 19 oktober 2022, QRVA95, 199, Vr. nr. 1413)

Gedachtewisseling over de escalatie van het drugsgeweld en toegevoegde vragen van O. Depoortere, S. Van Hecke, V. Matz, M. Dillen, J. Chanson, S. De Wit, N. Boukili, F. Demon, A. Laaouej, E. Thiébaut, S. Rohonyi, Y. Ingels, S. Van Hecke, E. Platteau en O. Depoortere aan de minister van Binnenlandse Zaken over 'de veiligheidscrisis in Antwerpen (diverse aanslagen in Borgerhout, Hoboken en centraal station)' (*Hand.* Kamer 2022-23, 24 oktober 2022, CRIV55COM913, 1, Vr. nrs. 55029729C, 55029739C, 55029740C, 55000317I, 55000318I, 55029776C, 55029784C, 55029785C, 55029819C, 55029820C, 55029967C, 55029968C, 55029976C, 55029984C, 55029994C, 55030001C55030013C, 55030014C, 55030015C, 55030016C, 55030018C, 55030019C, 55030020C, 55030021C, 55030022C, 55030025C, 55030026C, 55030031C, 55030032C, 55030033C, 55030036C, 55030037C, 55030039C, 55030040C, 55030044C en 55030146C)

Vraag van S. Van Hecke aan de minister van Justitie over 'personeelsuitbreiding bij de VSSE - gevolgen opvolging sektarische organisaties' (*Vr. en Ant.* Kamer 2022-23, 7 november 2022, QRVA96, 257, Vr. nr. 1425)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over 'index van het Institute for Jewish Research en het European Union Agency for Fundamental Rights - studies' (*Vr. en Ant.* Kamer 2022-23, 7 november 2022, QRVA96, 314, Vr. nr. 1500)

Samengevoegde vragen van A. Ponthier en P. Buysrogge aan de minister van Defensie over 'het ronselen van westerse ex-defensiepiloten door China' (*Hand.* Kamer 2022-23, 9 november 2022, CRIV55COM926, 6, Vr. nrs. 55031334C en 55031757C)

Samengevoegde vragen van S. Cogolati en M.-Ch. Marghem aan de minister van Justitie over 'de Chinese politiebureaus in het buitenland' (*Hand.* Kamer 2022-23, 9 november 2022, CRIV55COM927, 9, Vr. nrs. 55031668C en 55031524C

Vraag van M.-Ch. Marghem aan de minister van Justitie over 'het huwelijk van de terrorist Salah Abdeslam en het toezicht in de gevangenissen' (*Hand.* Kamer 2022-23, 9 november 2022, CRIV55COM927, 12, Vr. nr. 55031669C)

Gedachtewisseling over de mesaanval op politieagenten van de politiezone Brussel Noord en toegevoegde vragen en interpellatie van M. De Maegd, M. Dillen, E. Platteau, O. Depoortere, N. Boukili, K. Metsu, E. Thiébaut, H. Rigot, K. Aouasti, K. Geens, G. Vanden Burre, Ö. Özen en L. Zanchetta aan de minister van Binnenlandse Zaken over 'de aanval

op twee politieagenten in Brussel' (*Hand.* Kamer 2022-23, 14 november 2022, CRIV-55COM929, 1, Vr. nrs. 55031862C, 55000338I, 55031867C, 55031868C, 55031871C, 55031872C, 55031873C, 55031878C, 55031879C, 55031880C, 55031881C, 55031888C, 55031893C en 55031894C)

Vraag van C. Taquin aan de minister van Justitie over de 'onderzoeken naar sektarische bewegingen' (*Vr. en Ant.* Kamer 2022-23, 17 november 2022, QRVA97, 148, Vr. nr. 1344)

Vraag van S. Cogolati aan de minister van Justitie over 'het veiligheidsrisico en het risico op inmenging door de versterkte greep van China op onze havens' (*Hand.* Kamer 2022-23, 30 november 2022, CRIV55COM935, 4, Vr. nr. 55031913C)

Vraag van S. Cogolati aan Binnenlandse Zaken over de 'Chinese politiebureaus in het buitenland' (*Hand.* Kamer 2022-23, 14 december 2022, CRIV55COM947, 8, Vr. nrs.55031525C)

Samengevoegde vragen van M. Freilich en O. Depoortere, aan de minister van Binnenlandse Zaken over 'de verheerlijking van Hamas' (*Hand.* Kamer 2022-23, 14 december 2022, CRIV55COM947, 11, Vr. nrs.55031814C en 55031917C)

Vraag van N. Boukili aan de minister van Justitie over 'spionage met Pegasus- spyware in België' (*Hand.* Kamer 2022-23, 14 december 2022, CRIV55COM948, 44, Vr. nr. 55032489C)

Vraag van S. Rohonyi aan minister van Middenstand over de 'Qatargate en de corruptiebestrijding' (*Hand.* Kamer 2022-23, 15 december 2022, CRIV55PLEN220, 26, Vr. nr. 55003065P)

Vraag van H. Bogaert aan de minister van Defensie over de 'onderofficier geschorst' (*Vr. en Ant.* Kamer 2022- 23, 16 december 2022, QRVA99, 249, Vr. nr. 559)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'terreur - LIVC-R's' (*Vr. en Ant.* Kamer 2022-23, 16 december 2022, QRVA99, 301, Vr. nr. 1608)

RAPPORT D'ACTIVITÉS 2022
ACTIVITEITENVERSLAG 2022

Quis custodiet ipsos custodes ?

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

Rédaction

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

Déjà parus dans cette série

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Comité permanent R, *Rapport d'activités 2006,* 2007, 147 p.
3) Comité permanent R, *Rapport d'activités 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism - Fusion Centres throughout Europe*, 2010, 220 p.
5) Comité permanent R, *Rapport d'activités 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Comité permanent R, *Rapport d'activités 2009,* 2010, 127 p.
8) Comité permanent R, *Rapport d'activités 2010,* 2011, 119 p.
9) Comité permanent R, *Rapport d'activités 2011,* 2012, 134 p.
10) W. Van Laethem et J. Vanderborght, *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, 2013, 565 p.
11) Comité permanent R, *Rapport d'activités 2012*, 2013, 127 p.
12) Comité permanent R, *Rapport d'activités 2013*, 2014, 212 p.
13) Comité permanent R, *Rapport d'activités 2014*, 2015, 141 p.
14) Comité permanent R, *Rapport d'activités 2015*, 2016, 131 p.
15) Comité permanent R, *Rapport d'activités 2016*, 2017, 227 p.
16) Comité permanent R, *Rapport d'activités 2017*, 2018, 152 p.
17) Comité permanent R, *Rapport d'activités 2018*, 2019, 167 p.
18) J. Vanderborght (ed.), *Les méthodes particulières de renseignement : de l'ombre à la lumière*, 2019, 151 p.
19) Comité permanent R, *Rapport d'activités 2019*, 2020, 148 p.
20) Comité permanent R, *Rapport d'activités 2020*, 2021, 189 p.
21) Comité permanent R, *Rapport d'activités 2021*, 2022, 241 p.
22) Comité permanent R, *Rapport d'activités 2022*, 2023, 164 p.

RAPPORT D'ACTIVITÉS 2022

Comité permanent de Contrôle des services de renseignement et de sécurité

Comité permanent de Contrôle des services
de renseignement et de sécurité

Le présent Rapport d'activités 2022 a été approuvé par le Comité permanent de Contrôle des services de renseignement et de sécurité lors de la réunion plénière du 23 mai 2023.

(soussignés)
Serge Lipszyc, président
Thibaut Vandamme, conseiller
Linda Schweiger, conseillère
Bjorn Verschaeve, greffier faisant fonction

Rapport d'activités 2022
Comité permanent de Contrôle des services de renseignement et de sécurité

SOMMAIRE

LISTE DES ABRÉVIATIONS

AC(C)	Autorité de contrôle (compétente)
AG	Administrateur général (VSSE)
A.M.	Arrêté ministériel
Ann. parl.	Annales parlementaires
ANS	Autorité nationale de sécurité
ANSM	Autorité Nationale de la Sécurité Maritime
APD	Autorité de protection des données
A.R.	Arrêté royal
AR BDC	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 1erbis « de la gestion des informations » du chapitre IV de la loi sur la fonction de police
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 PH	Arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police
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	Banques de données communes
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)

BINII	*Belgian Intelligence Network Information Infrastructure*
BNG	Banque de données nationale générale
CAC	Cellule administrative de coordination
CCB	Centre pour la Cybersécurité Belgique
CCE	Conseil du Contentieux des Etrangers
CCRS	Comité de coordination du renseignement et de la sécurité
CEDH	Convention européenne des droits de l'homme
CelEx	Cellule Extrémisme (SPF Justice)
CI	*Counterintelligence*
CJUE	Cour de justice de l'Union européenne
CLSM	Comités Locaux de la Surêté Maritime
CM BDC	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
CNS	Conseil national de sécurité
Cour EDH	Cour européenne des droits de l'homme
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
CPS	Code Pénal Social
CRABV	Compte Rendu Analytique – *Beknopt Verslag*
CRIV	Compte Rendu Intégral – *Integraal Verslag*
CSIL-R	Cellule de Sécurité Intégrale Locale - Radicalisme
CTIF	Cellule de Traitement des Informations Financières
DG EPI	Direction générale des Établissements Pénitentiaires (SPF Justice)
DISCC	*Defense Intelligence and Security Coordination Centre* (SGRS)
DJSOC/Terro	Direction de la lutte contre la criminalité grave et organisée (section terrorisme) de la Police judiciaire fédérale
Doc. parl.	Documents parlementaires de la Chambre et du Sénat
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
EPV	Extrémiste potentiellement violent
FTF	*Foreign terrorist fighters*
HTF	*Homegrown terrorist fighters*
HUMINT	*Human intelligence*
ICT	*Information and communications technology*

IOWG	*Intelligence Oversight Working Group*
IPCO	*Investigatory Powers Commissioner's Office*
IRT	*Incident/intervention Response Team* (VSSE)
JDC	*Joint Decision Centre*
JIC	*Joint Intelligence Centre*
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
LPA	Loi du 11 avril 1994 relative à la publicité de l'administration
LPD	Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Loi protection des données)
L.R&S	Loi du 30 novembre 1998 organique des services de renseignement et de sécurité
LTF	*Local task force*
M.B.	Moniteur belge
MoU	*Memorandum of Understanding*
MPLUS	Méthodes ordinaires plus
MRD	Méthodes de recueil des données
NA	Note aux autorités
OCAM	Organe de coordination pour l'analyse de la menace
OE	Office des étrangers
OSINT	*Open sources intelligence*
OTAN	Organisation du Traité de l'Atlantique Nord
PCT	Personnes condamnées pour terrorisme
PH	Propagandistes de haine
PIO	*Prison Information Officer*
Plan R	Plan d'action Radicalisme
Plateforme CT	Plateforme commune contre-terrorisme
PROTEUS	Banque de données de l'OCAM

PSNR	Plan Stratégique National du Renseignement
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
RFC	*Requests for collect*
RFI	*Request for information*
RGPD	Règlement Général sur la Protection des Données
SGRS	Service Général du Renseignement et de la Sécurité
SIGINT	*Signal intelligence*
SOP	*Standard Operating Procedures*
SPF	Service public fédéral
Stratégie TER	note stratégique Extrémisme et Terrorisme
TF	*Terrorist fighters*
VSSE	Sûreté de l'État

PRÉFACE

Même si le constat n'est pas neuf, une rétrospective de l'année 2022 nous interpelle sur la fragilité de notre monde.

L'invasion de l'Ukraine le 24 février 2022, après la période COVID, a renforcé une crise mondiale qui nous touche comme cela n'était plus arrivé probablement depuis la Deuxième Guerre mondiale. Cette crise a provoqué une insécurité sociétale qui s'est manifestée non seulement par d'importantes difficultés socio-économiques mais qui a surtout entraîné un retour de très sombres réflexes de peur et de rejet d'autrui.

Dans l'accélération des mouvements géopolitiques, économiques et sociaux qu'elle entraîne, notre société de la communication semble clairement peiner face à des phénomènes dévastateurs pour l'Humanité comme le radicalisme, l'extrémisme ou encore le complotisme lesquels trouvent dans les médias sociaux des amplificateurs inédits de désinformation qui sont parfois hors de contrôle.[1]

Dans ce contexte, les menaces et les questions de sécurité qu'elles posent pour le développement démocratique de notre société questionnent radicalement nos gouvernements et leurs services de renseignement et de sécurité. En tout état de cause, les moyens et le fonctionnement de ces institutions essentielles doivent être adaptés.

A titre d'illustration, le « Qatargate » a secoué le landernau européen et belge en rappelant la réalité et les dangers d'une possible ingérence étrangère au sein de nos institutions. Cet 'épisode' entraîne et entraînera certainement encore un ajustement des mesures de prévention et des réponses à cette menace.

L'ouverture du procès des attentats de Bruxelles et de Zaventem constitue quant à lui un rappel de la nécessité accrue de protection des citoyens comme celle de l'Etat face au radicalisme, à l'extrémisme et au terrorisme.

Le Comité permanent R ne peut que saluer les plans d'investissement récents tant au niveau des ressources humaines, des infrastructures, des outils et des méthodes opérationnels pour nos deux services de renseignement. On relève également une volonté manifeste des autorités et des responsables des services de renforcer utilement les collaborations et leurs partenariats au profit de la sécurité nationale. L'analyse de la mise en œuvre des recommandations de la Commission parlementaire Attentats donne un aperçu du travail déjà effectué et du chemin

---

1 C. DUMBRAVA, *Les principaux risques des médias sociaux pour la démocratie. Risques liés à la surveillance, à la personnalisation, à la désinformation, à la modération et au microciblage*, Service de recherche du Parlement européen, décembre 2021, Bruxelles.
https://www.europarl.europa.eu/thinktank/fr/document/EPRS_IDA(2021)698845

encore à parcourir près de six ans après le dépôt du rapport sur l'architecture de la sécurité, le 15 juin 2017.[2]

A cet égard, le Comité R recommandait « *un débat public (parlementaire) plus large sur les tâches des deux services de renseignement prévues dans la loi organique des services de renseignement de 1998 et sur la priorisation qui y est liée. Ceci nécessite une discussion « stratégique » concernant l'octroi des capacités et moyens suffisants pour permettre à chacun des services de détecter, suivre et maîtriser comme il se doit toutes les menaces contre la sécurité (inter)nationale. Les services de renseignement et de sécurité doivent retenir l'attention du Parlement, et ce, pas uniquement ponctuellement lorsque surviennent des problèmes individuels* ».

Cette recommandation, comme bien d'autres, soulève également le problème de la juste appréhension des travaux du Comité par la Chambre, car il s'agit avant tout de veiller au bon fonctionnement de l'Etat ainsi qu'à celui des organes indépendants de contrôle. Ils sont là comme les oiseaux dans la mine, non pour détecter le CO, mais les dangers, les problèmes, les menaces qui touchent le citoyen et l'Etat.

Autre face d'une même pièce, le Comité permanent R veille, notamment en sa qualité d'autorité de protection des données, à ce que les services de renseignement et de sécurité assument et assurent pleinement leur rôle de protection des droits et libertés des individus. C'est le prix équilibré à payer pour notre démocratie.

De ce point de vue, le Comité permanent R maintient et renforce son attention pour que les services récoltent et traitent les renseignements de manière effectivement légale et proportionnelle. Pour rappel, le législateur a limité en 1998 la compétence du Comité aux seuls deux services de renseignement, mais des développements récents des missions de différents autres services entraînent une inquiétude grandissante quant au développement d'activités de renseignement sans véritable contrôle légal. Par ailleurs, si on peut se féliciter de la création en 2022 d'un « Cybercommand » au sein du SGRS, que cette unité soit envisagée comme nouvelle composante à part entière de la Défense interroge sur les capacités de contrôle de ses activités de renseignement dans le futur.

19 mai 2023

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

[2] COMITÉ PERMANENT R, Enquête de contrôle relative au suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats terroristes concernant les services de renseignement et de sécurité, octobre 2022.
https://www.comiteri.be/images/pdf/enquetes/Eindrapport_FR.pdf

CHAPITRE I.
LES ENQUÊTES DE CONTRÔLE

PRÉAMBULE

Diverses instances et personnes peuvent 'saisir' le Comité permanent R d'une enquête de contrôle : la Commission parlementaire de suivi, les ministres compétents, toute personne (morale) qui souhaite introduire une plainte ou faire une dénonciation, etc.

Le Comité permanent R a reçu, au total, 68 plaintes ou dénonciations en 2022.[1] Après une brève pré-enquête et la vérification de plusieurs données objectives, le Comité a rejeté 31 plaintes ou dénonciations parce qu'elles étaient manifestement non fondées (art. 34 de 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.Contrôle)), ou parce que le Comité n'était pas compétent pour en traiter les griefs. Dans ce dernier cas de figure, les plaignants ont été renvoyés, si possible, vers les instances compétentes (par exemple, le ministère public ou le Comité permanent P). 3 des 37 plaintes traitées ont pu être clôturées en 2022, 11 plaintes étaient toujours en cours de traitement début 2023. En 2022, 27 des 37 plaintes traitées l'ont été en tant que plaintes *Data Protection Authority* (DPA).[2]

Le Comité peut lui aussi prendre l'initiative d'ouvrir une enquête de contrôle. Ce fut le cas pour quatre des neuf enquêtes finalisées en 2022 (I.1, I.3, I.5 et I.9) tandis que cinq enquêtes ont été initiées à la demande de la Commission parlementaire de suivi (I.2, I.4., I.6, I.7 et I.8). Le Comité a par ailleurs poursuivi huit enquêtes ouvertes en 2022 ou antérieurement. Une description succincte des enquêtes en cours figure à la section I.10. Les recommandations émises à l'issue des enquêtes de contrôle ont été regroupées au Chapitre XI.

---

1 Dans un premier temps, la recevabilité de la plainte est examinée. Elle est ensuite classée dans une catégorie ('ordinaire', plainte APD, plainte MRD, etc.). Dans le cas d'une problématique générale, le Comité peut décider d'ouvrir une enquête de contrôle, sinon l'enquête reste limitée au traitement de la plainte.

2 Voir 'IV.2. Le traitement des requêtes individuelles'.

I.1. LE SUIVI DES CONDAMNÉS POUR TERRORISME

La récidive terroriste inquiète tant la Sûreté de l'Etat (VSSE)[3] que les responsables politiques.[4] Pourtant, des études scientifiques tendent à nuancer l'ampleur de ce danger et suggèrent au contraire un faible taux de récidivisme en matière de terrorisme.[5] Un seul cas de récidive peut toutefois avoir de lourdes conséquences et justifie que les services de renseignement s'y intéressent.

En Belgique, plus de 470 personnes ont été condamnées pour des faits de terrorisme entre 2015 et 2021.[6] En janvier 2022, parmi environ 10 700 détenus[7], on comptabilisait 136 détenus liés au terrorisme ou identifiés comme radicalisés dans les prisons belges.

Dans ce cadre, le Comité a ouvert en avril 2019 une enquête de contrôle afin d'évaluer la position d'information des services de renseignement et les moyens déployés dans le cadre du suivi des (anciens) détenus terro et radicalisés.[8] Le rapport d'enquête a été présenté à la Commission de suivi en juin 2022.

I.1.1. LE CADRE JURIDIQUE ET STRATÉGIQUE

Au-delà de la L.R&S qui détermine la compétence générale des services de renseignement (articles 7 et 8 pour la VSSE et articles 10 et 11 pour le SGRS), le suivi par la VSSE et le SGRS des (anciens) détenus terro et radicalisés est plus spécifiquement guidé par divers documents stratégiques. Certains de ces documents organisent le suivi *avant* et *après* la détention tandis que d'autres portent sur l'action des services de renseignement et de leurs partenaires *pendant* la détention. Il en résulte un cadre stratégique complexe et dispersé entre divers acteurs et niveaux de pouvoir.

---

3 VSSE, *Rapport d'activité 2017-2018*, 2018, p. 17 ; VSSE, *Rapport annuel 2020*, 2021, p. 27.

4 Enquête parlementaire 'Attentats', *Doc. parl.*, Chambre 2016-17, 54-1752/9, pp. 99-100.

5 T. RENARD, "Overblown: Exploring the gap between the Fear of Terrorist Recidivism and the Evidence", *CTC Sentinel*, Vol. 13, n°4, Avril 2020 ; Le faible taux de récidive des terroristes est confirmé dans un document du *Radicalisation Awareness Network* (RAN), une plateforme de concertation soutenue par la Commission européenne, qui l'évalue entre 5 et 8% en Europe mais encourage des recherches supplémentaires sur cette problématique, estimant manquer de données à la fois quantitatives et qualitatives. Dans : RAN, *La récidive chez les délinquants extrémistes violents et terroristes*, Document de conclusion, 24 février 2021.

6 *Doc. parl.* Chambre 2021-2, 55-148.

7 Belga, « Combien y-a-t-il de détenus dans les prisons belges ? », *Le Vif*, 27 décembre 2021.

8 Par l'expression « anciens détenus terro et/ou radicalisés », il est fait référence a) aux personnes prévenues ou inculpées pour faits qualifiés de terroristes, mises sous mandat d'arrêt ou bénéficiant soit d'un régime de détention préventive sous surveillance électronique, soit d'une mise en liberté sous conditions ; b) aux personnes, condamnées pour des faits de terrorisme, quittant un établissement pénitentiaire, par remise en liberté définitive ou sous quelques autres régimes ; c) et enfin, aux détenus (terro ou de droit commun) identifiés comme radicalisés pendant et après leur détention.

I.1.1.1. La Stratégie TER

En septembre 2021, la note stratégique Extrémisme et Terrorisme, dite Stratégie TER, a succédé au Plan d'Action Radicalisme (Plan R) pour organiser les échanges entre les partenaires nationaux en vue de la détection précoce des menaces terroristes et extrémistes.[9] Dans ce cadre, plusieurs plateformes de concertation ont été mises sur pied.

Pour le suivi des (anciens) détenus terro et/ou radicalisés, les partenaires échangent principalement, *pendant* la détention, lors des réunions du groupe de travail Prisons (GT Prisons), scindé depuis 2015 en un GT stratégique et un GT opérationnel. Désormais, le GT stratégique se compose de représentants de la VSSE, de l'OCAM, de l'Unité centrale antiterrorisme de la Direction centrale pour la lutte contre la criminalité grave et organisée de la police fédérale (DJSOC/Terro), de la Direction générale des Établissements pénitentiaires (DG EPI), du Centre de crise national, du SPF Affaires étrangères, de l'Office des Etrangers ainsi que de l'administration des Maisons de Justice (AGMJ). Trimestriellement, ces services se réunissent pour une consultation stratégique sur cette thématique et sur l'organisation du suivi de ces détenus.

A côté du GT stratégique, les réunions du GT opérationnel permettent aux partenaires d'identifier les détenus devant faire l'objet d'un suivi et d'échanger les informations à propos des dossiers individuels. Depuis 2021, le SGRS ne participe plus aux réunions (stratégiques ou opérationnelles) du GT Prisons.

Le suivi *après* la libération s'organise ensuite au sein des *local taskforces* (LTF) qui prennent le relai du GT Prisons opérationnel. Organisées au niveau des arrondissements judiciaires, les LTF stratégiques veillent « *à assurer la concordance entre les différentes taskforces locales opérationnelles* »[10] tandis que les LTF opérationnelles ont pour objectifs l'organisation du suivi des dossiers individuels ainsi que le traitement et l'échange d'informations entre les partenaires.[11]

---

9 OCAM, « La nouvelle stratégie contre le terrorisme et l'extrémisme remplace le plan d'action radicalisme », 8 septembre 2021, http://ocam.belgium.be.

10 OCAM, *Stratégie TER*, 2021, p. 10.

11 Au sein des LTF opérationnelles, présidées par le Directeur coordonnateur de l'arrondissement judiciaire (DirCo), sont représentés la (les) zone(s) de police locale, la (les) police(s) judiciaire(s) fédérale(s) (PJF), l'OCAM, les services de renseignement, DJSOC/Terro, l'Office des Etrangers, Fedasil ainsi que le parquet local. Les LTF stratégiques réunissent quant à elle le DirCo, le Procureur du Roi, et le Gouverneur de la province.

I.1.1.2. Le protocole d'accord VSSE – DG EPI

Dans le cadre de l'ancien Plan R, un protocole d'accord a été signé en 2006 entre la VSSE et la DG EPI.[12] L'objectif de ce protocole était de faciliter et d'organiser l'échange d'informations entre les deux administrations.

Dans ce cadre, la DG EPI communique d'initiative les informations recueillies par le personnel pénitentiaire sur les détenus terro ou en lien avec le radicalisme.[13] Pour sa part, la VSSE transmet les informations utiles en sa possession sur ces mêmes détenus.

Le protocole prévoit encore pour la VSSE un accès direct à la banque de données « SIDIS Suite » de la DG EPI. Cette banque de données reprend les informations relatives aux détenus telles que les données d'identification, les données judiciaires ou encore les visiteurs.

Au moment de l'enquête, un nouveau protocole d'accord, en discussion depuis 2016, était sur le point d'être finalisé.[14] Ce nouveau protocole vise à rendre compte de l'évolution des pratiques et des échanges entre la VSSE et de la DG EPI.

I.1.1.3. Le Plan d'action contre la radicalisation dans les prisons

En 2015, un plan d'action contre la radicalisation dans les prisons a été publié. Elaboré autour de dix points d'action, le document poursuit un double objectif : « *éviter que les détenus se radicalisent pendant leur séjour en prison* » et « *développer un encadrement spécialisé des personnes radicalisées pendant leur détention* ».[15]

Dans le cadre de la mise en œuvre de ce plan d'action, une cellule Extrémisme (CelEx) a été mise sur pied au sein de la DG EPI. Parmi ses missions, CelEx récolte les informations depuis les prisons et formule des recommandations quant au régime de détention à appliquer aux détenus identifiés comme radicalisés. Parmi les collaborateurs de CelEx, des coordinateurs servent également de points de contact pour les établissements pénitentiaires et les services partenaires.

Certains points d'action visent directement les services de renseignement et en particulier la cellule *Counter extremism Gevangenis* – Prison (CEGP) de la VSSE. Ainsi, le plan d'action appelle par exemple à « *une position plus forte en matière d'information ainsi qu'un recueil et une analyse de l'information plus ciblés* ».

---

12 Voir COMITE PERMANENT R, *Rapport d'activités 2016*, pp. 56-62 ('La VSSE et le Protocole de coopération avec les établissements pénitentiaires'). Voir également COMITE PERMANENT R, *Rapport d'activités 2018*, pp. 28-29 ('L'évaluation du protocole DG EPI/VSSE').

13 Par exemple, situation pénitentiaire, libérations, sorties, contacts externes (visiteurs, courriers, téléphonie) et en prison, comportements, incidents (bagarre, objets trouvés lors de contrôles, tentative de suicide, etc.), comptes cantine prison, lectures, activités culturelles ou tout autre élément à la demande de la VSSE.

14 Dans le rapport d'activités 2021-2022 de la VSSE, l'Administratice générale a.i. annonçait la signature d'un nouvel accord avec la DG EPI (VSSE, *Intelligence Report 2021-2022*, 2023, www.vsse.be, p. 4).

15 SPF Justice, *Plan d'action contre la radicalisation dans les prisons*, 11 mars 2015, p. 3.

En 2018, des discussions ont été entamées entre les partenaires (DG EPI, DJSOC/Terro, OCAM, VSSE) et le ministre de la Justice pour actualiser ce plan d'action. A cette occasion, a notamment été suggérée la désignation d'un *(Prison) Information Officer* (PIO)[16] parmi le personnel de direction de chaque prison. Collaborateur de la DG EPI et détenteur d'une habilitation de sécurité, le PIO serait chargé de récolter et de traiter les informations en prison et de faciliter les actions opérationnelles de la VSSE. La DG EPI insistait toutefois sur la réticence du personnel pénitentiaire face à cette fonction de récolte d'informations, pourtant considérée comme cruciale par la VSSE.

En décembre 2021, le ministre de la Justice annonçait l'engagement de plus de 20 coordinateurs de sécurité pour les prisons comme point de contact pour la VSSE.[17] Dans le cadre d'un projet pilote de la DG EPI, ces coordinateurs de sécurité prendront en charge les missions envisagées pour les PIO. Membres des équipes de direction des prisons, ils endosseront toutefois également des tâches de management. En cela, la fonction diffère de celle de PIO imaginée par la VSSE.

I.1.2. UN OUTIL CENTRAL POUR LE SUIVI DES (ANCIENS) DÉTENUS TERRO OU RADICALISÉS : LA BANQUE DE DONNÉES COMMUNE *TERRORIST FIGHTERS*

Depuis 2016, l'échange d'informations en matière de terrorisme et d'extrémisme entre les services de sécurité est facilité par la banque de données commune *Terrorist Fighters* (BDC TF).[18] Pour chaque entité inscrite, les BDC contiennent une fiche de renseignements avec les données non classifiées à disposition des services ainsi qu'une évaluation de la menace par l'OCAM.

La BDC TF est mobilisée pour le suivi des (anciens) détenus terro et radicalisés. Ce suivi spécifique a d'ailleurs encouragé l'ajout de deux nouvelles catégories en 2019, à savoir les 'personnes condamnées pour terrorisme' (PCT) et les 'extrémistes

---

16 Dans le cadre du Plan d'action contre la radicalisation au sein des prisons de 2015 déjà, il avait été question de coordinateurs locaux pour les prisons.

17 *Doc. parl.* Chambre 2021-2, CRIV 55 PLEN 144, p. 16. Appelés aussi « *coordinators security and safety* ».

18 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 ; A.R. du 23 avril 2018 modifiant l'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 et modifiant la banque de données commune '*foreign terrorist fighters*' vers la banque de données commune '*terrorist fighters*', *M.B.,* 30 mai 2018. Parallèlement, les ministres de l'Intérieur et de la Justice ont transformé en 2018 la *Joint Information Box* en une banque de données commune Propagandistes de haine (BDC PH).

potentiellement violents' (EPV).[19] [20] Aux yeux de la VSSE plus spécifiquement, ces nouvelles catégories présentent une plus-value car elles fournissent des critères objectifs et apportent davantage de clarté dans le suivi des entités concernées.

L'OCAM présente la catégorie des PCT[21] comme un « *dernier filet de sécurité* ».[22] En effet, elle vise à continuer à suivre les individus condamnés pour terrorisme mais qui n'attirent plus immédiatement l'attention des services de sécurité, en assurant un suivi à leur libération via les LTF ou les cellules de sécurité intégrale locales (CSIL).[23]

---

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

20 Voir COMITE PERMANENT R et C.O.C., Avis concernant un projet d'arrêté royal modifiant l'arrêté royal du 21 juillet 2016 relatif à la banque de données commune *Terrorist Fighters*, 1er août 2019, 001/CPR-C.O.C./2019.

21 Dans la banque de données, la catégorie PCT vise les individus qui, cumulativement :

- ont un lien avec la Belgique ;
- ont été condamnés ou pour lesquels ont été prononcées des décisions judiciaires d'internement ou, dans le cas de mineurs, ont fait l'objet d'une mesure de protection pour commission d'infractions terroristes, telles que décrites au Livre II Titre I Ter du Code pénal en Belgique ou des faits qualifiés comme tels ou par une infraction équivalente à l'étranger ;
- et dont l'OCAM évalue le niveau de menace comme moyen (niveau 2), grave (niveau 3) ou très grave (niveau 4).

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

22 OCAM, « Extrémisme de droite et Covid-19 », *Insight*, n° 10, p. 44.

23 Note VSSE.

La catégorie des EPV[24] a pour sa part été ajoutée afin de suivre les détenus identifiés comme radicalisés qui ne remplissaient pas les conditions nécessaires pour être inscrits dans les catégories FTF, HTF ou propagandiste de haine mais qui méritaient, aux yeux des services de sécurité, d'être suivis de près – par exemple de par leur comportement durant la détention.

Le tableau ci-dessous offre un aperçu chiffré de l'évolution des entités inscrites sous les catégories PCT et EPV.[25]

	Mai 2019	**Mai 2020**	**Octobre 2021**	**Janvier 2022**
PCT	NA	16 (2,4%)	29 (4,1%)	30 (4,2%)
EPV	NA	13 (2%)	77 (11%)	106 (14,8%)
Total BDC TF & HP	696	672	712	713

Entre mai 2020 et janvier 2022, le nombre de PCT enregistrées dans la BDC a presque doublé. Parmi les 30 entités enregistrées sous PCT en janvier 2022, 7 étaient encore en détention.

En janvier 2022, 23 des 106 EPV étaient en détention en Belgique tandis que 33 anciens détenus étaient enregistrés sous cette catégorie. Trois ans après sa création, la catégorie EPV représente près de 15% des entités inscrites dans la BDC, sans toutefois que cela ne soit jugé interpellant par la VSSE.[26]

---

[24] Les extrémistes potentiellement violents sont définis comme les individus qui répondent aux critères cumulatifs suivants :
- ils ont des conceptions extrémistes pouvant justifier l'usage de la violence ou de la contrainte comme méthodes d'action en Belgique ;
- il existe des indications fiables qu'ils ont l'intention de recourir à la violence, et ce en relation avec leurs conceptions extrémistes ;
- ils répondent à l'une des conditions suivantes, considérées comme facteurs de risque quant à l'utilisation de la violence :
  - ils entretiennent systématiquement des contacts sociaux au sein des milieux extrémistes ;
  - ils ont des problèmes psychiques constatés par un professionnel compétent ;
  - ils ont commis des actes ou présentent des antécédents qui peuvent être soit considérés comme a) un crime ou un délit portant atteinte à ou menaçant l'intégrité physique ou psychique de tiers ; b) des instructions ou des formations relatives à la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes ou substances nocives ou dangereuses, ou pour d'autres méthodes et techniques spécifiques en vue de commettre des infractions terroristes ; c) des agissements en connaissance de cause constituant un soutien matériel en faveur d'une organisation d'un réseau terroriste/extrémiste ; d) des agissements dont la nature indique un niveau de vigilance préoccupant des individus à l'égard de la sécurité.

[25] Si les entités peuvent être enregistrées sous plusieurs catégories, ce n'est pas le cas des PCT qui ne peuvent avoir de double statut.

[26] En janvier 2022, il s'agissait toutefois de la troisième catégorie la plus importante en nombre d'entités inscrites après les FTF de catégorie 1 (en Syrie/Irak) et les FTF de catégorie 3 (*returnees*).

I.1.3. LE SUIVI OPÉRATIONNEL PAR LES SERVICES DE RENSEIGNEMENT PENDANT LA DÉTENTION

Le travail des services de renseignement vis-à-vis des (anciens) détenus terro et radicalisés s'organise en deux temps : pendant la détention et après la libération. Pendant la détention, le suivi poursuit un double objectif : d'une part, éviter la radicalisation des (co-)détenus et, d'autre part, préparer le suivi après leur libération, ce afin d'empêcher toute (tentative) de récidive d'infractions terroristes.

I.1.3.1. Le SGRS : une compétence théorique

Dans le cadre du suivi des détenus terro et radicalisés, la compétence du SGRS se limite aux anciens militaires, militaires actifs, réservistes et candidats militaires ainsi qu'aux membres civils de la Défense. En pratique, le SGRS n'assure toutefois pas un suivi actif des anciens membres de la Défense condamnés pour terrorisme. En effet, parce qu'une condamnation pénale pour infractions terroristes est incompatible avec un emploi à la Défense, le SGRS ne suit ces individus que lorsqu'ils sont reliés à un membre *en exercice* de la Défense. En janvier 2022, le SGRS disait ne mener aucune enquête ou opération en lien avec des PCT inscrites dans la BDC.

I.1.3.2. La VSSE : un suivi au cas par cas

Au sein de la VSSE, la cellule *Counter extremism Gevangenis* – Prison (CEGP) est chargée de la collecte et du traitement des informations relatives aux détenus. A partir de ces informations, la CEGP rédige des notes d'analyse du phénomène de radicalisme et de terrorisme dans les prisons mais aussi, pour chaque détenu repris dans la BDC, une note en prévision de sa libération.

La récolte d'informations au sein des prisons par la VSSE

En prison, étant donné les moyens à sa disposition, la VSSE travaille principalement à obtenir une meilleure image du phénomène de radicalisation et cela, en étroite coopération avec les entités fédérées. Toutefois, la VSSE admet des relations difficiles avec certains acteurs compétents en matière de « désengagement » chez qui elle perçoit un manque de confiance, et de qui elle ne reçoit que peu de retour sur leurs contacts avec les détenus. En revanche, la VSSE dit entretenir une bonne collaboration avec les Maisons de Justice.

La récolte d'informations pendant la détention par la VSSE vise donc avant tout à obtenir une image de la situation en prison. Pour se faire, le service déploie différentes méthodes de recueil d'informations prévue par la L.R&S (artt. 14 à 19).

Parmi les obstacles qu'elle identifie à un suivi efficace des détenus terro et identifiés comme radicalisés, la VSSE souligne la lourde charge que représente le

travail de récolte et d'analyse des informations par la CEGP. Elle pointe en outre le besoin de coopération systématique avec les établissements pénitentiaires.

La VSSE salue par contre la très bonne coopération avec la CelEx, DJSOC/Terro et l'OCAM. Au sein du GT Prisons en particulier, la circulation de l'information semble satisfaisante.

La récolte d'informations à travers la coopération avec la Direction Générale des Etablissements Pénitentiaires

La DG EPI est un partenaire essentiel de la VSSE. Son logiciel SIDIS Suite, auquel la CEGP a accès, centralise les données des détenus (données personnelles, empreintes digitales, parcours et régime pénitentiaires, visiteurs, congés, etc.). Pour les détenus inscrits dans la BDC, l'encodage de tout mouvement extérieur (congé, libération conditionnelle, libération de fin de peine, etc.) est automatiquement transmis par message-*push* aux différents partenaires de la DG EPI, en ce compris la VSSE.

Au sein de la DG EPI, la CelEx est chargée de l'échange quotidien d'informations relatives à la radicalisation et à l'extrémisme vers les services locaux et centraux de l'administration pénitentiaire ainsi qu'à l'ensemble de ses partenaires externes.[27] Avec la CEGP plus spécifiquement, l'échange d'informations vise notamment à partager les fiches d'évaluation des détenus rédigées par CelEx reprenant par exemple des informations sur leur comportement quotidien, les éventuels incidents, les contacts internes, les visites, le passé carcéral et les mouvements financiers. Les observations effectuées par le personnel pénitentiaire (lectures, sujets de conversation, attitude, idéologie, etc.) y sont reprises.

Dans le cadre de ses missions, la CelEx a élaboré sa propre banque de données de détenus liés au terrorisme et à la radicalisation qui a longtemps guidé le travail des partenaires au sein du GT Prisons pour identifier les dossiers prioritaires. En 2018 toutefois, après l'attaque de Benjamin Herman à Liège et face à une multiplication de listes et banques de données propres à chaque service, le ministre de la Justice a demandé à ce que la liste CelEx soit intégrée aux banques de données communes quitte à supprimer les détenus qui n'entrent pas dans les définitions des catégories prévues dans les BDC PH et TF. Par le passé effectivement, la multiplication des listes avec des finalités, des définitions et donc des chiffres différents a pu créer de

[27] Tous les deux mois, la CelEx rédige ainsi des rapports d'observations sur les détenus qu'elle suit. Une synthèse de ces rapports est envoyée, pour information, aux partenaires (OCAM, DJSOC/Terro et VSSE) et est saisie dans les BDC. Les partenaires sont en outre informés de toute nouvelle incarcération de personnes suspectées ou condamnées pour des faits liés au terrorisme ainsi qu'en cas de soupçons de radicalisation d'un détenu. A la demande des directions de prison, la CelEx peut également émettre des avis non contraignants sur les conditions de détention des détenus ainsi que sur les modalités d'exécution de la peine.

la confusion.[28] Depuis 2020, la VSSE se base sur les chiffres de la BDC et affirme qu'il est désormais clair pour l'ensemble des partenaires que celle-ci constitue l'instrument de référence. Le Comité constate toutefois que chaque service a conservé sa propre base de données, bien que limitée à un usage interne.

Les fiches de synthèse individuelles

Six mois avant la libération, la VSSE rédige des fiches de synthèse individuelles pour chaque détenu repris dans la BDC. L'élaboration de telles fiches vise à réunir, avant la sortie effective de prison, les éléments pertinents en possession de la VSSE (par exemple, les actes commis par le détenu en prison, la mouvance et l'organisation à laquelle le détenu a appartenu ou appartient toujours, le réseau relationnel entretenu tant en Belgique qu'à l'étranger ainsi que les capacités techniques et organisationnelles potentielles de l'intéressé).

À partir de cette note classifiée, la CEGP rédige une fiche de synthèse non classifiée destinée à la banque de données commune.

L'instrument ThETIS comme outil d'analyse

Dans le cadre du suivi des détenus terro ou identifiés comme radicalisés, la VSSE utilise l'instrument ThETIS (*Target Evaluation Tool Indicator Based*)[29] pour évaluer le degré de radicalisation d'un individu et le risque de recours à la violence. Mobilisé pour l'ensemble des détenus qui arrivent en fond de peine, ThETIS permet ainsi à la VSSE de définir les cibles prioritaires.

La diffusion des informations et renseignements

Les informations récoltées par la VSSE, par ses propres moyens et dans le cadre de sa coopération avec la DG EPI, sont ensuite partagées avec les partenaires externes sous différents formats.

Depuis 2015, la CEGP rédige une note annuelle générique à propos des détenus de la BDC[30] qui seront ou pourraient être libérés au cours de l'année à venir. Actualisée pluri-annuellement, cette note est transmise à la DG EPI, au SGRS, à l'OCAM, à l'OE, à la Police Fédérale, au parquet fédéral et aux cabinets respectifs des Premier ministre et ministres de la Justice et de l'Intérieur. Le contenu des

---

28 Ainsi, au 31 décembre 2018, CelEX suivait 212 détenus (dont 112 détenus terro). De son côté, la VSSE estimait – sur base d'une extrapolation – le nombre de détenus terroristes ou radicalisés autour de 450, mais pointait le risque que beaucoup étaient sans doute suivis à tort.

29 Développé par la VSSE à partir du *Violent Extremist Risk Assessment 2 Revised* (VERA-2R) du *Nederlands Instituut voor Forensische Psychiatrie en Psychologie* (NIFP).

30 Jusqu'en 2018, les notes génériques traitaient de tous les détenus de la liste CelEx.

notes est également discuté en GT Prisons et en LTF. Cette note est également envoyée, à leur demande, à certains partenaires étrangers.

Outre la note annuelle générique, la VSSE réalise également une note « fond de peine » pour chaque détenu terro ou identifié comme radicalisé.[31] Cette note aux autorités (NA) résume le parcours carcéral dudit détenu arrivant à fond de peine, ses contacts et les observations faites durant sa détention. Elle contient en outre des éléments sur l'évolution probable du détenu après sa sortie de prison.[32] Ces NA sont transmises aux partenaires de la VSSE (DG EPI, DJSOC/Terro, OCAM, Parquet fédéral, SGRS) un mois avant la libération des détenus inscrits dans la BDC et sont ensuite discutées au sein des LTF ou dans le cadre des CSIL-R selon le profil des entités.

A la lecture de différentes notes fond de peine transmises par la VSSE, le Comité a pu constater la pertinence de l'exercice qui offre un regard complet sur le parcours pénitentiaire du détenu. Ces notes alimentent ensuite les discussions et échanges au sein du GT Prisons opérationnel.

I.1.4. LE SUIVI OPÉRATIONNEL PAR LES SERVICES DE RENSEIGNEMENT APRÈS LA LIBÉRATION FOND DE PEINE

Après la détention, la nécessité d'un suivi par les services de renseignement et/ou par les services de police est discutée entre les partenaires. Il n'y a donc pas de suivi automatique des anciens détenus terro et/ou radicalisés par les services de renseignement. En outre, ceux-ci se concentrent principalement sur les libérations fond de peine, les (quelques) individus libérés sous conditions[33] faisant l'objet d'un suivi par les services de police et les Maisons de Justice.[34]

---

31 Sauf si la collecte de nouvelles informations ne justifie pas la rédaction d'une note. Le cas est alors discuté au sein du GT opérationnel.

32 Depuis 2018, la VSSE assure ainsi la rédaction des notes pour les détenus libérés à fond de peine tandis que l'OCAM se charge des notes pour les détenus libérés anticipativement, sous conditions ou non. Cette répartition des tâches, avant tout pragmatique, est toutefois artificielle.

33 Voir notamment la COL 10/2018 du Collège des procureurs généraux près les cours d'appel du 28 juin 2018 détaillant les conditions pouvant être imposées à des personnes poursuivies ou condamnées pour des faits de terrorisme ou engagées dans l'extrémisme violent.

34 Notamment sur la base de l'article 20 de la Loi du 5 août 1992 sur la fonction de police (*M.B.*, 1 janvier 1993) et de la COL 11/2013 du ministre de la Justice, du ministre de l'Intérieur et du Collège des procureurs généraux près les cours d'appel du 7 juin 2013.

I.1.4.1. La concertation avec les partenaires au sein des local taskforces

Dans le cadre de la Stratégie TER, les *local taskforces* sont chargées du « suivi de sécurité » (traduction libre)[35] afin de garantir la sécurité publique en prenant en charge les dossiers amenés par la CSIL-R ou par l'un des partenaires.

Les cas particuliers des anciens détenus terro ou identifiés comme radicalisés sont également discutés en LTF. Lors des réunions opérationnelles, à partir des informations encodées dans la BDC et des notes de fond de peine rédigées par la VSSE, les services définissent ensemble les actions à entreprendre dans le cadre du suivi des entités concernées.[36]

Malgré l'obligation d'au minimum une réunion par mois, les 20 LTF déployées à l'échelle provinciale se rencontrent en moyenne 10 fois par an, soit entre six et douze réunions annuelles selon les LTF.

I.1.4.2. Le SGRS : un champ d'action très restreint

Le SGRS s'intéresse exclusivement aux anciens détenus qui apparaissent dans un dossier terro concernant un membre *actif* de la Défense (y compris les réservistes). Le SGRS justifie ce champ d'action restreint par son rôle de soutien dans cette matière, d'une part, et par des moyens limités, d'autre part – qui par exemple l'empêchent de prévoir une représentation autonome aux réunions du GT Prisons.

Ce suivi théorique ne fait l'objet d'aucune directive interne et aucun moyen structurel n'est dédié à cette problématique. Et pour cause, en janvier 2022, le SGRS disait ne suivre aucun dossier de ce genre.

Par le passé, le SGRS a regretté ne pas être systématiquement averti par le SPF Justice ou par ses partenaires des libérations des détenus terro anciennement reliés à la Défense dont il ne prenait connaissance que lors des réunions opérationnelles des LTF. L'accès à la base de données SIDIS Suite permettrait « *de pallier ce manque d'informations* » mais n'était toujours pas effectif au moment de l'enquête et restait en l'attente d'un arrêté royal.[37]

---

35 « *veiligheidsopvolging* » (Note VSSE).

36 Les partenaires peuvent par exemple opter pour un « *zichtbare en aanklampende opvolging* » par les corps de police locale à travers des discussions avec la famille/l'école/l'employeur, ou l'organisation de visites domiciliaires mensuelles. Le dossier peut également être renvoyé vers l'Office des Etrangers en vue d'un éloignement du territoire ou vers la CSIL-R compétente (voir Annexe 2). En 2021, la VSSE pointait toutefois le feedback quasi-inexistant des CSIL-R.

37 La Loi du 5 mai 2019 portant dispositions diverses en matière d'informatisation de la Justice, de modernisation du statut des juges consulaires et relativement à la banque des actes notariés (*M.B.*, 19 juin 2019) prévoit un droit de lecture des données traitées dans SIDIS Suite à divers services dont la VSSE, le SGRS et l'OCAM. L'étendue et les modalités de ce droit de lecture doivent par contre être définies dans un arrêté royal.

I.1.4.3. La VSSE : un suivi selon l'évaluation de la menace et les moyens disponibles

Après la libération à fond de peine, la VSSE poursuit le suivi de certains anciens détenus terro et/ou radicalisés selon le résultat de l'évaluation réalisée en interne ainsi que les capacités du service.

Le rôle des sections Contre-Extrémisme et Contre-Terrorisme et des front offices de la VSSE

Une fois les détenus libérés, ce sont les sections Contre-Extrémisme (CE) et Contre-Terrorisme (CT) ainsi que les *front offices* de la VSSE[38] qui se partagent le travail de suivi des anciens détenus. La stratégie de récolte d'informations après la libération fait l'objet d'une concertation en interne et est définie selon les priorités du service et les moyens disponibles.

Le cas des détenus étrangers : la coopération avec l'Office des Etrangers

La VSSE travaille également étroitement avec l'OE et sa Cellule Radicalisme dans le cadre du suivi des détenus étrangers libérés et placés en centres fermés en vue d'un éloignement.

Les fiches individuelles élaborées par la VSSE sur les détenus terro et/ou radicalisés n'ayant pas droit au séjour sur le territoire belge sont envoyées à l'OE. Celui-ci pourra alors transmettre des informations complémentaires à la VSSE afin qu'elle puisse étoffer sa note de fond de peine. Plus encore, ces informations permettront d'effectuer le suivi effectif des détenus sans droit de séjour après leur libération et leur placement en centres fermés en vue de l'éloignement du territoire.

La coopération internationale

Un échange d'informations est également organisé avec les partenaires étrangers sur base d'une évaluation de la menace représentée par l'intéressé, pour autant que celui-ci ait un lien direct avec le pays partenaire. Ce besoin d'échanger avec les partenaires est évalué au cas par cas.

Plus particulièrement, sur la base de la L.R&S et des instructions du Collège des procureurs généraux, la VSSE envoie une copie de la note annuelle générique à un partenaire étranger, à sa demande. Cet échange respecte le cadre légal prévu dans la L.R&S (en particulier, en son article 19). Le Comité s'interrogeait toutefois sur la spécificité d'un tel échange d'informations avec un partenaire particulier et, surtout, sur l'usage qui en est fait par celui-ci. Le Comité s'inquiète en outre

[38] Ou délocalisations des sections centrales.

du partage d'informations sur des détenus ayant purgé leur peine et qui ne font potentiellement pas ou plus l'objet d'un suivi par les services de renseignement et de sécurité belges. Une telle démarche semble en outre contraire à l'approche au cas par cas supposée guider l'échange d'informations avec les partenaires étrangers.

I.1.5. CONCLUSIONS

Inquiétude sociale et politique, le danger de récidive terroriste est pris au sérieux par les services de renseignement. Si le SGRS restreint son action à une compétence avant tout théorique, la VSSE assure le suivi des détenus terro et/ou radicalisés tout au long de l'exécution de leur peine ainsi qu'après leur libération.

Dans le cadre de la Stratégie TER, la VSSE travaille étroitement avec ses partenaires afin d'assurer ce suivi. À ce stade de l'évaluation, le Comité permanent R se doit de constater que le système de suivi fonctionne.

La VSSE, l'OCAM et DJSOC/Terro encouragaient la désignation de *prison information officers* dans chaque établissement pénitentiaire afin d'y suivre le phénomène terroriste et extrémiste. L'engagement de coordinateurs de sécurité annoncé en décembre 2021 par le ministre de la Justice semble être une alternative prometteuse dont il faudra observer la concrétisation.

Au cours de son enquête de contrôle, le Comité a pu constater la coopération étroite entre la VSSE et la DG EPI qui permet une récolte satisfaisante d'informations. Les plateformes de concertation, et en particulier le GT Prisons et les LTF, ainsi que la banque de données commune TF semblent en outre assurer une bonne circulation de l'information. La principale difficulté rencontrée dans le cadre du suivi des (anciens) détenus terro ou radicalisés semble davantage toucher au manque structurel de moyens qui oblige la VSSE (et ses partenaires) à prioritiser les dossiers. La coordination entre les services prévue dans le cadre de la Stratégie TER et de ses différentes plateformes de concertation permet toutefois de pallier le manque de ressources.

I.2. DES MOYENS DE RENSEIGNEMENT OFFENSIFS POUR LES SERVICES DE RENSEIGNEMENT ?

I.2.1. ORIGINE ET DÉLIMITATION DE LA QUESTION D'ENQUÊTE

Mi-2020, la Commission parlementaire d'accompagnement a demandé au Comité permanent R de se pencher sur la nécessité éventuelle de doter les services

de renseignement belges, à l'instar de certains pays voisins, de capacités de renseignement à l'étranger, par exemple sous la forme de « *services extérieurs* ».[39]

Le Comité a décidé de limiter le rapportage de cette enquête à la VSSE. En effet, en ce qui concerne le SGRS, le service de renseignement militaire est déjà actif à l'étranger, et tant sa mission légale que la manière dont certaines de ses compétences sont définies ne laissent planer aucun doute sur ses « capacités à l'étranger ». Le SGRS est un service qui, par nature et compte tenu des missions qui lui sont assignées, collecte des renseignements sur et à l'étranger. Il s'agit donc d'un service qui, par définition, est actif à l'étranger.[40]

Différents termes sont mobilisés pour désigner les activités de services de renseignement en dehors de leur territoire national. Il est par exemple fait usage des termes 'services extérieurs', 'services étrangers', 'services offensifs'[41], mais aussi 'services de renseignement' (dont la sphère d'intérêt serait axée sur les menaces extérieures alors que les menaces intérieures seraient la sphère d'intérêt des services dits 'de sécurité'), etc. Le Comité permanent R a opté pour la terminologie « capacités de renseignement à l'étranger » qui renvoie aux :

> *activités opérationnelles, clandestines ou non, déployées à l'étranger par les services de renseignement (cela inclut également les activités de collecte qui sont effectuées à partir du territoire belge mais qui ont leurs effets à l'étranger) en vue de collecter des informations sur des menaces tant intérieures qu'extérieures.*

Conformément à leurs missions légales, les services de renseignement belges ne se limitent pas au suivi de phénomènes survenant à l'intérieur des frontières nationales. Les informations *sur* l'étranger font également partie de leurs missions. Ainsi, il peut être nécessaire de collecter des informations sur une menace nationale à l'étranger.

Les renseignements peuvent être collectés à l'étranger de manière ouverte (comme par exemple consulter des sources ouvertes) ou dans la clandestinité la plus totale (lorsque, par exemple, les activités déployées ne sont pas portées à

---

39 Le rapport d'enquête a été envoyé à la commission de suivi en octobre 2022.

40 Comme en témoignent plusieurs enquêtes de contrôle antérieures du Comité, le SGRS fait usage de ces capacités à l'étranger. Voir par exemple COMITÉ PERMANENT R, *Rapport d'activités 2014* ('Le rôle du SGRS dans le suivi du conflit en Afghanistan'), pp. 11-12 ; *Rapport d'activités, 2018*, pp. 18-21 ('Les activités du SGRS dans une zone d'opération à l'étranger') ; *Rapport d'activités 2020*, p. 65 ((I.10. Incidents dans une zone d'opération à l'étranger'). Dans le même sens, les compétences du SGRS et les interceptions à l'étranger, les prises d'images et les intrusions dans des systèmes informatiques.

41 Les termes 'services offensifs' ont finalement été abandonnés car ils sont souvent associés à des opérations clandestines à l'étranger. Ces actions menées à l'étranger sont souvent associées à de la propagande, à la livraison d'armes, à l'endommagement d'infrastructures voire à l'élimination physique de certaines personnes et au soutien actif ou à l'exécution de coups d'État. La VSSE a insisté sur ce point, arguant que l'utilisation des termes 'services offensifs' pourrait générer une confusion inutile parmi ses partenaires étrangers.

la connaissance des autorités étrangères, voire sont illégales dans le pays où les activités sont exercées).

Par ailleurs, tout ou partie de la collecte peut se faire à partir du territoire belge (par exemple, extraire des informations de communications étrangères à partir de la Belgique).

Enfin, il convient de préciser que les capacités de renseignement envisagées dans le cadre de l'enquête de contrôle se limitent à un objectif de collecte d'informations. Les capacités d'intervention directe à l'étranger – par exemple dans le cadre d'une mesure d'entrave – n'ont pas été examinées.

I.2.2. LES CAPACITÉS DE RENSEIGNEMENT DE LA VSSE À L'ÉTRANGER : LE CADRE LÉGAL

Conformément aux articles 7 et 8 de la Loi du 30 novembre organique des services de renseignement et de sécurité (L.R&S), les compétences de la VSSE en matière de renseignement sont définies par des intérêts à protéger combinés à des menaces à maîtriser.[42] A cette fin, la VSSE recherche et analyse « *le renseignement relatif à toute activité* » (art. 7, 1°) qui menace ou pourrait menacer un ou plusieurs intérêts énumérés par la loi.

Dans ce cadre, la VSSE ne doit pas limiter son attention aux menaces présentes à l'intérieur des frontières nationales. Les menaces dont l'origine ou le(s) motif(s) dépasse(nt) les frontières nationales font partie de la sphère d'intérêt du service. Cette orientation extraterritoriale est importante pour la protection des intérêts de l'État, qu'ils soient dirigés vers l'extérieur ou vers l'intérieur.

Et pour suivre efficacement cette menace intérieure ou étrangère, la VSSE (tout comme le SGRS) ne doit pas limiter ses opérations au territoire belge. Le cadre légal permet à la VSSE, dans les limites décrites ci-dessous, de collecter des renseignements à l'étranger et de déployer des activités de collecte en dehors du territoire belge via quatre procédés.

(1) Par la coopération et l'échange d'informations avec des services partenaires étrangers

L'article 20 §1er L.R&S dispose *in fine* que le SGRS et la VSSE *« veillent à assurer une coopération avec les services de renseignement et de sécurité étrangers »*. Cette coopération peut être bilatérale ou multilatérale.

---

42 Les 'intérêts' à protéger sont : (1) la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, (2) la sûreté extérieure de l'État et les relations internationales, (3) le potentiel scientifique ou économique du pays. Les 'menaces' à maîtriser sont : (1) l'espionnage, (2) l'ingérence, (3) l'extrémisme, (4) le terrorisme, (5) la prolifération, (6) les organisations sectaires nuisibles et (7) les organisations criminelles.

Via des échanges avec des services partenaires, la VSSE peut prendre connaissance et traiter des renseignements relatifs à des phénomènes étrangers. La coopération informelle au niveau international au sein du Club de Berne est importante à cet égard. Ce procédé de collecte de renseignements ne requiert aucune activité sur un territoire étranger, à l'exception de réunions de travail occasionnelles.

En outre, des officiers de liaisons (LO) peuvent être envoyés à l'étranger. Il va de soi que ceux-ci se trouvent alors physiquement à l'étranger, travaillent souvent (mais pas toujours) dans les bureaux de services homologues, mais ne se rendent pas seul sur le terrain pour collecter des renseignements.

(2) Via des méthodes ordinaires de renseignement

Afin de collecter des renseignements, la VSSE peut également faire usage de méthodes de renseignements ordinaires. En effet, la loi n'a nullement limité l'utilisation de ces méthodes – autres que les méthodes particulières – au territoire belge.

Cela ne signifie évidemment pas que ces méthodes seraient autorisées par ce pays tiers, ni que les acteurs étrangers sont tenus de se conformer à ce qui peut être considéré comme une « réquisition » pour les acteurs belges (comme l'obligation pour les autorités, les opérateurs de télécommunications ou les établissements de logement de fournir des informations sur demande). D'un point de vue juridique belge, rien n'empêche toutefois la VSSE d'utiliser toutes les méthodes ordinaires (ouvertement ou clandestinement) à partir du territoire belge ou même dans un pays tiers.

Dans la pratique, le Comité identifie deux possibilités pour la VSSE en vue de collecter des renseignements à l'étranger en matière de méthodes de renseignement ordinaires :

— La VSSE peut, à l'étranger, avoir recours à des sources humaines (art. 18 L.R&S) conformément aux directives du Conseil National de Sécurité (CNS) et tel que prévu dans le Plan Stratégique National du Renseignement (PSNR)[43] ;
— La VSSE peut, à l'étranger, mener une observation au sens de l'article 16/1 §1 L.R&S, c'est-à-dire une observation, sans l'aide de moyen technique, « *dans les lieux accessibles au public et vise l'observation de personnes, d'objets ou d'événements* ».

(3) Via certaines méthodes particulières de renseignement

Outre les méthodes de renseignement ordinaires, il existe les méthodes particulières de renseignement ou méthodes de recueil de données (MRD).

[43] Il s'agit d'un plan approuvé par le Conseil National de Sécurité, élaboré conjointement par la VSSE et le SGRS et qui définit principalement la manière dont certaines priorités sont suivies par les deux services de renseignement.

A cet égard, il convient de mentionner une importante modification de loi en matière de mise en œuvre de MRD. À l'origine, les MRD étaient exclusivement autorisées « *sur le territoire du Royaume* ». En 2017, l'article 18/1, 1° L.R&S a été remplacé (Loi du 30 mars 2017, *M.B.* 28 avril 2017) et stipule à présent que les MRD peuvent désormais être mises en œuvre par la VSSE « *sur ou à partir du territoire du Royaume* ».

Depuis, le recueil d'information via une MRD peut avoir lieu à l'étranger, mais depuis la Belgique. Il est donc possible, par exemple, de pénétrer dans une boîte mail reliée à un serveur à l'étranger, mais seulement si les manipulations sont effectuées en Belgique. Un autre exemple classique est l'observation d'un véhicule au moyen d'une balise.[44] La balise devra être placée sur le véhicule en Belgique mais les informations collectées via cette balise pourront l'être en dehors des frontières nationales.

(4) Avec le concours du SGRS

Le SGRS étant doté de capacités juridiques, matérielles et humaines bien plus importantes pour la collecte à l'étranger, il peut être intéressant pour la VSSE de solliciter son concours.

La L.R&S prévoit ici une possibilité très spécifique : « *À la requête de la Sûreté de l'État, le Service Général du Renseignement et de la Sécurité prête son concours à celle-ci pour recueillir les renseignements lorsque des militaires sont impliqués dans les activités visées à l'article 7, 1° 1 et 3° /1* » (art. 9 L.R&S).

Une possibilité de coopération plus générale se présente lorsque la VSSE suit une menace qui relève également de la compétence du SGRS. On pourrait alors demander à ce dernier d'utiliser ses dispositifs et de partager avec la VSSE les informations obtenues. Cette forme de coopération a toutefois ses limites. En effet, l'intention de la VSSE ne peut être de contourner ses propres restrictions légales via le SGRS.

I.2.3. LES PRATIQUES DE COLLECTE DE RENSEIGNEMENTS À L'ÉTRANGER DE LA VSSE

Si cela n'a pas toujours été la position du service[45], le développement d'« *un réseau d'agents de [la] VSSE à l'étranger* » est désormais une ambition déclarée de la VSSE depuis l'adoption de sa 'Vision stratégique 2019-2020'.[46] Concrètement, les

---

44 Une balise est un équipement grâce auquel les mouvements du véhicule peuvent être suivis.

45 Dans les premières décennies qui ont suivi l'adoption de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S), la VSSE avait une vision restrictive de son rôle, considérant que celui-ci est strictement limité au territoire national. Cette vision, propre au service, reposait sur une interprétation restrictive de la loi.

46 *Vision stratégique 2019-2020 de la VSSE*, p. 7.

activités de collecte de renseignements à l'étranger de la VSSE prennent des formes multiples.

I.2.3.1. L'échange de données avec des partenaires étrangers

À l'heure actuelle, la VSSE obtient une grande partie des renseignements étrangers via sa coopération et l'échange d'informations avec des services partenaires étrangers. Ces relations peuvent aller de simples contacts protocolaires à une collaboration opérationnelle poussée.[47] Sur les quelque 120 services étrangers avec lesquels la VSSE a établi une relation bilatérale, une septantaine ont désigné des officiers de liaison auprès de la VSSE.[48]

I.2.3.2. Le déploiement de ses propres officiers de liaison

Dans sa note de mars 2021 intitulée "*VSSE internationale relaties 2021-2024. Visie – Context – Doelstellingen*"[49], la VSSE exprime sa volonté d'améliorer sa propre position d'information à l'étranger et de réduire sa dépendance à l'information provenant de services partenaires externes. La VSSE y défend l'idée que le déploiement de représentants permanents à l'étranger est une voie à poursuivre et qu'elle doit compléter l'échange d'informations avec les services partenaires étrangers. Selon la VSSE, en fonction des objectifs de ses services et de sa nature, opérationnelle ou stratégique, la représentation peut prendre deux formes :

— Une représentation dans les pays ayant un impact opérationnel significatif et direct sur les phénomènes en Belgique prioritaires pour la VSSE, et pour lesquels une présence permanente est jugée bénéfique d'un point de vue opérationnel ;
— Une représentation de type diplomatique où la présence permanente peut clairement représenter une valeur ajoutée aux relations institutionnalisées existantes et qui ne peut être obtenue d'une autre manière.

Comme indiqué dans l'enquête sur le suivi des recommandations de la Commission d'enquête Attentats, la VSSE ne compte actuellement que peu d'officiers de liaison.

Il y a, dans le chef de la VSSE, une intention de voir augmenter le nombre d'officiers de liaisons à l'avenir.

---

47 La manière dont les services de renseignement belges coopèrent au niveau bilatéral avec des services partenaires étrangers est définie dans une directive approuvée le 26 septembre 2016 par le Conseil National de Sécurité et intitulée « Directive relative aux relations de la Sûreté de l'État (VSSE) et du Service Général du Renseignement et de la Sécurité (SGRS) avec les services de renseignement étrangers » (traduction libre). Cette directive prévoit une évaluation de ces coopérations tous les deux ans.

48 Note de la VSSE intitulée « VSSE internationale relaties 2021-2024. Visie – Context – Doelstellingen » datant du 12 mars 2021.

49 'Relations internationales VSSE Vision – Contexte – Objectifs' (traduction libre).

Le document stratégique de la VSSE sur les relations internationales pour la période 2021-2024 indique que le déploiement des OL doit se faire dans un contexte de complémentarité et de synergies avec les partenaires nationaux, *in casu* le SGRS et la Police fédérale.

I.2.3.3. Le recours au réseau d'officiers de liaison de la Police fédérale à l'étranger

La VSSE a exprimé son intention de recourir au réseau assez étendu d'officiers de liaison de la Police fédérale à l'étranger. En septembre 2020, un accord de coopération a été conclu à cette fin entre la VSSE et la Police fédérale.

Dans le cadre de l'enquête de contrôle relative au suivi des recommandations formulées par la Commission d'enquête parlementaire Attentats, la VSSE avait été invitée à préciser la collaboration avec la Police fédérale à cet égard et avait indiqué : « *Concrètement, la VSSE rencontre régulièrement les officiers de liaison de la police fédérale et, à travers ses experts, échange des informations avec eux. La VSSE participe également chaque année à la 'semaine des officiers de liaison' organisée par la police fédérale* ».[50]

Le protocole d'accord indique que la collaboration entre la Police fédérale et la VSSE fera l'objet d'une évaluation au minimum annuelle. La dernière évaluation a eu lieu début avril 2022 et a conclu à la satisfaction des deux parties au protocole d'accord.[51]

I.2.3.4. Quant à la mise en œuvre de HUMINT à l'étranger

Comme le Comité, la VSSE juge conforme au cadre légal le recours aux sources humaines à l'étranger. La VSSE ajoute qu'il convient d'établir une distinction entre (1) une source déjà recrutée en Belgique qui voyage à l'étranger ou y séjourne et (2) l'approche, le recrutement et le traitement d'une source à l'étranger.

1.2.4. CONCLUSIONS

Le cadre juridique actuel offre à la VSSE des possibilités suffisantes pour répondre à ses besoins et ambitions potentiels en matière de (capacités de) renseignement à l'étranger si les circonstances l'exigent. Alors que dans le passé, le service défendait la position selon laquelle la L.R&S ne lui offrait pas de telles possibilités, il considère

50 Courrier de la VSSE du 3 août 2022 au Comité permanent R relatif aux recommandations de la commission d'enquête parlementaire Attentats – réactions VSSE.

51 *Ibidem.*

aujourd'hui, comme le Comité, que les méthodes ordinaires et certaines méthodes spéciales peuvent être utilisées à l'étranger.

I.3. LES CONSÉQUENCES DES RÉSEAUX DE SURVEILLANCE ÉTRANGERS POUR LES SERVICES DE RENSEIGNEMENT BELGES : LES AFFAIRES CRYPTO AG, RUBICON ET MAXIMATOR

En octobre 2022, le Comité permanent R a clôturé une enquête relative aux conséquences des réseaux de surveillance étrangers pour les services de renseignement belges composée de deux volets :

— le premier volet concernait l'opération de surveillance 'RUBICON' relative au dispositif de codage CRYPTO AG (I.3.1.) ;
— le deuxième volet concernait l'alliance secrète SIGINT MAXIMATOR (I.3.2.).[52]

Pour ces deux opérations de surveillance, le Comité s'est attaché à vérifier, d'une part, si les services de renseignement belges avaient connaissance de leur existence avant les révélations au grand public, et d'autre part, et dans quelle mesure les services de renseignement belges avaient été impactés par ces opérations.

I.3.1. CRYPTO AG – RUBICON

Au premier semestre de 2020, des révélations ont été publiées dans la presse sur le programme d'espionnage dénommé 'RUBICON'. Certains articles faisaient état de la prise d'intérêts, au début des années 60, des services de renseignement américains *Central Intelligence Agency* (CIA) et *National Security Agency* (NSA) ainsi que du service de renseignement allemand *Bundesnachrichtendienst* (BND) dans une société suisse, CRYPTO AG, qui fabriquait le matériel permettant d'établir des communications cryptées ou chiffrées.

Fort de leur contrôle de cette société dont ils sont devenus par la suite propriétaires exclusifs, les services de renseignement américains et le BND ont pu, des décennies durant, prendre connaissance de messages envoyés via le dispositif de codage CRYPTO. Il était question non seulement de communications entre puissances ennemies, mais également entre pays amis, voire entre pays alliés de l'OTAN. En 1993, l'Allemagne décida de se retirer du programme et laissa la société CRYPTO AG aux mains de la CIA, qui a été, au cours des 25 années suivantes, la seule propriétaire de la société.

[52] Ces enquêtes avaient été ouvertes en 2020.

De nombreux pays avaient connaissance, dans une plus ou moins grande mesure, de certains aspects dudit programme d'espionnage, essentiellement à partir des années 80, époque des premières interrogations sur les activités de la société CRYPTO AG.[53] Le Comité permanent R, par son enquête, a voulu déterminer si les services de renseignement belges avaient connaissance de cette opération, y ont pris part ou s'ils en ont été victimes.[54]

La VSSE a fait savoir que ce n'est que par les révélations dans la presse que le service a été informé des liens entre la société CRYPTO AG et les services de renseignement américains CIA et NSA et le service allemand BND. Quant au SGRS, dès les révélations dans la presse des écoutes RUBICON, le SGRS fit publier, le 12 février 2020, via Belga, un communiqué déclarant être au courant de l'affaire RUBICON et être en train d'examiner l'ampleur potentielle des mises sur écoute.

Le SGRS l'a également confirmé au journal De Tijd, affirmant que : « *Le SGRS met tout en œuvre pour s'en protéger (sont visées ici les mises sur écoute) et, surtout, met un point d'honneur à respecter le cadre légal en la matière, d'une part, et d'autre part, à appliquer un 'code' moral à ses partenaires, dans un monde où, sans être naïf, la confiance va souvent de pair avec la prudence dans le cadre de l'utilisation de matériel de cryptographie* » (traduction libre).[55]

Le Comité permanent R a interrogé les deux services de renseignement belges sur une éventuelle compromission interne à la suite de l'affaire RUBICON. Sur la base des informations classifiées fournies tant par la VSSE que par le SGRS, le Comité a conclu que la compromission des dispositifs utilisés par les services était « *minime* », et, pour la Défense, « e*xtrêmement minime* ».

I.3.2. MAXIMATOR

Dans le contexte du scandale de cryptage RUBICON, un universitaire néerlandais et expert en sécurité informatique, le Prof. Bart JACOBS, a publié en avril 2020

---

53 J. BAMFORD, 1982, *The Puzzle Palace, A Report on America's Most Secret Agency*.

54 Le Comité a mené, dans le passé, plusieurs enquêtes de contrôle sur d'autres types d'écoutes et interceptions. Voir notamment : COMITÉ PERMANENT R, *Rapport d'activités 1999*, pp. 23-47 ('Enquête sur la manière dont les services belges de renseignement réagissent face à l'éventualité d'un système américain "Echelon" d'interception des communications téléphoniques et fax en Belgique') ; *Rapport d'activités 2006*, pp. 39-48 ('L'affaire SWIFT') ; *Rapport d'activités 2014*, pp. 8-36 ('Les révélations d'Edward Snowden et la position d'information des services de renseignement belges') ; *Rapport d'activités* 2013, pp. 172-3 ('Le logiciel malveillant chez Belgacom').

55 "*De ADIV doet er alles aan om zich tegen hen (bedoeld wordt: afluisterpraktijken) te wapenen en maakt vooral een erezaak van om het wettelijk kader op dit gebied te respecteren en anderzijds een morele code te hanteren ten opzichte van zijn partners/bondgenoten in een wereld waar, zonder naïef te zijn, vertrouwen vaak met voorzichtigheid gepaard gaat*" (L. BOVE*De Tijd*, « België onderzoekt jarenlange spionage door CIA », 12 février 2020).

un article scientifique sur l'existence d'une alliance secrète SIGINT entre plusieurs pays européens, connue sous la dénomination 'MAXIMATOR'.[56]

L'article révèle qu'une collaboration SIGINT au niveau européen aurait été instaurée en 1976. Au départ, il s'agissait du Danemark, de la Suède et de l'Allemagne. Les Pays-Bas auraient rejoint l'alliance en 1978, tandis que la France l'aurait intégrée en 1985, et en aurait pris le lead à partir de 2006.[57,58] Le réseau MAXIMATOR se serait appuyé considérablement sur les informations fournies par le partenaire allemand, informations émanant du décryptage de communications CRYPTO AG.

Nonobstant le caractère particulièrement secret du programme, plusieurs autres pays européens auraient, après un certain temps, été informés de l'existence de cette structure de coopération. Quelques pays auraient même pris l'initiative de demander à pouvoir adhérer au réseau MAXIMATOR. La plupart aurait essuyé un refus, souvent en raison d'un manque d'expérience ou d'expertise en matière de cryptanalyse.

Dans son article, JACOBS indiquait que la Belgique avait été exclue de l'alliance – et consistait de la sorte à une exception notable de l'Europe du Nord-Ouest – en raison de son manque de capacité SIGINT. L'auteur précisait encore que : *"As a result, Belgium was not 'protected' by the Maximator members and bought (weakened) CRYPTO AG equipment, as also reported in the leaked BND and CIA documents, so that its (CRYPTO AG based) communication was readable by both Western five-member SIGINT alliances (Five-eyes and Maximator)."*[59]

Invités par le Comité à réagir face à ces affirmations, le deux services de renseignement belges ont indiqué qu'ils n'étaient pas au courant de l'existence de l'alliance MAXIMATOR avant la parution de l'article du Prof. Jacobs.

A la clôture de son enquête, le Comité permanent R estime fort probable que la Belgique ait fait l'objet d'activités d'interception de ses messages cryptés par le réseau MAXIMATOR.

---

56 "Maximator: European signals intelligence cooperation, from a Dutch perspective", *Intelligence and National Security*, Routledge, Volume 35, Number 5, August 2020, p. 659-668.

57 www.electrospaces.net/2020/05/maximator-and-other-european-sigint-alliance

58 J.J. QUISQUATER, « Cruel paradoxe de la cryptographie belge », 20 mai 2020, www.regional-it.be/detached/cruel-paradoxe-de- la-cryptographie-belge

59 « *Par conséquent, la Belgique n'était pas protégée par les activités de membres de MAXIMATOR et a fait l'acquisition du dispositif CRYPTO AG (version édulcorée et moins sécurisée), ce qui ressort également des documents du BND et de la CIA qui ont fuité. Ses communications qui transitaient par les dispositifs AG CRYPTO ont ainsi été écoutées tant par les FIVE EYES (NDLR : une alliance entre les services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des Etats-Unis) que par la structure de coopération MAXIMATOR* » (traduction libre).

I.4. SUIVI DE L'ENQUÊTE DE CONTRÔLE 'PRISM'

En 2013, le Comité permanent R a mené une enquête de contrôle sur l'attention que les services de renseignement belges accordaient aux menaces éventuelles pour le potentiel économique et scientifique (PES) belge émanant de programmes de surveillance électronique des systèmes de communication et d'information déployés à grande échelle par les services de renseignement étrangers.[60]

A la demande de la Commission de suivi, le Comité permanent R a examiné l'implémentation des onze recommandations formulées suite à son enquête de 2013.[61] Ces recommandations sont regroupées ci-dessous en cinq thématiques.

I.4.1. UN NÉCESSAIRE SUIVI DES TECHNOLOGIES ÉMERGENTES DE CAPTATION MASSIVE DES DONNÉES

Lors de son enquête initiale, le Comité permanent R appelait les deux services de renseignement à suivre de près les nouveaux moyens technologiques et les risques qu'ils comportent en matière de captation massive de données et d'espionnage économique et scientifique.

L'attention portée à ce phénomène est nécessaire, en ce qui concerne la VSSE et le SGRS, pour consolider leur position d'information quant aux moyens et *modus operandi* d'autres services. Cela permet non seulement d'en informer, le cas échéant, les autorités, ou de prendre des mesures de rétorsion, mais aussi d'évaluer leurs propres techniques de collecte.

Le Comité permanent R a constaté qu'aucune analyse du phénomène – destinée à identifier la menace que représentent les systèmes d'interception étrangers pour le PES et les infrastructures critiques de la Belgique – n'a été réalisée.

Le Comité relèvait que les deux services disent ne pas disposer des moyens suffisants pour traiter correctement cette problématique. Il insiste toutefois sur les nécessaires investissements dans la protection contre de telles pratiques massives de captation des données. A cet égard, le Comité salue la création du Cyber Command au sein de la Défense (sous l'égide du SGRS), officiellement opérationnel depuis octobre 2022 et chargé de la mise en œuvre de la stratégie de cyber sécurité.

---

60 Voir COMITÉ PERMANENT R, *Rapport d'activités 2016*, pp. 52-56 ('La protection du potentiel économique et scientifique et les révélations d'Edward Snowden').

61 Suite à la demande de la Commission de suivi de novembre 2019, le Comité permanent R a ouvert une enquête de contrôle en septembre 2020 et a transmis son rapport d'enquête à la Commission de suivi en octobre 2022.

I.4.2. LA COOPÉRATION ENTRE PARTENAIRES NATIONAUX

En 2013, plusieurs recommandations formulées par le Comité permanent R concernaient la coopération entre les services belges. Ainsi, le Comité appelait d'abord les deux services de renseignement à intensifier leur coopération. Il regrettait notamment que la VSSE et le SGRS n'aient pas mobilisés les mécanismes d'échanges d'informations prévus dans leur protocole de coopération signé en 2004 – par exemple, la mise en place de plateforme de collaboration *ad hoc*. Depuis 2013, aucune plateforme concernant la captation de données n'a été créée. Par contre, une plateforme de coordination est désormais dédiée à la préservation du PES, sous la présidence de la VSSE.

De l'avis du Comité permanent R, des moyens supplémentaires doivent être affectés – de façon permanente – à la protection du PES. Le Comité estimait également que la protection du PES pourrait faire l'objet d'un suivi au sein d'une plateforme commune aux deux services de renseignement, à l'instar de la plateforme CT dans le cadre de la lutte contre le terrorisme.

Plus spécifiquement formulée à l'encontre du SGRS, une recommandation du Comité permanent R portait en outre sur le compartimentage et la circulation des informations au sein du service. Au vu des constatations faites à l'occasion d'une enquête antérieure[62] et des réponses du SGRS, le Comité permanent R regrette les progrès insuffisants engrangés à cet égard, notamment en l'absence d'un système informatique intégral unique au sein du service.

Au-delà des seuls services de renseignement, le Comité appelait également à une plus large coopération interdépartementale en matière de *cybersecurity, ICT-security* et *cyberintelligence*. Le Comité permanent R constate que le Centre pour la cybersécurité Belgique (CCB) a été créé en octobre 2014. Si le CCB prend part depuis décembre 2020 aux discussions de la plateforme de coordination PES, il ne participe pas systématiquement aux réunions du Comité stratégique et du Comité de coordination du renseignement et de la sécurité, ni à celles du Conseil national de sécurité. Le CCB n'a pas non plus pour mission de détecter les cybermenaces, ni la responsabilité directe de protéger le PES.

Outre la création du CCB, la réforme de l'Autorité Nationale de Sécurité (ANS) et le Cyber Command de la Défense vont changer radicalement le paysage actuel du renseignement et de la sécurité.

---

62 COMITÉ PERMANENT R, *Rapport d'activités 2021*, pp. 36-49 ('Enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings').

I.4.3. UN ENDOSSEMENT POLITIQUE

Au niveau international, le Comité recommandait au SGRS et à la VSSE de « *prendre chaque menace au sérieux, même si elle provient de services amis ou de services de pays amis* ». Le Comité recommandait en outre que les conditions de coopération avec les partenaires étrangers soient inscrites dans des directives et soumises au contrôle politique. Une autre recommandation visait plus précisément les accords de coopération bi- ou multilatéraux à faire endosser par les responsables politiques.[63]

A cet égard, il convient de mentionner la « *Directive concernant les relations des services de renseignement belges avec les services de renseignement étrangers* » édictée le 26 septembre 2016 par le Conseil national de sécurité (CNS). Le document vise à objectiver le choix des partenaires internationaux du SGRS et de la VSSE, en vue de déterminer la mesure et la nature de la collaboration avec ces partenaires et d'évaluer cette collaboration sur une base régulière. La directive fournit également des orientations concernant le partage de données à caractère personnel à des services étrangers. Cette directive ne précise toutefois pas clairement si la VSSE et le SGRS doivent obtenir une autorisation ministérielle (ou d'une autre instance) préalable. Aux yeux du Comité permanent R, une telle autorisation semble essentielle.[64]

Depuis l'enquête du Comité permanent R sur le *Memorandum of Understanding* entre le SGRS et un service de renseignement rwandais en 2020, les services sont en outre tenus de procéder, tous les deux ans, à des évaluations conjointes de leurs partenaires stratégiques communs. À cette occasion, le Comité permanent R a également recommandé que les accords bilatéraux entre les services et leurs partenaires stratégiques soient approuvés ou couverts par le ministre compétent.

Le Comité permanent R estime que la menace que représente l'utilisation de systèmes de captation massive par un partenaire stratégique doit être incluse dans l'évaluation que le service de renseignement fait de sa relation avec un service partenaire « ami ».

Plus largement, le Comité recommandait en 2013 que le Comité ministériel du renseignement et de la sécurité – devenu Conseil national de sécurité – définisse une orientation politique à suivre par les services de renseignement.

Pour autant que le Comité permanent R ait pu le vérifier, le Conseil national de sécurité n'a pas, après l'enquête de 2013, accordé d'attention spécifique au phénomène de la captation massive de données. Le Comité estime qu'il appartient

---

63 Cette recommandation sera réitérée dans le cadre d'une enquête ultérieure en 2017. Voy. COMITÉ PERMANENT R, *Rapport d'activités 2017*, 107 ('XII. Couverture politique des accords de coopération.')

64 Voir en ce sens : Proposition de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en vue d'instaurer des notes d'évaluation pour la collaboration avec les services de renseignement et de sécurité étrangers, *Doc. parl.* Chambre 2019-20, nº 55- 956/001 (23 janvier 2020).

au CNS de définir la politique générale en matière de renseignement et les priorités qui en découlent. Cependant, le Comité permanent R attend toujours du CNS une implication plus active en la matière.

I.4.4. DES PRÉCISIONS LÉGISLATIVES

En 2013, le Comité permanent R appelait à différentes précisions législatives quant aux méthodes de recueil de données des services. Tout d'abord, le Comité recommandait de préciser le champ d'application territorial des méthodes particulières de recueil de données (MRD) étant donné les évolutions technologiques.

En 2017, la Loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal[65] (ci-après la loi d'actualisation MRD) a apporté d'importantes modifications au champ d'application territorial des MRD, y compris l'interception de (télé)communications (art. 18/17 L.R&S) et l'intrusion dans des systèmes informatiques (art. 18/16 L.R&S).

Avant la modification législative précitée, une méthode MRD ne pouvait être mise en œuvre par la VSSE que « *sur le territoire du Royaume* ». La loi stipule désormais que le service de renseignement exerce les méthodes MRD *« sur ou à partir du territoire du Royaume »* (*cf.* art. 18/1, 1° L.R&S). L'exposé des motifs[66] de la loi d'actualisation MRD précise à cet égard que la VSSE doit mettre en œuvre les MRD « *sur* » le territoire belge, ce qui signifie que les agents de la VSSE ne peuvent pas se rendre à l'étranger pour, par exemple, inspecter une habitation, installer un micro ou une caméra, voire encore scanner un téléphone. La collecte d'informations elle-même peut en revanche se dérouler à l'étranger.[67]

En ce qui concerne le SGRS, le législateur a encore franchi une étape supplémentaire pour le SGRS en ne liant plus aucune restriction territoriale à l'exercice des MRD (art. 18/1, 2° L.R&S). L'exposé des motifs[68] de la loi d'actualisation MRD précise que cette modification se justifie par le fait que la majorité des missions du SGRS sont exécutées à l'étranger, comme par exemple la protection des missions des Forces armées ou des ressortissants belges à l'étranger. Il est également indiqué que, dans le cadre des opérations avec mandat donné par le Conseil de Sécurité des Nations unies, il est souvent attendu des services de renseignement de la coalition qu'ils mènent des enquêtes de renseignement nécessitant le recours à des méthodes spécifiques et exceptionnelles et que la limitation du champ d'application territorial

---

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

66 EdM, *Doc. parl.* Chambre 2015-16, nº 54-2043/001, 46-47.

67 Par exemple, l'intrusion informatique exécutée à partir de la Belgique mais sur un réseau qui dépasse les frontières, ou si une cible mise sur écoute reçoit un appel de l'étranger.

68 EdM, *Doc. parl.* Chambre 2015-16, nº 54-2043/001, 47-50.

empêche le SGRS de remplir adéquatement sa part de travail dans le cadre de la coopération internationale.[69]

Toutefois, il convient de noter que l'exposé des motifs précise que la mise en œuvre de méthodes spécifiques et exceptionnelles lors d'opérations à l'étranger n'est pas toujours praticable.[70]

De l'avis du Comité permanent R, la loi d'actualisation MRD apporte une clarification bienvenue de l'application territoriale des MRD. Étonnamment, le Comité a toutefois constaté à la suite du contrôle qu'il a mené sur les MRD que le SGRS n'avait, en octobre 2022, jamais déployé de méthode MRD à l'étranger.

Une seconde recommandation portait ensuite sur la réglementation INT belge, qui autorise le SGRS à intercepter des communications à l'étranger (ou *Signals Intelligence*, SIGINT). Etant donné l'évolution des technologies, le Comité suggérait une réexamination de cette réglementation par le législateur.[71]

A cet égard, la loi d'actualisation MRD de 2017 apporte une série de modifications dans cette matière, par exemple :

— Les possibilités d'interception du SGRS ne concernent plus seulement les communications « émises à l'étranger » mais sont étendues aux communications « reçues à l'étranger ». Le SGRS a ainsi acquis la compétence d'intercepter toute forme de communication à l'étranger, indépendamment de la personne à l'origine de l'appel et de l'endroit où se trouve la personne à l'origine de l'appel, pour autant qu'une partie de la communication se déroule à l'étranger.
— Une obligation légale de coopérer a été créée dans le cadre de la mise en œuvre de la compétence d'interception dans le chef des opérateurs et fournisseurs de télécommunications. Le *cable taping*, qui faisait déjà partie des possibilités légales du SGRS depuis 2003, gagne ainsi en praticabilité.
— La réglementation SIGINT, à savoir l'interception de communications étrangères (*cf.* art. 44 L.R&S), a été élargie à une réglementation CYBER, à savoir l'intrusion dans des systèmes informatiques étrangers (*cf.* art. 44/1 L.R&S) et une réglementation pour l'enregistrement d'images à l'étranger (*cf.* art. 44/2 L.R&S).[72]
— En outre, la mission de renseignement du SGRS a été élargie en soutien aux opérations militaires. Le service se doit désormais également : « *de rechercher,*

---

69 EdM, *Doc. parl.* Chambre 2015-16, nº 54-2043/001, 6.

70 EdM, *Doc. parl.* Chambre 2015-16, nº 54-2043/001, 7, 84 et 86.

71 « *Des éléments qui doivent en tous points être examinés lors d'une telle révision, sont dans quelle mesure les interceptions doivent ou non être ciblées, la portée exacte de la possibilité de 'rechercher' des signaux, le degré de précision du Plan d'écoutes annuel, la possibilité de procéder à du datamining dans des informations en vrac et la question de savoir si les opérations SIGINT internationales doivent entrer dans le cadre d'un 'mandat international' plus large* ». Cette compétence SIGINT avait déjà été élargie en 2003 à toutes les communications émises à l'étranger (et non plus les seules communications militaires) : EdM, *Doc. parl.* Chambre 2002-2003, nº 50-2059/001, 4-6.

72 Précisons que le SGRS peut mettre en œuvre ces compétences SIGINT, CYBER et de prise d'images dans toutes les missions légales de renseignement et de sécurité du service de renseignement, à l'exception de la réalisation d'enquêtes de sécurité et de vérifications de sécurité.

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 [...] et d'en informer sans délai les ministres compétents » (cf. art. 11, §1, 1° *in limine* L.R&S). Cette extension du champ d'application crée également logiquement un champ d'application plus large pour la compétence d'interception visée à l'article 44 L.R&S.

— Le contrôle a été renforcé notamment par une motivation plus élaborée de la liste annuelle et par la transmission mensuelle au Comité d'une liste motivée de pays ou d'organisations et institutions qui ont fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images.

I.4.5. UN RESPECT STRICT DE L'ARTICLE 33 L.CONTRÔLE

Enfin, dans une dernière recommandation, le Comité permanent R insistait « *sur l'obligation reprise à l'article 33 L.Contrôle de transmettre 'd'initiative au Comité permanent R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services'* ». Cette obligation vaut également pour les conventions, MoU ou accords conclus au niveau international.

Répétée à plusieurs reprises[73], cette recommandation reste d'actualité. En effet, la transmission de directives, de SOP et d'autres documents internes n'est toujours pas automatique ni systématique. Le respect de l'article 33 de la L.Contrôle demeure un point d'amélioration, en particulier pour le SGRS.

I.5. ENQUÊTE DE CONTRÔLE À LA SUITE DES RÉVÉLATIONS SUR L'UTILISATION DU LOGICIEL PEGASUS

Le 18 juillet 2021, dix-sept médias internationaux, dont *Le Soir* et *Knack* en Belgique, révélaient l'existence du logiciel Pegasus, vendu par une société israélienne, NSO Group, à des gouvernements et à leurs services de renseignement et/ou de sécurité pour leur permettre d'administrer des smartphones à l'insu de leur propriétaire.

---

73 Voir notamment COMITÉ PERMANENT R, *Rapport d'activités 1996*, 28-32 (Rapport sur l'application par les services de renseignements de l'article 33 alinéa 2 L.Contrôle) ; *Rapport d'activités 2001,* 218-220 (Les informations indispensables dont le Comité permanent R estime devoir disposer afin d'accomplir sa mission efficacement) ; *Rapport d'activités 2002,* 27 (La transmission d'initiative par les services de renseignement de certains documents au Comité permanent R) ; *Rapport d'activités 2006,* 12 ; *Rapport d'activités 2013*, 116 ; *Rapport d'activités 2014*, 120.

Le consortium de journalistes révélait avoir eu accès à plus de 50.000 numéros de téléphone qui auraient été pris pour cibles par des clients utilisateurs du logiciel Pegasus. *Le Soir* faisait état du fait que parmi les 50.000 numéros de téléphone figuraient plusieurs numéros belges mais aussi que, selon trois sources, « *la Belgique figurerait parmi les clients de NSO* ».[74]

Le Comité permanent R a pris la décision d'ouvrir une enquête qui se composait de deux volets.[75] Il s'agissait, d'abord, de vérifier si les services de renseignement belges utilisent/ont utilisé le logiciel Pegasus (ou équivalent) dans le cadre de leurs missions, et si cette utilisation est conforme au cadre légal en vigueur. Ensuite, face à l'utilisation du logiciel Pegasus par des services étrangers (services de renseignement et/ou de sécurité, entreprises privées, etc.) contre des personnes physiques et/ou morales belges, l'enquête visait à déterminer si les services de renseignement belges sont outillés pour identifier et gérer, voire contrer, cette menace. Afin de couvrir ces deux volets, cinq questions ont été discutées.

I.5.1. LE CADRE LÉGAL EN BELGIQUE PERMET-IL AUX SERVICES DE RENSEIGNEMENT BELGES D'UTILISER UN LOGICIEL DE TYPE PEGASUS ?

Le législateur belge a érigé en principe général l'interdiction des écoutes, des prises de connaissance et des enregistrements des communications et des communications électroniques privées pendant leur transmission et à l'aide d'un appareil quelconque. Ces interdictions, qui concernent des atteintes graves à la vie privée, sont érigées en infractions sanctionnées par des peines correctionnelles d'amende et d'emprisonnement en vertu des articles 259*bis* et 314*bis* du Code pénal.

Toutefois, le législateur belge a été amené à encadrer le recours à titre exceptionnel à une atteinte à la protection des communications électroniques privées face à certaines menaces. Le législateur a en effet cherché à concilier des intérêts *a priori* contraires, soit, d'une part, le respect de la vie privée des personnes et, d'autre part, la nécessité d'une protection plus efficace de la société contre des

---

74 *Le Soir*, 18 juillet 2021, ('Projet Pegasus : un logiciel de cyberespionnage quasiment indétectable'). Ni la Sûreté de l'État (VSSE), ni le Service Général du Renseignement et de la Sécurité (SGRS), ni la Police fédérale n'ont souhaité réagir auprès des médias, évoquant une information « confidentielle ».

75 Le rapport de l'enquête de contrôle, ouverte en juillet 2021, a été transmis à la Commission de suivi en octobre 2022. Il convient de relever la publication, depuis la clôture de l'enquête du Comité permanent R, du « Projet de rapport relatif à l'enquête sur les allégations d'infraction et de mauvaise administration dans l'application du droit de l'Union lors de l'utilisation de Pegasus et de logiciels espions de surveillance équivalent » de la Commission d'enquête chargée d'enquêter sur l'utilisation de Pegasus et de logiciels espions de surveillance équivalents du Parlement européen (2022/2077(INI), 28 novembre 2022, https://www.europarl.europa.eu/doceo/document/PEGA-PR-738492_FR.pdf).

menaces telles que le terrorisme ou encore la criminalité grave et organisée. En effet, il s'imposait au regard des articles 12 et 22 de la Constitution ainsi que de l'article 8 de la Convention européenne des droits de l'homme, de déterminer de manière claire et précise les compétences qui pouvaient être mobilisées par les services de renseignement lorsqu'ils s'immiscent dans l'exercice des droits et libertés individuels. L'objectif recherché était de permettre, dans certaines conditions et dans le cadre d'un strict contrôle juridictionnel, d'intercepter, de prendre connaissance, d'explorer et d'enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou d'étendre la recherche dans un système informatique ou une partie de celui-ci. Ces règles ont été intégrées dans le code de procédure pénale et dans la L.R&S.

La L.R&S prévoit ainsi l'ensemble des méthodes qui peuvent être mises en œuvre par les services de renseignement, moyennant, pour les méthodes les plus intrusives, un contrôle juridictionnel *a priori* et *a posteriori*.[76] Toute technique particulière qui ne serait pas expressément autorisée par la loi serait, par voie de conséquence, interdite.

Plus précisément, l'article 18/16 de ladite loi autorise l'intrusion dans un système informatique et la collecte de données. Les interceptions, prises de connaissance et enregistrement des communications sont, quant à elles, encadrées par l'article 18/17 L.R&S. Il s'agit de méthodes dites « exceptionnelles » dont la mise en œuvre nécessite impérativement une décision motivée du dirigeant de service concerné et ce, sous peine de nullité.[77]

Il faut relever que si la législation sur les services de renseignement encadre le principe de telles méthodes intrusives, elle ne traite nullement des 'techniques' de mise en œuvre. Ces questions dites techniques – entre autres, avec quels matériels et logiciels les méthodes sont mises en œuvre – sont laissées à l'appréciation des services, tenant compte des évolutions permanentes des technologies.

Le cadre légal actuel autorise donc les services de renseignement belges à faire usage d'un logiciel de type Pegasus dans le cadre de la mise en œuvre de MRD moyennant le strict respect des principes de légalité, proportionnalité et subsidiarité. Un contrôle juridictionnel strict est exercé afin que l'utilisation de chaque MRD réponde aux exigences de légalité, de proportionnalité et de subsidiarité.

Par ailleurs, dans l'état actuel du droit, rien n'empêcherait le SGRS d'utiliser un logiciel de type Pegasus dans le cadre de l'exercice de ses compétences prévues à l'article 44 L.R&S. Cet article prévoit la possibilité pour le SGRS de capter des communications émises ou reçues à l'étranger, de les intercepter, les écouter et les enregistrer. Un contrôle est également exercé sur le recours à ce type de procédés

---

76 L'article 18/3 L.R&S prévoit un double contrôle dans la mise en œuvre de ces méthodes de recueil de données (MRD) au niveau de la légalité, de la subsidiarité et de la proportionnalité : un contrôle *a priori* par la Commission administrative BIM et un contrôle *a posteriori* par le Comité permanent R.

77 Article 18/10 § 2 L.R&S.

mais il diffère du contrôle pour les MRD. En effet, ici seul le Comité permanent R intervient et exerce un contrôle préalable, un contrôle concomitant et un contrôle *a posteriori* conformément à l'article 44/3 L.R&S.

Le Comité souhaitait néanmoins attirer l'attention sur le fait qu'à l'heure actuelle, le contrôle juridictionnel exercé ne porte pas sur les aspects techniques de mise en œuvre des méthodes de recueil de données (notamment la question de savoir si un logiciel de type Pegasus est utilisé pour mettre en œuvre la MRD autorisée) ou de l'article 44 L.R&S. Le Comité ne dispose, à l'heure actuelle, ni des ressources humaines suffisantes ni des compétences techniques requises pour exercer un tel contrôle. Ce manque de moyens peut avoir une influence sur l'appréciation du caractère subsidiaire et proportionnel de la MRD ou procédé visé à l'article 44 L.R&S.

I.5.2. LES SERVICES DE RENSEIGNEMENT BELGES UTILISENT-ILS LES *REMOTE INFECTION TECHNOLOGIES* DANS LE CADRE DE LEURS MISSIONS LÉGALES ?

Le Comité a examiné la question de savoir si les services de renseignement ont utilisé/utilisent Pegasus ou des outils similaires. L'analyse du Comité n'a pas été partagée dans le rapport d'enquête public en raison de la classification des informations mobilisées.

À la question de savoir s'il est nécessaire pour les services de renseignement belges de disposer de ce type d'outils, le Comité permanent R conclut que face à l'évolution rapide et complexe des menaces dans un environnement digital lui-même en expansion, l'utilisation des technologies digitales les plus à la pointe apparaît essentielle pour assurer le meilleur niveau d'efficacité des missions des services de renseignement et de sécurité belges. Il est incontestable que le recours à des outils technologiques de renseignement et de sécurité comme les *Remote Infection Technologies* est de nature à renforcer significativement la position d'information des services. Cependant, il est important que le recours à ce type de technologie s'opère dans le strict respect du cadre légal.

Le Comité permanent R insiste également sur le fait que ces technologies devraient idéalement être développées en Belgique. À défaut, les technologies utilisées devraient être celles développées par des partenaires étrangers stratégiques avec lesquels un accord de sécurité a été signé et être acquises après une analyse de risques formalisée, approfondie et standardisée.

Par ailleurs, le Comité estime que le contrôle à exercer dans le cadre de l'usage de ce type de logiciel doit être 'plus approfondi' en raison de la gravité de l'intrusion dans la vie privée.

I.5.3. LE SGRS ET LA VSSE SONT-ILS COMPÉTENTS POUR DÉTECTER L'UTILISATION PAR DES PUISSANCES ÉTRANGÈRES DE CE TYPE DE LOGICIEL CONTRE DES BELGES ET EN ONT-ILS LA CAPACITÉ ?

Les révélations médiatiques ont montré qu'il existe un risque pour les droits et la vie privée du citoyen belge susceptible d'être la cible d'un espionnage par des services de renseignement *étrangers* via des technologies de type Pegasus. La détection et la gestion de ce type de menace incombe à la VSSE et au SGRS.

En vertu des articles 7 et 8 L.R&S, la VSSE a en effet pour mission de rechercher, d'analyser et de traiter le renseignement relatif à toute activité pouvant menacer la sûreté intérieure et extérieure de l'État ainsi que le potentiel scientifique ou économique de la Belgique, dont l'espionnage. En outre, l'article 7, 3°/1 donne à la VSSE pour mission spécifique de « *rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge* ».

L'article 11 § 1er, 5° prévoit la même mission pour le SGRS. Ce service est également chargé, en vertu de l'article 11 § 1er, 1°, « *de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer : (…) e) la sécurité des ressortissants belges à l'étranger* ».

Le Comité permanent R a constaté que les services de renseignement ont pris certaines initiatives, tant sur le volet de la détection que sur le volet de la prévention pour limiter les infections des téléphones.

Dans son rapport public, le Comité permanent R n'a pas pu donner davantage d'informations en raison de la classification des informations mis à sa disposition.

I.5.4. LES SERVICES DE RENSEIGNEMENT BELGES ONT-ILS LA CAPACITÉ DE SUIVRE LES ÉVOLUTIONS RELATIVES AUX *REMOTE INFECTION TECHNOLOGIES* ?

En ce qui concerne le suivi des évolutions en la matière, le Comité permanent R a estimé que les deux services de renseignement doivent être plus attentifs aux menaces que les nouvelles possibilités technologiques peuvent représenter en termes de captation de données et d'espionnage économique et politique, même si ces risques émanent de pays avec lesquels ils entretiennent des relations stratégiques. À cet égard, des analyses de risques devraient être effectuées régulièrement en portant une attention renforcée à l'impact de la présence de nombreuses institutions internationales sur le territoire belge.

I.5.5. QUELLE EST LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT BELGES RELATIVE AUX ÉVENTUELLES CIBLES BELGES DU LOGICIEL PEGASUS (PAR DES SERVICES DE RENSEIGNEMENT ÉTRANGERS) ?

Le Comité permanent R a constaté que lors de l'identification d'éventuelles cibles belges de services étrangers en lien avec l'utilisation de Pegasus, le SGRS s'est uniquement concentré sur l'éventuelle implication des services de renseignement rwandais, et la VSSE sur les services de renseignement rwandais et marocains.

Selon des informations consultables dans des sources ouvertes, un lien a également été établi entre les services de renseignement saoudiens et émiratis et l'utilisation de Pegasus ainsi que l'espionnage d'activistes des droits humains et de journalistes occidentaux (notamment américains et britanniques). Mais à la rédaction du rapport final par le Comité permanent R, aucun nom de cible belge n'avait été cité à cet égard.

Les autres informations mobilisées par le Comité dans son rapport original et relatives aux éventuelles cibles belges demeurent classifiées.

I.6. LE SUIVI PAR LES SERVICES DE RENSEIGNEMENT DES ORGANISATIONS PHILOSOPHIQUES À VISÉES POLITIQUES CONTRAIRES À L'ORDRE DÉMOCRATIQUE

En juillet 2021, la Présidente de la Chambre des Représentants chargeait le Comité permanent R d'ouvrir une enquête de contrôle portant sur la manière dont les services de renseignement et de sécurité s'intéressent « *aux activités des mouvements sectaires à obédience religieuse ayant des visées politiques (autres mouvements salafistes, Opus Dei, Civitas,...)* ».

Cette nouvelle enquête constituait le troisième volet d'une série d'enquêtes commanditées par la Commission de suivi du Comité permanent R après celles sur la manière dont la Sûreté de l'Etat avait assuré le suivi de la commissaire du gouvernement Ihsane Haouach[78] et sur le suivi par les services de renseignement de la mouvance des Frères Musulmans.[79]

Très rapidement, il est apparu nécessaire de préciser et de réorienter l'objet de la recherche. Notamment, la notion de « *secte* » semblait inadéquate, les

---

78 Pour rappel, cette enquête, s'intéressait à la nature du suivi réalisé par la VSSE concernant cette personne présumée entretenir (délibérément ou à son insu) des liens avec la mouvance des Frères musulmans, dans : COMITÉ PERMANENT R, *Rapport d'activités 2021*, 75 e.s.

79 Cette enquête visait à déterminer si la mouvance des Frères musulmans faisait l'objet d'un suivi par la VSSE et le SGRS, d'une part, et si, elle était constitutive, selon ceux-ci, d'une menace en Belgique, d'autre part, dans : COMITÉ PERMANENT R, *Rapport d'activités 2021*, 79 e.s.

mouvements cités à titre exemplatif dans la demande de la Commission n'étant pas des sectes en tant que tels.[80] Aussi, le Comité ne souhaitait pas se limiter à l'étude des mouvements cités mais préférait mener une enquête de contrôle sur les organisations philosophiques, confessionnelles et non confessionnelles, au sens large, ayant des visées politiques contraires à l'ordre démocratique. Enfin, pour rattacher l'objet de la recherche à une menace spécifique, et s'inscrire ainsi dans le prolongement des deux précédents volets, le Comité proposait de s'intéresser à la menace d'ingérence (potentielle), initiée ou non à l'étranger, que peuvent représenter ces organisations.

Avec l'accord de la Présidente de la Chambre, la portée de l'enquête a été redéfinie pour examiner le suivi des organisations philosophiques à visées politiques contraires à l'ordre démocratique. La question des capacités et stratégies mises en place par les services de renseignement et de sécurité pour détecter et suivre ce type d'organisations paraissait être particulièrement intéressante aux yeux du Comité.

I.6.1. LE CADRE LÉGAL

La Loi organique des services de renseignement et de sécurité (L.R&S), en ses articles 7 et 8, définit les missions légales attribuées à la VSSE. Parmi les menaces que doit suivre le service de renseignement civil, l'article 8 définit les organisations sectaires nuisibles et les organisations criminelles comme suit :

- l'organisation sectaire nuisible [81, 82] : « *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* » ;
- l'organisation criminelle : « *toute association structurée de plus de deux personnes, établie dans le temps, en vue de commettre de façon concertée des*

---

80 Le Comité s'était déjà penché sur le suivi des menaces constituées par les organisations sectaires nuisibles et les organisations criminelles : COMITÉ PERMANENT R, *Rapport d'activités 2021*, 35 e.s.

81 Cette définition est textuellement reprise de l'article 2 de la Loi du 2 juin 1998 (*M.B.* 25 novembre 1998) portant création d'un Centre d'information et d'avis sur les organisations sectaires nuisibles et d'une Cellule administrative de coordination de la lutte contre les organisations sectaires nuisibles.

82 Le caractère nuisible d'une organisation sectaire est examiné sur base des principes contenus dans la Constitution, les lois, décrets et ordonnances et les conventions internationales de sauvegarde des droits de l'homme ratifiées par la Belgique. En 2021, le Comité permanent R rappelait déjà « *qu'en général, aucun autre service de renseignement étranger n'a pour mission officielle de surveiller les sectes nuisibles. Cette mission spécifique de la Sûreté de l'Etat belge constitue donc une exception dans le monde des services de renseignement. La plupart des pays démocratiques refusent même d'impliquer ces services dans la surveillance des mouvements religieux. Parce que cette mesure pourrait être considérée comme une atteinte à la liberté religieuse* » (COMITÉ PERMANENT R, *Rapport d'activités 2021*, 22).

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 à l'article 8, 1°, a) à e) et g), ou qui peuvent avoir des conséquences déstabilisantes sur le plan politique ou socio-économique ».

Précisons que toutes les organisations sectaires nuisibles et toutes les organisations criminelles ne font pas partie de la sphère d'intérêt légale de la VSSE. La L.R&S prévoit que ces organisations ne relèvent de la compétence de la VSSE que si leurs activités peuvent représenter une menace pour la sécurité intérieure ou extérieure de l'Ètat et/ou pour le potentiel économique ou scientifique du pays.

En ce qui concerne le SGRS, l'article 11, §1er, 1° L.R&S indique qu'il a, entre autres, pour missions 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. Les compétences du SGRS en la matière sont donc limitées et impliquent qu'il y ait un lien avec la Défense ou les intérêts militaires.

Outre la L.R&S, il convient de mentionner l'article 9 de la Convention européenne des droits de l'homme (CEDH) qui garantit la liberté de pensée, de conscience et de religion, considérée comme « *l'une des assises de la société démocratique ; d'une façon particulière, les juges voient dans la liberté religieuse un élément vital contribuant à former l'identité des croyants et leur conception de vie* ».[83] Cette liberté bénéficie d'une protection rigoureuse.[84]

[83] Division de la Recherche, Cour européenne des droits de l'homme, « Aperçu de la jurisprudence de la Cour en matière de liberté de religion », octobre 2013, p. 27.

[84] Les organes de la Convention n'ont pas compétence pour définir la religion mais celle-ci doit être envisagée dans un sens non restrictif. Quant aux religions minoritaires et aux groupements religieux qualifiés parfois de *sectes* au niveau national, il ressort de la jurisprudence de la Cour que tous les groupements bénéficient d'une égale garantie au regard de la Convention. Considérant le droit à la liberté de religion comme « *pilier d'une société démocratique* », la Cour n'a eu de cesse de rappeler aux Etats leur obligation de neutralité et d'impartialité dans l'exercice de leurs pouvoirs de réglementation en la matière et dans leurs relations avec les diverses religions, cultes et croyances.

I.6.2. L'ÉTAT DU SUIVI DE LA PROBLÉMATIQUE PAR LA VSSE ET LE SGRS

I.6.2.1. Quant à la VSSE

La VSSE confirme d'emblée qu'elle ne suit des « *organisations philosophiques (confessionnelles ou non-confessionnelles) ayant des visées politiques contraires à l'ordre démocratique* » que dans le cadre strict d'une menace.

Elle indique toutefois que, davantage que l'ingérence, ce sont les menaces d'extrémisme et de terrorisme qui sont, à ses yeux, déterminantes lors du suivi des groupes idéologiques ou religieux considérés comme problématiques. Ainsi, selon la VSSE, les principales menaces justifiant le suivi d'une telle organisation philosophique sont celles de l'extrémisme (article 8, al. 1, c L.R&S) et du terrorisme (article 8, al. 1, b) L.R&S).

Au sein de la VSSE, la diffusion de discours extrémistes violents et le risque de passage à l'acte violent sont les deux principaux critères qui guident la détection et justifient le suivi d'une organisation extrémiste. À cela s'ajoutent d'autres critères tels que la présence en Belgique, le lien (par exemple, financier) avec une organisation ou un Ètat étranger(e).

La VSSE organise son travail autour de la distinction entre trois principaux types d'extrémisme, à savoir l'extrémisme religieux, l'extrémisme idéologique et l'extrémisme exogène.

L'extrémisme religieux

Au moment de l'enquête, la VSSE disait travailler prioritairement sur des mouvements extrémistes islamistes. Car, même si ceux-ci sont marginaux au sein de l'« *islam belge* », la VSSE considère qu'ils constituent la principale menace en matière d'extrémisme quant au discours qu'ils propagent et l'audience qu'ils retiennent.

La VSSE se concentre en particulier sur le suivi du salafisme. Cette mouvance conservatrice et rigoriste demeure, selon la VSSE, le mouvement le plus dynamique et le plus populaire de la « *nébuleuse islamiste* ». Outre le suivi du salafisme sur le territoire belge, la VSSE travaille à diminuer l'influence qu'ont certains pays du Golfe sur le développement du salafisme en Belgique et en Europe, notamment via un simple soutien financier voire le financement global de divers groupements.

C'est ainsi que la VSSE suit également attentivement la mouvance des Frères musulmans en ses composantes belges et européennes.[85]

---

[85] Voir COMITÉ PERMANENT R, *Rapport d'activités 2021*, 61-66 ('I.12. Une attention renouvelée pour les Frères Musulmans').

Pour l'heure, la VSSE indique ne pas travailler sur des organisations liées à d'autres cultes car, à ce stade et selon l'évaluation de la VSSE, aucunes autres organisations liées à d'autres cultes ne représentent une menace suffisamment importante.

L'extrémisme idéologique

Dans le cadre de l'extrémisme idéologique, la VSSE indiquait s'occuper, prioritairement, des personnes et groupements d'extrême droite inspirés du nazisme ou de l'ultranationalisme.

Par ailleurs, et dans le même ordre d'idée, ces dernières années, la VSSE a encore constaté, comme d'autres partenaires belges ou étrangers, une recrudescence de l'activisme anti-islam et anti-immigration ainsi que l'émergence sur le territoire belge de groupements dits « *identitaires* ».

Quant à l'extrême gauche, la menace représentée par les individus et groupements de cette mouvance extrémiste existe également mais elle reste actuellement plus limitée. Dans le cadre de ce suivi spécifique, la VSSE se focalise sur l'extrême gauche violente hostile à l'ordre démocratique et constitutionnel.

Selon la VSSE, trois tendances principales se dessinent, à savoir l'anarchisme insurrectionnel, l'activisme libertaire et le communisme révolutionnaire ; la VSSE signalant encore que les attaques extrémistes de gauche visent plutôt des biens ou des infrastructures que des personnes.

L'extrémisme exogène

Enfin, la VSSE suit des personnes et des groupes extrémistes exogènes actifs depuis la Belgique. Il s'agit de mouvements extrémistes étrangers, parfois considérés comme terroristes, dont les cibles et les objectifs principaux se trouvent dans leur pays d'origine.

Dans ce cadre, la Belgique en général et Bruxelles en particulier sont des lieux particulièrement privilégiés pour asseoir un intense « *lobbying* » voire l'ingérence de ces mouvements étant donné la présence de nombreuses institutions européennes et internationales sur le territoire national. A cet égard, la VSSE ajoute qu'il est souvent complexe d'appréhender une menace d'ingérence car il est difficile de faire la différence entre ingérence et activités d'influence ou de lobbying légales.

I.6.2.2. Quant au SGRS

Dans cette matière, les compétences du SGRS sont limitées et exigent un lien avec la Défense ou les intérêts militaires. En 2022, le service indiquait ne suivre aucune organisation philosophique.[86]

I.7. LE SUIVI DES RECOMMANDATIONS FORMULÉES PAR LA COMMISSION D'ENQUÊTE PARLEMENTAIRE ATTENTATS TERRORISTES CONCERNANT LES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ [87]

I.7.1. CONTEXTUALISATION

I.7.1.1. Recommandations de la Commission d'enquête parlementaire Attentats terroristes[88]

Le 22 mars 2016, la Belgique a été la cible de deux attentats terroristes, le premier à l'aéroport national de Zaventem, le second à la station de métro Maelbeek à Bruxelles. Le jour même, la responsabilité des attentats-suicides a été revendiquée par le groupe terroriste État islamique.

Le 11 avril 2016, les plus grands groupes politiques de la Chambre ont déposé une proposition commune visant à créer une Commission d'enquête parlementaire.[89]

Elle a réalisé un travail minutieux axé sur trois volets : Assistance et secours aux victimes, Architecture de la sécurité et Radicalisme. Cela s'est traduit par quatre rapports intermédiaires contenant plus de 400 recommandations adoptées à l'unanimité. Très larges, ces recommandations dépassaient souvent le simple domaine du terrorisme, de l'extrémisme et de la radicalisation.

Le troisième rapport intermédiaire « Architecture de la sécurité »[90] était le plus volumineux. Il formule des constatations et des recommandations sur le fonctionnement, la réglementation et les procédures des différents services de sécurité (police, justice, service de renseignement et autres). En ce qui concerne les services de renseignement, il a notamment été recommandé de donner une plus

---

86 Courrier SGRS du 3 mars 2022.

87 Le 15 juin 2022, le Comité permanent R a ouvert une enquête de contrôle dans les limites de ses compétences (relatives aux services de renseignement et de sécurité) et en a informé la Présidente de la Chambre, les ministres concernés ainsi que les chefs de service de la VSSE et du SGRS. Le rapport final a été remis à la présidente de la Chambre le 4 octobre 2022.

88 Voir : Chambre des représentants, *Commission d'enquête Attentats terroristes 22 mars 2016. Résumé des travaux et recommandations*, 2018, 84 p.

89 *Doc. Parl.* Chambre, 2016-17, n° 54-1752/001.

90 *Doc. Parl.* Chambre, 2016-17, n° 54-1752/008, 15 juin 2017.

grande marge de manœuvre aux services, d'améliorer la position d'information, de finaliser le Plan stratégique national du renseignement (PSNR), ou encore, de mener une politique de gestion des ressources humaines plus flexible.

Nombre de ces recommandations ont été formulées en termes assez généraux.

La mise en œuvre précise et concrète des recommandations a été laissée aux ministres et aux chefs des services respectifs concernés. Des éléments concrets d'amélioration ont cependant été avancés çà et là, par exemple la recommandation de créer une Banque-carrefour de la sécurité, et la suggestion d'une colocation entre l'OCAM et le Centre de crise national, d'une part, et la VSSE et le SGRS, d'autre part. En outre, une grande attention a été accordée aux problèmes et aux propositions d'amélioration de la coordination entre les différents services et les différents niveaux (à la fois aux niveaux fonctionnels – administratif et judiciaire – et aux niveaux géographiques – local *vs* supralocal). La conclusion à en tirer était qu'il s'agissait de la principale faiblesse dans la culture et l'architecture de la sécurité dans notre pays. La Commission d'enquête a fait remarquer qu'un travail considérable avait déjà été accompli par les services respectifs, mais elle constatait que ce travail s'était caractérisé par un manque de concertation, de coordination et de complémentarité.

I.7.1.2. (Encore) une évaluation ?

À l'issue de ses travaux, la Commission d'enquête avait constaté que la menace terroriste était en constante évolution et nécessitait donc une vigilance continue. La Commission d'enquête a donc recommandé la création d'une Commission de suivi chargée de contrôler la mise en œuvre des recommandations de la Commission d'enquête parlementaire. Une Commission de suivi a été mise en place concernant la mise en œuvre des recommandations du volet « Architecture de la sécurité ». Par la suite, cette tâche a été confiée aux Commissions permanentes compétentes (Intérieur et Justice).

En mars 2021, les ministres ont présenté un état des lieux commun.[91] En 2022, le même exercice a été réalisé mais cette fois, les Commissions Intérieur et Justice se sont réunies séparément.[92] Les documents remis en 2022 par les ministres de l'Intérieur et de la Justice[93] dressent l'état d'avancement de chaque

91 Réunion commune de la Commission Justice et de la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives, 19 mars 2021, CRIV 55 COM 418 ; Réunion commune de la Commission Justice et de la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives, 23 mars 2021, CRIV 55 COM 422.

92 Commission de l'Intérieur, 25 mai 2022 ; Commission de la Justice, 3 juin 2022, CRIV 55 COM 806 ; Commission de l'Intérieur, 21 juin 2022, CRIV 55 COM 824.

93 Le document remis par le ministre de la Justice s'intitule « Team Justice, Rapport de synthèse. État des lieux en date du 01/03/2022 Recommandations Justice - Commission d'enquête parlementaire Attentats Bruxelles 22 mars 2016, 80 p ». Il a été remis à la Chambre des représentants le 18 mars 2022.

recommandation, et précisent pour celles qui n'ont pas encore été exécutées si elles sont programmées ou non. Le ministre de la Justice listait ainsi 50 recommandations pour la VSSE, dont 18 seraient finalisés, 20 en cours, une programmée et onze non programmées.[94]

Il est important de noter que la Commission Défense n'a pas été impliquée ni en 2021 ni en 2022 dans cet exercice. Le président de la Commission Défense a fait savoir que celle-ci n'avait pas tenu de réunion spécifique consacrée au suivi des recommandations.[95]

Enfin, dans son 'rapport de synthèse' (voir infra), le ministre de la Justice avait proposé, « *afin de maintenir une vue d'ensemble et de mieux coordonner les efforts* » que « *le Comité de coordination du renseignement et de la sécurité (CCRS), créé dans le giron du Conseil national de sécurité, assure le suivi. Il appartient ensuite au CCRS de mettre un tableau de bord à la disposition du CNS, du CSRS et, si nécessaire, du Parlement* ».[96]

Mais la Commission d'accompagnement parlementaire y a également vu un rôle pour le Comité permanent R et a proposé d'orienter les travaux comme suit : « *La Commission devrait confier au Comité permanent R la mission d'effectuer un travail supplémentaire de surveillance des services en examinant de plus près les recommandations non encore exécutées en matière d'échange de données et de renseignement* » (nous soulignons).[97]

Et plus loin : « *La Commission demande au Comité permanent R de lui fournir [...] une liste actualisée de l'état d'avancement des recommandations concernant les services de renseignement et en particulier les banques de données et les échanges d'informations, ainsi qu'une analyse de l'état des lieux des services de renseignement et des pistes d'amélioration pour un meilleur fonctionnement des services* » (nous soulignons).[98,99]

---

94 Pour l'OCAM, le ministre liste huit recommandations, dont quatre qui seraient finalisées et quatre en cours.

95 Lettre du président de la Commission, Peter BUYSROGGE, au Comité permanent R, datée du 21 juin 2022. Il est toutefois noté en marge que la ministre de la Défense et le chef du SGRS ont présenté le Plan directeur 2022 du SGRS lors d'une séance à huis clos le 30 mars 2022.

96 Team Justice*, Rapport de synthèse. État des lieux en date du 01/03/2022 Recommandations Justice - Commission d'enquête parlementaire Attentats Bruxelles 22 mars 2016*, s.d., 3.

97 *Doc. Parl.* Chambre, 2021-22, 55K2745/001, p. 10.

98 *Ibid.*, p. 16.

99 Bien que de nombreuses recommandations aient été formulées dans le contexte de la lutte contre l'extrémisme et le terrorisme, et donc vis-à-vis de l'Organe de Coordination pour l'Analyse de la Menace (OCAM), le Comité n'a pas été explicitement mandaté pour l'analyse de *leur* mise en œuvre. La mise en œuvre des recommandations relatives à l'OCAM pourrait éventuellement faire l'objet d'une enquête de contrôle conjointe ultérieure (Comités permanents R et P).

I.7.2. LES GRANDS AXES DES RECOMMANDATIONS

La Commission d'enquête a passé au crible tous les aspects de l'architecture belge de la sécurité. Les grands axes des recommandations étaient[100]:

- Les différents services publics et de sécurité fonctionnaient encore trop en parallèle. Ils doivent former un appareil de sécurité aux rouages bien huilés dont chacune des pièces remplit une fonction clairement définie ;
- Les informations pertinentes doivent circuler rapidement d'un niveau de pouvoir à l'autre, d'un service public à l'autre. Cette circulation rapide de l'information doit également être effective entre les services belges et leurs homologues internationaux. Cela doit permettre aux services de sécurité de détecter de façon précoce les terroristes potentiels, de se concerter rapidement et de fixer des priorités de façon flexible ;
- La radicalisation et le terrorisme doivent faire l'objet d'une approche intégrale. La répression et les poursuites sont certes cruciales, mais il convient également d'accorder une attention suffisante à l'action proactive et à la prévention ;
- Divers organes de sécurité ont besoin de plus de moyens et d'effectifs. À certains niveaux de l'appareil de sécurité, il est indiqué d'accroître l'échelle et d'intensifier la collaboration car l'émiettement géographique et opérationnel sont des facteurs de risque pour son bon fonctionnement ;
- Il convient d'intensifier la coopération européenne et internationale. La Belgique escompte une modification des traités européens qui permettrait la création d'un service de renseignement européen. Dans l'intervalle, la Belgique peut intensifier sa coopération avec les États membres partageant son point de vue au sein du Counter Terrorism Group d'Europol ;
- Il convient d'endiguer la multiplication des réglementations et procédures (internationales et nationales), car elle risque d'aggraver l'incohérence des politiques menées ;
- Les autorités doivent veiller à ce que les mesures de lutte contre le terrorisme et la radicalisation ne vident en aucun cas de leur substance les valeurs fondant notre démocratie.

Les recommandations spécifiquement adressées à la Sûreté de l'État et au Service général du renseignement et de sécurité ont été rassemblées sous les thématiques suivantes :

- La position d'information des services de renseignement ;
- Les synergies entre la VSSE et le SGRS ;
- La dimension internationale du renseignement ;
- La gestion et la circulation des informations ;
- Les Joint Intelligence et Joint Decision Centres ;
- La gestion des ressources humaines.

---

100 La Chambre des représentants, C*ommission d'enquête attentats terroristes, 22 mars 2016, Résumé des travaux et recommandations*, pp. 38-39.

I.7.3. L'INFLUENCE DE LA COMMISSION PARLEMENTAIRE SUR LE TRAVAIL DE RENSEIGNEMENT

I.7.3.1. Évaluation globale

En modifiant la loi en 1996, le législateur a voulu donner plus de poids aux enquêtes parlementaires. Désormais, chaque Commission d'enquête parlementaire est tenue de rédiger un rapport sur ses travaux à l'issue de son enquête.[101] Ce rapport doit contenir une conclusion finale et, le cas échéant, formuler des propositions sur les futures initiatives législatives. En d'autres termes, le législateur a voulu éviter, à tout moment, que les travaux des Commissions d'enquête parlementaire ne restent lettre morte. Les activités des Commissions d'enquête parlementaires se situent avant le travail législatif (débats, évaluation des alternatives, suggestion de solutions possibles) ou après le travail législatif (contrôle de la mise en œuvre, du respect et de la sanction, suggestion d'autres règles...).

On a pu noter que la Commission d'enquête parlementaire Attentats s'est certainement conformée à l'article 13 de la loi sur l'enquête parlementaire : sur le plan de l'architecture de la sécurité en Belgique, entre autres, les travaux de la Commission ont abouti à un rapport particulièrement volumineux, assorti d'un grand nombre de recommandations. En outre, pour la première fois, une Commission de suivi a été mise en place pour contrôler le respect des recommandations formulées. Le suivi de la mise en œuvre des recommandations a également été annoncé tel quel dans l'accord de gouvernement.[102] La menace terroriste est en constante évolution, ce qui rend nécessaire une vigilance permanente.[103]

Les recommandations étaient nombreuses, adressées aussi bien aux pouvoirs législatif, exécutif et judiciaire et ont exercé, et exercent encore toujours,[104] une influence significative sur les réformes (dans le secteur du renseignement). Toutefois, le Comité a pu constater que de nombreuses recommandations étaient, en fait, une répétition de conclusions et de recommandations antérieures. Plusieurs réformes avaient déjà été anticipées et une série de réformes planifiées ont été accélérées. Force est également de constater que (au moins) certaines des recommandations n'étaient pas ou peu SMART, étaient répétitives ou n'exprimaient qu'une préoccupation qui ne pouvait pas être réalisée à court ou même à moyen

---

101 « *Art. 13. La commission consigne la relation de ses travaux dans un rapport public. Elle acte ses conclusions et formule, le cas échéant, ses observations quant aux responsabilités que l'enquête révèle, et ses propositions sur une modification de la législation* », Loi du 3 mai 1880 sur les enquêtes parlementaires, *M.B.* 5 mai 1880.

102 Gouvernement fédéral, *Accord de gouvernement,* 30 septembre 2020, 74 p.

103 M. VAN DER HULST, *Commission d'enquête Attentats terroristes 22 mars 2016, Résumé des travaux et recommandations,* Chambre des représentants de Belgique, 13 p.

104 Par exemple, l'exposé des motifs de la loi du 14 juillet 2022 modifiant la loi organique des services de renseignement dans le cadre de l'autorisation de la commission d'infractions par des sources humaines fait référence aux recommandations de la Commission d'enquête parlementaire. *Doc. Parl.* Chambre 2021-2022, 55DOC2706/002.

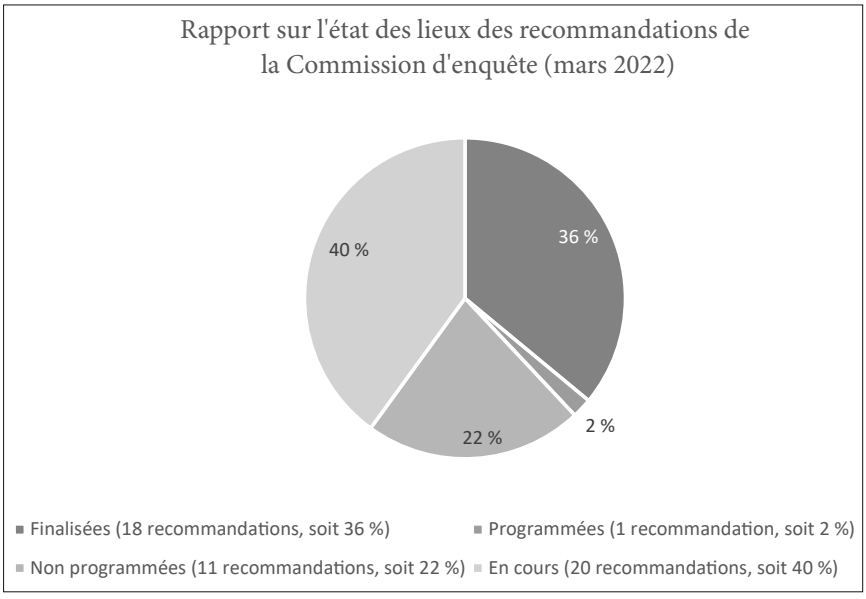
terme (par exemple, la création de la Banque-carrefour). Bon nombre des recommandations de la Commission d'enquête ont néanmoins été réalisées depuis lors : on peut donc parler à juste titre d'un rôle de catalyseur.

I.7.3.2. Avancée dans la réalisation des recommandations[105]

En ce qui concerne la VSSE

En 2020 et 2021, les ministres de la Justice et de l'Intérieur ont procédé à un échange de vues en Commission mixte à la Chambre sur l'état d'avancement des recommandations de la Commission d'enquête parlementaire.[106] En juin 2022, la discussion – basée sur un rapport de synthèse du ministre de la Justice[107] – s'est poursuivie au sein de la Commission de la Justice.

En ce qui concerne la mise en œuvre des recommandations (le ministre a retenu une cinquantaine[108] de recommandations pour la VSSE), l'état des lieux suivant a été rapporté :



105 Le rapport visait à évaluer les progrès réalisés dans la mise en œuvre de chaque recommandation, ainsi qu'à fournir des commentaires et à identifier les points d'attention pour l'avenir. Pour une évaluation détaillée de toutes les recommandations, il est renvoyé vers le rapport d'enquête repris dans son intégralité sur le site internet du Comité permanent R (www.comiteri.be).

106 Les députés n'ont pas semblé satisfaits de ces premières évaluations.

107 Team Justice, *Rapport de synthèse. État des lieux du 01/03/2022 Recommandations Justice*. 80 p.

108 Dans son exposé, le ministre de la Justice a retenu un total de 142 recommandations (y compris pour la police, l'OCAM...), dont 69 ont été indiquées comme étant "finalisées". 54 recommandations sont "en cours".

Selon le ministre, 36 % des recommandations concernant la VSSE ont été finalisées et 40 % sont en cours ; il a été noté précédemment que la majeure partie de l'ensemble des recommandations «non programmées» concerne la VSSE.[109] Toutes les recommandations n'ont ainsi pas été mises en œuvre ou ne sont pas programmées.[110] Pour certaines de ces recommandations qui ne sont pas encore mises en œuvre ou pas encore programmées, les services de renseignement ont fourni une justification.

L'état des lieux est un instantané, par nature évolutif : les recommandations qui étaient encore répertoriées comme étant «en cours» en mars ont entre-temps (quelques mois plus tard) été réalisées (par exemple, la commission d'infractions par des sources). En raison de l'ambiguïté des recommandations, des contradictions ont également été constatées : en ce qui concerne la police, la recommandation relative au JIC/JDC était « en cours », alors que pour la VSSE, elle portait le statut « finalisée ». « Finalisée » à Bruxelles, mais en cours dans d'autres cours d'appel ; et « finalisée » au sens opérationnel, mais pas « ancrée légalement », comme le recommandait la Commission d'enquête. La question de savoir si certaines recommandations peuvent être considérées comme ayant été « réalisées » dépend souvent de l'angle sous lequel on les considère. Peut-on considérer que la recommandation relative à la mise en place d'un réseau d'officiers de liaison a été réalisée parce qu'un ou deux officiers de liaison sont en fonction, ou est-il préférable dans ce cas de parler d'une recommandation « en cours » ? Il n'était pas, non plus, toujours clair de déterminer ce que l'on entendait par certaines recommandations.

Ou, comme l'a dit le ministre de la Justice lui-même, « *si vous demandez à quatre experts ce qu'est la Banque-carrefour Sécurité, vous obtiendrez cinq réponses différentes* ». D'autres recommandations, signalées comme « non programmées », ont ensuite été interprétées différemment. De plus, certaines recommandations semblent avoir été répétées plusieurs fois, ce qui peut fausser l'évaluation (et par extension le diagramme). Enfin, certaines recommandations évidentes (par exemple, « *lutter contre les fuites* ») ne semblent pas avoir été retenues par la VSSE.

Si le Comité n'était pas nécessairement d'accord avec l'ensemble de l'évaluation, il est, de manière générale, d'accord avec les réponses formulées par la VSSE, qui témoignent de l'importance (des recommandations) de la Commission d'enquête parlementaire. Les experts l'ont exprimé comme suit : « *De par son poids politique, le rapport de la commission d'enquête est incontournable pour les services qui doivent s'y référer. Mais si certains estiment que 'la commission d'enquête a un peu boosté les*

---

109 *Ann.* Chambre 2021-2022, CRIV 55 COM 806, 3 juin 2022, 23.

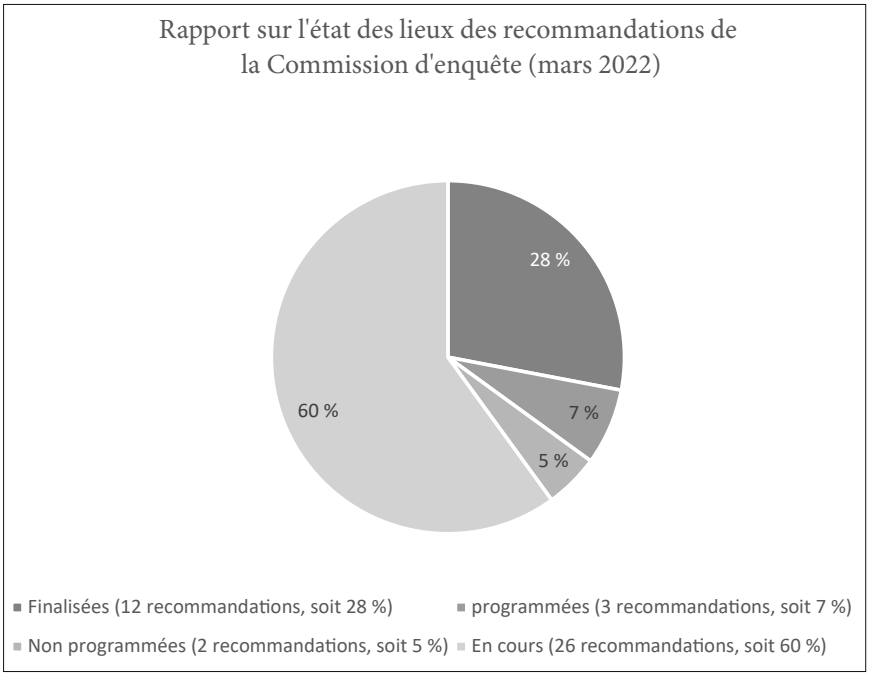
110 Un parlementaire se demandait *'jusqu'à quel point une administration peut considérer comme judicieux d'exécuter des recommandations émises par le Parlement'* (*Ann.* Chambre 2021-2022, CRIV 55 COM 806, 3 juin 2022, 26). Le ministre était d'avis qu'il y avait parfois des points de vue différents.

choses', les agents insistent plus généralement sur le fait qu'ils n'ont pas attendu la commission pour réorganiser leurs pratiques et renforcer leur coopération ».[111]

En ce qui concerne le SGRS

Contrairement à la VSSE et, par extension, au ministre de la Justice, le SGRS n'avait pas fourni précédemment d'aperçu des recommandations formulées par la Commission d'enquête parlementaire. Cependant, bon nombre des recommandations revêtent également une grande importance pour le renseignement militaire.

Le Comité a préparé un aperçu similaire à celui du ministre de la Justice, qui a été soumis au SGRS. 43 recommandations ont été retenues. Le statut d'exécution de ces recommandations a été interprété par le SGRS comme suit :



Le SGRS semble considérer moins de recommandations comme étant « finalisées » (28 %) que la VSSE ; beaucoup plus (60 %) semblent toujours « en cours », cinq ans après la publication du rapport. Seuls 5 % des recommandations ont reçu le statut «non programmées», ce qui représente une différence notable par rapport à l'estimation de la VSSE (22 %).

111 C. THOMAS (2021), *'Une menace possible et vraisemblable'. Dire et faire la sécurité : l'Organe de Coordination pour l'Analyse de la Menace et la structuration du champ antiterroriste belge*, Université Saint-Louis - Bruxelles, décembre 2021.

Comme indiqué, cet état des lieux de l'avancement des recommandations est un instantané, qui a ensuite été présenté sous forme de graphique. Selon les paramètres d'évaluation utilisés, une recommandation peut être considérée comme « finalisée » ou « en cours », ce qui peut donner une image différente. Cela signifie que de tels diagrammes doivent être interprétés avec prudence. Ils sont indicatifs, tout au plus.

I.7.3.3. Points d'attention (prioritaires) pour l'avenir

Selon le Comité permanent R et sur la base des observations ci-dessus, le bilan de cette Commission d'enquête (concernant ce qui a été étudié *in casu*) est majoritairement positif.[112]

Un certain nombre de préoccupations importantes demeuraient néanmoins. Elles sont reprises ci-dessous – de manière non exhaustive et par ordre d'importance :

- Le Comité permanent R plaide, comme le prévoyait aussi la Commission, pour l'ancrage légal d'un certain nombre de principes. Ceci semble aujourd'hui faire défaut (par exemple dans le contexte de l'entrave primaire, la mise en œuvre du JIC/JDC, la relation entre l'art. 29 CP et 19/1 L.R&S, les modalités de la coopération internationale, etc.). Compte tenu de l'impact potentiel de ces pratiques pour les citoyens, le Comité estime qu'il est essentiel de prévoir les garanties juridiques nécessaires, en définissant non seulement les conditions d'application, mais aussi les mécanismes de contrôle requis ;
- Depuis longtemps déjà, le Comité plaidait pour que les déficits soient comblés ainsi que pour le renforcement des services de renseignement. Il ne s'agissait, bien entendu, pas exclusivement d'améliorer la lutte contre le terrorisme et l'extrémisme : l'allocation des ressources (humaines) nécessaires doit permettre d'accomplir correctement toutes les tâches énumérées dans la loi organique des services de renseignement. Etant donné que la VSSE et le SGRS voient leurs effectifs augmenter, le recrutement doit être activement poursuivi et la réalisation du projet de statut unique du personnel doit être accélérée[113] ;
- La coordination et la coopération entre les deux services de renseignement doivent être améliorées de manière continue, notamment par une approche commune et planifiée des phénomènes, une utilisation rationnelle des ressources, un échange et un flux d'informations horizontaux renforcés et de meilleure qualité, une coopération étroite en termes d'OSINT, SOCMINT,

---

112 D'autres sont également parvenus à cette conclusion, voir par exemple : A. KENTANE, *Invloed van parlementaire onderzoekscommissies op het strafrechtelijk beleid*, Universiteit Gent, 2020.

113 Dans le rapport d'activités 2021-2022 de la VSSE, l'Administratice générale a.i. confirmait travailler à l'introduction du statut unique du personnel (VSSE, *Intelligence Report 2021-2022*, 2023, www.vsse.be, p. 5).

HUMINT et SIGINT, sans que les services ne perdent leur identité ou leurs caractéristiques spécifiques ;
– Les technologies de l'information et de la communication (TIC) restent un domaine prioritaire pour les services de renseignement et de sécurité, qui doit être assorti des ressources humaines et budgétaires nécessaires (outils TIC de qualité pour les services ; TIC open source ; développement d'un réseau de communication sécurisé[114] ; cryptage des informations, interconnexion des bases de données ; ...). Cela demande plus de temps et de ressources que ce qui est actuellement disponible au sein des services. Le Comité recommande de (continuer à) travailler sur ce point et à en faire une priorité ;
– La Commission d'enquête parlementaire a également plaidé pour « *la rationalisation, la clarification et la mise à jour des lois et de la réglementation* ». Le Comité permanent R constate que la logique et l'équilibre dans le contexte du déploiement des méthodes spéciales de renseignement et des méthodes dites ordinaires sont plus mis sous pression. En raison des modifications législatives successives, la logique interne se perd (par exemple, le degré d'intrusion) et les possibilités de contrôle sont réglementées d'une manière pratiquement différente pour chaque méthode. Une rationalisation est urgente ;
– Les services doivent s'engager de manière continue en termes de coopération internationale (échange d'informations, nomination d'officiers de liaison...). Mais il était également urgent d'établir un cadre juridique clair pour l'échange d'informations et de données personnelles avec les pays étrangers.

Enfin, le Comité permanent R souhaitait attirer l'attention sur un certain nombre d'autres points :
– Le Comité recommande un débat public (parlementaire) plus large sur les tâches des deux services de renseignement prévues dans la loi des services de renseignement de 1998 et sur la priorisation qui y est liée. Ceci nécessite une discussion « stratégique » concernant l'octroi des capacités et moyens suffisants pour permettre à chacun des services de détecter, suivre et maîtriser comme il se doit toutes les menaces contre la sécurité (inter)nationale. Les services de renseignement et de sécurité doivent retenir l'attention du Parlement, et ce, pas uniquement ponctuellement lorsque surviennent des problèmes individuels (politique du chalumeau) ;
– Il est essentiel que l'élargissement des pouvoirs, des ressources matérielles et humaines des services de renseignement et de sécurité se fasse dans le respect des principes de l'État de droit. Les *checks and balances* nécessaires doivent être prévus. Dans le cadre de cette extension, il convient également de prévoir

[114] Le Comité recommande la plus grande prudence dans le choix des équipements techniques sécurisés pour le traitement des informations sensibles et classifiées. Les équipements techniques doivent être évalués, certifiés et homologués – en termes de fiabilité et de sécurité – selon des critères et des procédures conformes aux normes de l'Union européenne.

un renforcement des effectifs des organes de contrôle. Sans cela, le contrôle démocratique risque d'être réduit à du *window dressing*.[115] Bien que les tâches et compétences du Comité permanent R ont été considérablement élargies ces dernières années, le budget et l'extension du personnel sont à la traîne ;

– Par extension, le Comité permanent R veut également attirer l'attention sur le fait qu'il formule également des recommandations annuelles à l'intention du législateur et du pouvoir exécutif qui portent notamment sur la légalité, la coordination et l'efficacité de l'action des deux services de renseignement belges (et de l'OCAM). Ces recommandations résultent de différents avis et enquêtes de contrôle. Celles-ci ont été compilées, à l'intention de la Commission d'accompagnement parlementaire, dans un aperçu (1994-2005)[116], (2006-2016)[117] et une mise à jour jusqu'en 2021 a récemment été réalisée. Un (grand) nombre de ces recommandations ont été réalisées entre-temps, certaines se recoupent avec celles de la Commission d'enquête, et d'autres doivent encore être mises en œuvre. Le Comité permanent R suggère à la Commission de suivi d'en faire une lecture conjointe ;
– Un exercice d'évaluation similaire pour les recommandations formulées par la Commission d'enquête en ce qui concerne l'Organe de coordination pour l'analyse de la menace (OCAM) s'impose. Il doit toutefois faire l'objet d'une enquête de contrôle conjointe avec le Comité permanent P.

I.8. LES TENTATIVES D'INGÉRENCE RUSSE DANS LA VIE POLITIQUE EN BELGIQUE

Mi-septembre 2022 était rendu public un extrait déclassifié d'un rapport des services de renseignement américains, largement relayé par la presse internationale, faisant état de (tentatives) d'ingérence russe dans la vie politique de nombreux pays à travers le monde.[118] Selon ce rapport, « *Russia has covertly transferred over $300 million, and planned to covertly transfer at least hundreds of million more, to foreign politicial parties, officials, and politicians in more than two dozen countries and across four continents since 2014* ». L'objectif ainsi poursuivi par le Kremlin

---

115 L'objectif est de faire passer le nombre de membres du personnel de la VSSE d'environ 600 à 1 000 ; le SGRS travaille également à une extension de son personnel (jusqu'à 1 200). Le nombre de membres du personnel déployés pour le contrôle démocratique du fonctionnement des services de renseignement et de sécurité doit évoluer en proportion. Dans la négative, il y a un risque de déficit démocratique.

116 COMITÉ PERMANENT R, *Rapport d'activités 2006*, pp. 1-21.

117 COMITÉ PERMANENT R, *Rapport d'activités 2017*, pp. 128-152.

118 Notamment : « *Russia Secretly Gave $300 Million to Political Parties and Officials Worldwide, U.S. Says* », The New York Times, 13 septembre 2022 ; « *Russia has spent $300m since 2014 to influence foreign officials, US says* », The Guardian, 13 septembre 2022 ; « *Russia spent $300 million secretly interfering in foreign politics, U.S. says* », NBC News, 14 septembre 2022.

serait d'affaiblir les démocraties et renforcer les mouvements politiques considérés comme « alignés » aux intérêts russes.[119]

Bien que le rapport ne pointe aucun pays explicitement, la presse relaya des commentaires anonymes de hauts responsables américains qui, concernant Bruxelles, déclaraient « *the Kremlin had used Brussels as a hub for foundations and other fronts that back far-right candidates. Fictitious companies were said to be used to fund European parties and to buy influence elsewhere* ».[120]

Suite à ces révélations, la Présidente de la Chambre adressait début décembre 2022 un courrier au Comité permanent R lui demandant « *de s'enquérir de la réaction des services quant à ces informations et de lui fournir endéans le mois une note circonstanciée quant à la position d'information des services sur ce mode d'ingérence* ».

I.8.1. UNE PROBLÉMATIQUE CONNUE

La problématique de l'ingérence russe pointée dans le rapport américain n'est pas neuve et retient l'attention depuis plusieurs années déjà. Depuis les élections présidentielles américaines en 2016 – où une immixtion de la Russie a été constatée par les services de renseignement américains (notamment par la diffusion sélective des informations, les actions de propagande et les tentatives de piratages des systèmes de vote)[121] – l'ingérence russe dans les processus électoraux est source d'inquiétude dans de nombreux pays européens et plusieurs scrutins semblent d'ailleurs avoir été influencés par le Kremlin.[122]

---

119 Le rapport révèle encore que les financements russes sont généralement opérés par des membres des services de renseignement, mais aussi des oligarques russes. Les moyens de paiement sont multiples (argent liquide, cryptomonnaies…). Les opérations financières s'opèrent par le biais d'intermédiaires (think tanks, fondations, groupes criminels…) et les ressources des ambassades russes sont souvent mises à profit pour soutenir ces procédés.

120 « *Russia covertly spent $300m to meddle abroad – US* », BBC news, 14 septembre 2022 ; « *Comment la Russie a pesé sur des élections étrangères à coups de millions de dollars* », L'Express, 14 septembre 2022.

121 SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE, Report « *Russian Active campaigns and interference in the 2016 U.S. Election* », july 2020 : Publications | Intelligence Committee (senate.gov) ; OTAN, « *L'ingérence de la Russie dans les élections des pays de l'Alliance* », Rapport de la Commission des sciences et des technologies (Rapporteuse générale : Susan Davis), novembre 2018, Rapport général STC 2018 (nato-pa.int).

122 Voy. par exemple : Intelligence and Security Committee of Parliament ; Report « *Russia* », 21 July 2020, HC 632 – Intelligence and Security Committee of Parliament - Russia (independent.gov.uk) et « *Russia report reveals UK governement failed to investigate Kremlin interference* », The Guardian, 21 juillet 2020 ; OTAN, « *L'ingérence de la Russie dans les élections des pays de l'Alliance* », Rapport de la Commission des sciences et des technologies (Rapporteuse générale : Susan Davis), novembre 2018, Rapport général STC 2018 (nato-pa.int) ; « *Nederlandse geheime dienst: Russen beïnvloeden verkiezingen met nepnieuws* », De Morgen, 4 avril 2017 ; « *Ingérence russe : enquête en Allemagne sur les liens avec l'extrême droite* », Le Figaro, 14 février 2019 ; « *Européennes : Berlin "attentif" face au risque d'ingérence russe* », Le Point, 13 mai 2019.

En Belgique, la menace d'ingérence russe sur les élections européennes, fédérales et régionales de mai 2019 a été un point d'attention prioritaire pour la VSSE. Le SGRS s'intéressa également à la problématique en se penchant sur « *le phénomène de cyber-ingérence dans les élections* ».[123] Dans une enquête de contrôle précédente, le Comité permanent R a d'ailleurs pu constater que « *les deux services de renseignement avaient pris les mesures nécessaires pour contrer les éventuelles menaces visant les élections belges et européennes de mai 2019. Les services avaient reconnu et assimilé la problématique ; avaient examiné et identifié les risques et les menaces ; s'étaient organisés comme il se doit ; avaient développé la collaboration qui s'imposait entre eux et avec d'autres acteurs ; avaient sensibilisé et informé le Gouvernement et d'autres parties intéressées pour leur permettre, le cas échéant, de prendre les mesures nécessaires* ».[124] À la fin des opérations, les services n'avaient pas détecté de trace d'activité d'ingérence à grande échelle au cours de ces élections en Belgique.[125]

Dans sa note, le Comité permanent R revenait sur différentes initiatives directement liées à cette problématique, par exemple la commission spéciale du Parlement européen sur l'ingérence étrangère (INGE) dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation[126] ou au sein du Parlement belge.[127]

---

123 COMITÉ PERMANENT R, *Rapport d'activités 2020*, pp. 27-28. Concernant la compétence du SGRS en la matière, le Comité indiquait « *A première vue, la compétence du SGRS en la matière semblait moins évidente que celle de la VSSE. En effet, le SGRS est en premier lieu un service de renseignement militaire qui doit se concentrer sur les menaces militaires. Cependant, le SGRS s'est penché sur le phénomène de cyber-ingérence dans les élections, vu que l'influence clandestine de processus politiques a généralement une origine militaire* ».

124 COMITÉ PERMANENT R, *Rapport d'activités 2020*, pp. 27-28.

125 VSSE, Rapport annuel 2019, p.22 ; COMITÉ PERMANENT R, *Rapport d'activités 2020*, pp.27-28.

126 Voy. Parlement européen, Résolution du 10 octobre 2019 sur l'ingérence électorale étrangère et la désinformation dans les processus démocratiques nationaux et européen (2019/2810(RSP)) ; Résolution du 9 mars 2022 sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (2020/2268(INI)) ; Décision du 10 mars 2022 sur la constitution, les compétences, la composition numérique et la durée du mandat de la commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (INGE 2) (2022/2585 (RSO)).

127 Voy. notamment Sénat de Belgique, Demande d'établissement d'un rapport d'information relatif à la lutte contre les ingérences de puissances étrangères visant à saper les fondements de l'état de droit démocratique, session 2021-2022, 22 avril 2022, 7-344-1.indd (senate.be) ; Chambre des représentants, Proposition de loi modifiant, en vue d'interdire le financement étranger de partis politiques, la loi du 4 juillet 1989 relative à la limitation et au contrôle des dépenses électorales engagées pour l'élection de la Chambre des représentants, ainsi qu'au financement et à la comptabilité ouvertes des partis politiques, DOC 55 2905/001, 27 septembre 2022 ; Chambre des représentants, Proposition de loi la loi du 4 juillet 1989 relative à la limitation et au contrôle des dépenses électorales engagées pour l'élection de la Chambre des représentants, ainsi qu'au financement et à la comptabilité ouvertes des partis politiques, en vue d'interdire les dons des ressortissants étrangers et le sponsoring des entreprises, des associations de fait et des personnes morales dont le siège social n'est pas établi en Belgique, DOC 55 2997/001, 10 novembre 2022 ; Chambre des représentants, Proposition de résolution relative à la lutte efficace et effective contre l'influence étrangère et la mise à mal de notre démocratie, DOC 55 3045/001, 30 novembre 2022.

I.8.2. LE SUIVI PAR LES SERVICES DE RENSEIGNEMENT BELGES

Sur la base des réponses fournies par les services en décembre 2022, le Comité permanent R a conclu que la vie politique en Belgique – lisez belge, mais aussi européenne – est une cible potentielle des tentatives d'ingérences russes. Les services de renseignement belges sont conscients de cette menace et opèrent un suivi de celle-ci selon des angles différents, tenant compte de leurs compétences respectives.

I.8.2.1. Une position d'information solide selon la VSSE

La VSSE enquête sur l'ingérence principalement en vertu de ses missions de protection de la sécurité intérieure et extérieure de l'Etat.[128] Le service explique qu'il est depuis longtemps établi que la Russie vise les milieux politiques belges ainsi que l'opinion publique et certains médias. En ce qui concerne la sécurité extérieure de l'État, la VSSE suit également l'ingérence russe vis-à-vis des organisations internationales dont le siège est situé à Bruxelles – en particulier, l'Union européenne et l'OTAN. Le service précise enfin que l'impact potentiel de l'ingérence russe sur les relations extérieures belges constitue également une composante de ses enquêtes.

Selon la VSSE, l'ingérence russe est difficile à quantifier. Elle pointe plus précisément une probable tendance à l'intensification de l'ingérence russe ces dernières années, jusqu'à la guerre en Ukraine. La VSSE précise en effet que les individus qui, auparavant, ne voyaient aucun problème à entretenir des liens avec la Russie ne souhaitent plus, dans leur grande majorité, être associés à la Russie.

La VSSE qualifie la stratégie russe « *d'hybride* » et ce, à deux égards. D'abord, les services de renseignement ne sont pas les seuls acteurs russes à se livrer à de l'ingérence, d'autres organisations et individus agissant de leur propre initiative afin de se rapprocher du président russe Poutine. Ensuite, selon la VSSE, l'ingérence russe prend des formes variées et s'exerce par le biais d'agents (le recours à des personnes pour la diffusion des messages russes, etc.), de cyberopérations (par ex. les fameuses usines à trolls) et des médias (désinformation dans les médias publics russes, etc.).

Le service revendique une solide position d'information sur l'ingérence russe grâce aux moyens et ressources investis dans le suivi de cette menace. Ainsi, la VSSE a informé le Comité permanent R que depuis 2017, plus de cent MRD ont été lancées sur cette thématique.

Sur cette base, la VSSE indique ne pas disposer d'éléments concrets qui démontrent que des partis politiques belges sont financés de manière structurelle par des puissances étrangères (Russie ou autres puissances). Le service rappelle

[128] Selon la VSSE, la protection du Potentiel scientifique et économique (PSE) est moins présente dans les enquêtes sur l'ingérence (art. 7 L.R&S).

également que l'enquête menée en collaboration avec le SGRS sur les possibilités d'ingérence russe dans les élections belges de 2019 n'avait démontré aucune ingérence notable.

La VSSE indique encore que le service coopère étroitement avec le SGRS sur cette thématique. Lors de réunions (bi)mensuelles, les deux services échangent informations et évaluations. Selon la VSSE, la répartition des tâches entre le suivi du service de renseignement militaire GRU (SGRS) et celui du service civil SVR (VSSE) crée généralement une collaboration harmonieuse, mais la distinction entre les deux n'est pas toujours simple à faire, d'où des concertations régulières sur des dossiers concrets.

I.8.2.2. Un suivi guidé par les intérêts militaires pour le SGRS

Si le SGRS suit de près les menaces d'espionnage et d'ingérence en provenance de la Russie, il n'étudie cette problématique qu'au regard des intérêts militaires belges et des intérêts belges à l'étranger. Dès lors, le service indique que le suivi des flux financiers en provenance de Russie vers les partis politiques belges n'est pas sa première priorité.

Le SGRS confirme que l'ingérence est l'un des moyens utilisés par la Russie pour atteindre ses objectifs et mentionne plus spécifiquement les méthodes russes de désinformation et de manipulation de l'information.

A propos des cibles d'une telle ingérence, le SGRS indique qu'il dispose d'indications suggérant que les services de renseignement russes accordent une attention particulière aux partis extrémistes, dont ils estiment qu'ils peuvent à terme imposer un cours politique plus favorable à la Russie. En particulier, les partis et individus qui remettent en question l'ordre libéral international en place depuis la Seconde Guerre mondiale sont des alliés idéologiques des services de renseignement russes. L'anti-atlantisme et une aversion pour la migration sont des caractéristiques de ces cibles.

I.8.3. CONCLUSIONS

À l'issue de sa note, le Comité concluait que la menace d'ingérence dépasse la seule problématique du financement russe d'acteurs politiques et recommandait qu'une enquête de contrôle soit entamée afin de déterminer si les services de renseignement belges disposent des moyens suffisants (légaux et opérationnels) pour détecter la menace d'ingérence de puissances étrangères par le financement de partis politiques, institutions politiques ou personnalités politiques en Belgique.

I.9. ANALYSE JURIDIQUE RELATIVE À L'ARMEMENT ET À L'ÉQUIPEMENT DES AGENTS APPARTENANT À LA '*INCIDENT RESPONSE TEAM*' (VSSE)[129]

Depuis l'entrée en vigueur de la Loi du 30 mars 2017[130], la Loi organique des services de renseignement et de sécurité[131] stipule qu'il peut être institué au sein de chaque service de renseignement – donc tant au sein de la Sûreté de l'État (VSSE) qu'au sein du Service Général du Renseignement et de la Sécurité (SGRS) – une équipe d'intervention ayant pour fonction de protéger le personnel, les infrastructures et les biens du service concerné. Une telle équipe d'intervention, dénommée *Incident Response Team* (IRT), a effectivement été mise en place au sein de la VSSE, ce qui n'est pas encore le cas au SGRS.

La création de l'équipe d'intervention au sein de la VSSE remonte à mai 2015 et constituait une réponse au danger et à l'insécurité croissante dans lesquels le service évoluait depuis un certain temps. Cette équipe d'intervention – initialement dénommée *Intervention Response Team*, en abrégé 'IRT' – conférait une capacité de sécurité permanente à la VSSE pour encadrer les activités du personnel avec des garanties de sécurité accrues. En septembre 2016, le gouvernement a déposé un projet de loi modifiant la Loi Renseignement afin, entre autres, de moderniser l'IRT. L'objectif était de doter l'équipe d'un statut juridique et d'un mandat. Le projet de loi prévoyait également un arsenal de pouvoirs coercitifs administratifs de la police pour l'IRT et créait un statut spécial de responsabilité civile et d'aide juridique pour les membres de l'IRT. Tout cela était nécessaire pour que l'IRT devienne un service de sécurité complet et mature, un besoin qui se faisait particulièrement sentir après la survenance des attentats terroristes de Paris (13 novembre 2015) et de Bruxelles (22 mars 2016). Dans le cadre de la Loi d'actualisation MRD du 30 mars 2017, la modernisation et la poursuite du développement de l'IRT sont devenues une réalité. En juin 2017, le nom a été modifié en *Incident Response Team* (également abrégé en IRT).[132]

Début octobre 2022, le Comité permanent R a lancé une analyse juridique sur l'armement et l'équipement de cette *Incident Response Team*. L'enquête était cependant sans objet. L'arrêté ministériel du 6 mai 2003 *'déterminant les armes et les munitions faisant partie de l'équipement réglementaire des agents des services*

---

129 Voir B. VERSCHAEVE, "Het incident response team van de staatsveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht", *Politie & Recht*, 2022, n°1, pp. 3-20.

130 Loi du 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal (*M.B.* 28 avril 2017 ; ci-après : Loi d'actualisation MRD).

131 Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (*M.B.* 18 décembre 1998 ; ci-après : Loi Renseignement ou L.R&S).

132 Comme la dénomination initiale de l'IRT, la Loi Renseignement (art. 22 à 35 L.R&S, insérés par les art. 52 à 69 de la Loi d'actualisation MRD) utilise les termes 'équipe d'intervention' et 'membres de l'équipe d'intervention'.

extérieurs de la Sûreté de l'État et fixant les dispositions particulières relatives à la détention, à la garde et au port de ces armes' a été abrogé et le ministre de la Justice a créé un cadre juridique général pour la détention et le port d'armes par les agents de la VSSE. L'arrêté ministériel du 16 juin 2022 *'déterminant l'équipement réglementaire des agents de la Sûreté de l'État et fixant les dispositions particulières relatives à la détention, au port et à la garde de l'armement*'[133] offre la possibilité aux agents de la VSSE de porter une arme dans l'exercice de leurs missions. Le texte permet également le port d'armes supplémentaires par les membres de l'équipe d'intervention. L'Arrêté ministériel est entré en vigueur le 29 octobre 2022.

I.10. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ EFFECTUÉS EN 2022 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2022

I.10.1. L'APPLICATION DE NOUVELLES MÉTHODES (PARTICULIÈRES) DE RENSEIGNEMENT

Le Comité s'est vu attribuer une série de possibilités de contrôle en ce qui concerne certaines méthodes 'ordinaires'. Il s'agit notamment du contrôle de l'identification de l'utilisateur de télécommunications (art. 16/2 L.R&S), de l'accès à des données des dossiers passagers (*Passenger Name Record*, art. 16/3 L.R&S), de l'accès aux images des caméras utilisées par les services de police (art. 16/4 L.R&S), ou encore du contrôle préalable aux interceptions, aux intrusions dans un système informatique et la prise d'images animées (art. 44/3 L.R&S). Le Comité a décidé d'étudier cette matière dans une enquête 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 2020, l'accent a été mis sur l'élaboration d'une méthodologie dans le cadre du contrôle de l'identification de l'utilisateur de télécommunications (art. 16/2 L.R&S), ainsi que l'accès aux données PNR (art. 16/3).

Début 2021, le volet méthodologique relatif au contrôle préalable aux interceptions, aux intrusions dans un système informatique et à la prise d'images animées (art. 44/3 L.R&S) a été finalisé. En 2021, le Comité s'est en outre penché sur l'opérationnalisation de l'article 16/4, §2 L.R&S. Cet article régit l'extraction rétroactive des images des caméras de police par les services de renseignement. Cette disposition législative a une portée générale. Cela implique que les exigences procédurales qui y sont énoncées sont d'application pour l'extraction ciblée des images des caméras de police par un accès direct (en ligne) aux banques de données

133 *M.B.* 19 octobre 2022.

de la police concernées ainsi que pour l'extraction ciblée via une requête écrite adressée au service de police compétent (à savoir la Direction de l'information policière et des moyens ICT (DRI)). En raison d'une plainte DPA, l'enquête a été interrompue. La plainte a conduit à la rédaction d''Instructions de traitement du Comité permanent R (APD) concernant les extractions rétroactives par les services de renseignement des images de caméras de police sur la base de l'article 16/4, §2 L.R&S' (traduction libre).[134]

En 2022, le Comité a reçu les statistiques des deux services de renseignement quant à la mise en œuvre de cette méthode et a terminé le volet juridique de son analyse. Le rapport d'enquête n'a toutefois pu être finalisé en raison d'autres dossiers prioritaires mais sera achevé courant 2023.

I.10.2. LE RISQUE D'INFILTRATION AU SEIN DES DEUX SERVICES DE RENSEIGNEMENT

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

Plusieurs réunions de travail ont été organisées avec le SGRS et la VSSE sur la thématique 'cartographie et évaluation du risque d'infiltration au sein des services de renseignement'. À cet égard, le processus de gestion du risque, tel que repris dans la norme ISO 31000, constituait une base de départ.[135]

Après une interruption en 2021 en raison d'autres dossiers prioritaires et de l'impact de la crise sanitaire sur les effectifs du Comité, les devoirs d'enquête ont repris en 2022. Les informations déjà récoltées ont ainsi pu être traitées et des compléments d'informations ont été demandés aux services. Le traitement de leurs réponses et le rapport final seront finalisés courant 2023.

I.10.3. CONTRÔLE DES FONDS SPÉCIAUX : ENQUÊTE DE SUIVI

À l'instar de tout service public, les services de renseignement se voient également allouer des fonds publics pour exercer leurs missions légales. La règle pour l'utilisation de ces fonds doit être une transparence parfaite et un contrôle total. Cependant, comme certaines tâches de la VSSE et du SGRS sont imprévisibles ou

134 '*Verwerkingsinstructie van het Vast Comité I (DPA) m.b.t. de door de inlichtingendiensten ingestelde retroactieve opvragingen van politionele camerabeelden gegrond op artikel 16/4, §2 W.I&V*'.

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

doivent être tenues secrètes, une partie de leur budget échappe à cette règle. Cette partie est mieux connue sous le nom de 'fonds spéciaux'. Bien que le montant de ces fonds soit intégré dans le budget alloué aux services, des règles particulières s'appliquent à leur gestion, leur utilisation et leur contrôle. En 2015[136], le Comité s'est notamment attaché à déterminer la nature de ces 'fonds spéciaux', leur montant et leur répartition. Il a également contrôlé l'utilisation des moyens et les interactions entre ces 'fonds spéciaux' et les budgets dits 'normaux'. Enfin, le Comité s'est penché sur le cadre réglementaire et a examiné les mécanismes de contrôle, et ce tant en interne (au sein des services) qu'en externe (Cour des comptes, Inspection des Finances, Comité permanent R, etc.). Différentes recommandations ont été formulées.

Depuis 2018 (VSSE) et 2020 (SGRS), la Cour des comptes a exprimé son intention de réaliser un contrôle périodique de ces fonds. Dans ce contexte, la Cour des comptes a pu recourir à une assistance technique, telle que proposée par le Comité permanent R.[137] Le Comité pouvait à son tour « *exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds* ». Une enquête de suivi a été ouverte fin 2020 sur la gestion, l'utilisation et le contrôle des fonds spéciaux. Interrompus en raison de la prise en charge de dossiers prioritaires en 2021, les devoirs d'enquête ont repris en 2022. L'enquête a ainsi pu être clôturée et les résultats ont été présentés à la Commission de suivi au début de l'année 2023.

I.10.4. LE SUIVI DE L'IMAM MOHAMED TOJGANI PAR LA VSSE

En janvier 2022, la presse se faisait l'écho du recours de Mohamed TOJGANI, imam principal de la mosquée Al Khalil à Molenbeek, devant le Conseil du Contentieux des Etrangers (CCE) contre la décision de retrait de son permis de séjour en Belgique. Interrogé en séance plénière à la Chambre des Représentants, le secrétaire d'Etat à l'Asile et à la Migration a confirmé cette décision fondée sur des informations des services de sécurité.

À la demande de la Présidente de la Chambre, le Comité permanent R a ouvert une enquête de contrôle sur la manière dont la VSSE a assuré le suivi de l'imam. Plus particulièrement, il s'agit d'examiner la position d'information du service concernant l'intéressé et la manière dont le service a assuré son suivi. L'enquête du Comité vise également le traitement des données à caractère personnel de Mohamed TOJGANI par la VSSE et leur partage à d'autres administrations. Dans

---

136 COMITÉ PERMANENT R, *Rapport d'activités 2015*, pp. 11-16 ('La gestion, l'utilisation et le contrôle des fonds spéciaux').

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

ce cadre, le Comité évalue l'adéquation des informations communiquées aux autorités avec les renseignements récoltés et analysés par le service, d'une part, ainsi qu'au regard du prescrit de la législation en matière de protection des données personnelles, d'autre part.

Les devoirs d'enquête et l'analyse ayant été clôturés en 2022, le rapport d'enquête a été présenté à la Commission de suivi au premier trimestre de l'année 2023.

I.10.5. LES SCREENINGS DE SÉCURITÉ DES CANDIDATS À LA VSSE

Dans un passé récent, le Comité permanent R a formulé de nombreuses recommandations relatives aux screenings de sécurité : à propos des nécessaires screenings de sécurité pour certaines fonctions de confiance[138], davantage de screenings des militaires et des civils de la Défense[139], l'application conforme de la possibilité d'introduire des demandes de screenings de sécurité[140], … Dans le cadre de l'enquête de contrôle spécifiquement dédiée aux screenings de sécurité, plusieurs recommandations ont également été formulées.[141] Le Comité y avait soulevé la question du pré-screening des candidats à des emplois au sein de la VSSE et a décidé, en sa qualité d'autorité de contrôle compétente au sens de la Loi du 30 juillet 2018, d'y dédier une enquête. Fin 2022, plusieurs devoirs d'enquête ont été effectués ; le rapport d'enquête sera finalisé dans le courant de 2023.

I.10.6. UNE PLAINTE DE L'EXÉCUTIF DES MUSULMANS DE BELGIQUE CONTRE DES FUITES PRÉSUMÉES DE LA VSSE

Le 14 février 2022, l'Exécutif des Musulmans de Belgique (ci-après, EMB) a déposé devant le Comité permanent R une « *plainte formelle, écrite concernant le fonctionnement, l'intervention, les actes ou les ommissions de la Sûreté de l'Etat* ».[142] Dans son courrier, l'EMB affirme que « *ces dernières années, des rapports et notes de la Sûreté de l'Etat sont souvent utilisées comme moyens pour discréditer les Musulmans et les mosquées* » et plainte est déposée « *concernant le fonctionnement de la Sûreté de l'Etat, plus particulièrement la fuite systématique de rapports et la*

138 COMITÉ PERMANENT R, *Rapport d'activités 2021*, p. 208.
139 COMITÉ PERMANENT R, *Rapport d'activités 2021*, p. 196.
140 COMITÉ PERMANENT R, *Rapport d'activités 2021*, p. 195.
141 COMITÉ PERMANENT R, *Rapport d'activités 2019*, pp. 2-13 ('I.1. La réalisation de screenings de sécurité par les services de renseignement'), pp. 126-129 ('XI.2.1. Diverses recommandations concernant l'enquête de controle sur les screenings de sécurité').
142 Courrier de maître Verbist, en sa qualité d'avocat de l'Exécutif des Musulmans de Belgique, du 14 février 2022 déposant une « plainte concernant la fuite de documents de la Sûreté de l'Etat à propos de la communauté musulmane » (traduction libre).

consultation de rapports par des journalistes alors que les intéressés visés par ces rapports n'ont pas cette possibilité » (traductions libres).

Ces notes fuitées créeraient une image négative et stigmatisante (permanente) de l'Islam et des Musulmans en Flandre. La fuite systématique vers les médias constitue, selon l'EMB, une atteinte à la vie privée des personnes qui font l'objet de ces rapports (art. 22 de la Constitution et art. 8 CEDH). Une vingtaine d'exemples sont énumérés[143] et de nombreuses questions sont posées.

Début mars 2022, le Comité permanent R a informé la Présidente de la Chambre ainsi que le plaignant de l'ouverture d'une enquête de contrôle suite à la plainte de l'EMB contre des fuites présumées de la Sûreté de l'Etat. Il a également été précisé qu'en raison d'autres dossiers prioritaires, l'enquête ne serait lancée que fin 2022.

I.10.7. L'ACCÈS DES SERVICES DE RENSEIGNEMENT AUX IMAGES DES CAMÉRAS DE POLICE

Mi-mai 2022, le chef de corps d'une zone de police locale a adressé un courrier au Comité permanent R à propos de l'accès aux images des caméras de police par les services de renseignement.

Conformément à la loi organique des services de renseingement et à la loi sur la fonction de police, les services de renseignement peuvent avoir accès, sous réserve de certaines conditions, aux images des caméras de vidéosurveillance des services de police. Le chef de corps faisait état de conventions ou d'accords avec des zones de police en vue de la transmission de données à distance (c'est-à-dire la VSSE qui, depuis Bruxelles, prend la main sur des images collectées ailleurs en Belgique). La méthode 'traditionnelle' consiste pourtant à solliciter les images *in situ* et à être présent avec un opérateur politicer dans le centre de gestion des images au sein de la zone de police. Le chef de corps estimait qu'une analyse juridique s'imposait afin d'assurer la sécurité juridique de tous les acteurs impliqués.

I.10.8. ANALYSE JURIDIQUE RELATIVE AUX POSSIBILITÉS LÉGALES D'ENTRAVE

En 2022, le Comité permanent R a réalisé une analyse juridique des options légales dont disposent les services de renseignement en matière d'entrave (ou disruption). Cette analyse visait à clarifier une question soulevée dans divers dossiers examinés par le Comité, notamment l'enquête de contrôle sur la manière dont la Sûreté

[143] Entre autres, la fuite d'une note de la VSSE sur les possibles liens entre Ihsane Haouach et les Frères musulmans. Cet épisode avait déjà fait l'objet d'une enquête du Comité permanent R ('Enquête de contrôle sur la manière dont la Sûreté de l'Etat a assuré le suivi de la commissaire du gouvernement Ihsane Haouach', voir : www.comiteri.be).

de l'État a assuré le suivi de l'imam Mohamed TOJGANI.[144] Dans le cadre de sa compétence en tant qu'autorité de protection des données (DPA) à l'égard de la VSSE et du SGRS, en particulier dans le cadre du traitement des dossiers de plaintes DPA, le Comité est également ponctuellement confronté à cette question.

A travers cette analyse, le Comité souhaitait examiner la manière dont la VSSE organise sa stratégie d'« entrave » en interne. Le Comité s'est concentré sur le cadre réglementaire interne et son adéquation au cadre légal applicable à la VSSE. Le Comité n'a pas examiné comment le service de renseignement civil met en pratique sa théorie de la disruption à ce stade. Bien que celle-ci trouve son origine à la VSSE, l'analyse a également porté sur les conditions auxquelles le SGRS est autorisé à combattre et à entraver les menaces à la sécurité.

L'analyse juridique du Comité et les recommandations qui en découlent ont été transmises aux services de renseignement et ont fait l'objet d'une discussion devant la Commission de suivi au premier trimestre 2023.

144 COMITÉ PERMANENT R, « Enquête de contrôle sur la manière dont la Sûreté de l'État a assuré le suivi de l'imam Mohamed TOJGANI » (voir www.comiteri.be).

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

L'article 35 de la Loi Contrôle prévoit que, dans son rapport d'activités, le Comité « *consacre une attention spécifique aux méthodes spécifiques et exceptionnelles de recueil de données, telles qu'elles ont été visées dans l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité. […] Le rapport indique le nombre d'autorisations accordées, la durée des méthodes exceptionnelles de recueil de données, le nombre de personnes concernées et, le cas échéant, les résultats obtenus* ».

Outre ces méthodes particulières, il existe des méthodes ordinaires pour lesquelles le Comité s'est vu confier une modalité de contrôle spécifique et limitée ou pour lesquelles les services de renseignement sont tenus de fournir au Comité certaines informations susceptibles de l'aider dans sa mission de contrôle régulière. Ces méthodes sont appelées 'méthodes ordinaires plus' par le Comité. Pour certaines d'entre elles, le législateur a prévu qu'un rapport spécifique soit établi à l'attention du Parlement (notamment les méthodes prévues à l'article 16/2 L.R&S). Le Comité a cependant décidé d'évoquer brièvement chacune de ces méthodes.

Il en va de même pour les mesures dites de protection et d'appui qui peuvent être déployées par la Sûreté de l'État (VSSE) et le Service Général du Renseignement et de la Sécurité (SGRS) dans le cadre d'une mission de renseignement. Étant donné que le Comité s'est vu attribuer un certain rôle, ces mesures sont brièvement expliquées dans le présent chapitre.

La réglementation relative aux méthodes particulières, aux 'méthodes ordinaires plus' et aux mesures de protection et d'appui a été modifiée en profondeur à plusieurs reprises en 2022. Deux lois sont à l'origine de ces modifications :

– La Loi du 14 juillet 2022 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité[145]; et

[145] Voir également à ce propos COMITÉ PERMANENT R, *Rapport d'activités 2021*, 144 et suiv. (Chapitre VI.4. Avis concernant l'avant-projet de loi modifiant la loi organique des services de renseignement).

– La Loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités.[146]

Dans cette seconde loi, le Comité s'est encore vu confier un contrôle particulier relatif à la conservation des données. Cet aspect est examiné au point II.5 du présent chapitre.

II.1. LES MÉTHODES PARTICULIÈRES DE RENSEIGNEMENT

II.1.1. UN APERÇU DES PRINCIPALES MODIFICATIONS LÉGISLATIVES EN 2022

Depuis la mi-août 2022, des méthodes spécifiques et exceptionnelles peuvent également être utilisées pour évaluer la fiabilité des sources humaines ou pour assurer leur protection (art. 18 § 2, 18/1, 3° et 18/9 § 1er L.R&S).

En outre, les compétences du SGRS ont été étendues, dans le cadre d'une crise nationale de cybersécurité[147], à la neutralisation d'une cyberattaque de systèmes informatiques et de communications non gérées par le ministre de la Défense nationale et à l'identification des auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect dispositions du droit international (art. 11 § 1er, 2° /1, L.R&S).

En ce qui concerne les méthodes spécifiques à mettre en œuvre, il convient de signaler les modifications suivantes :

– En vertu de la méthode spécifique prévue à l'article 18/7 § 1er, 2°, L.R&S, la VSSE ou le SGRS peut également exiger la communication des factures afférentes aux abonnements identifiés ;
– La possibilité tout à fait nouvelle de s'infiltrer dans le monde virtuel sous couvert d'une identité fictive ou d'une qualité fictive (art. 18/5/1 L.R&S) ;

En ce qui concerne les méthodes exceptionnelles à mettre en œuvre, l'on notera les modifications suivantes :

– En vertu de l'article 18/12/1 L.R&S, les services de renseignement et de sécurité peuvent s'infiltrer dans le monde réel, conformément aux directives du Conseil

146 Voir également à ce propos COMITÉ PERMANENT R, *Rapport d'activités 2021*, 140 et suiv. (Chapitre VI.3. Avis relatif à la rétention des données).

147 Une crise nationale de cybersécurité est un événement de cybersécurité qui, en raison de sa nature ou de ses conséquences, menace les intérêts vitaux du pays ou les besoins essentiels de la population, nécessite une prise de décision urgente et requiert le déploiement coordonné de plusieurs départements et organismes.

national de sécurité. Le Comité n'ayant pas connaissance d'une telle directive, cette méthode ne peut pas encore être utilisée ;
– La réquisition d'informations financières a été élargie, notamment par le renvoi au point de contact central de la Banque nationale de Belgique (art. 18/15 L.R&S).

II.1.2. LES MRD EN CHIFFRES

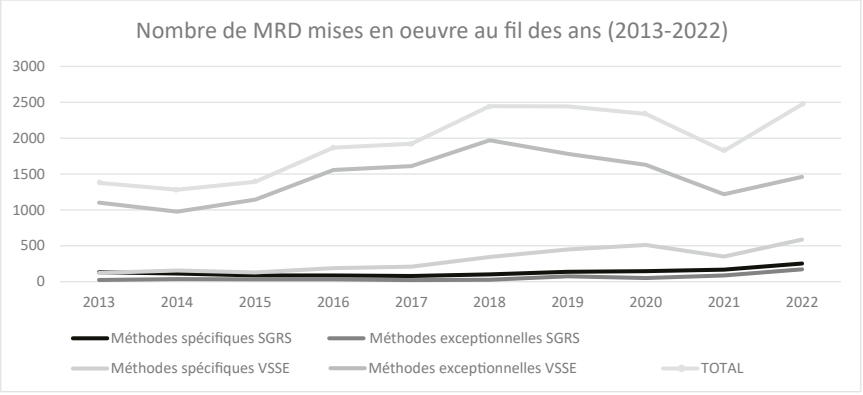
II.1.2.1. Tendance générale

Entre le 1er janvier et le 31 décembre 2022, 2472 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 2047 par la VSSE (dont 1460 spécifiques et 587 exceptionnelles) et 425 par le SGRS (dont 253 spécifiques et 172 exceptionnelles). Nonobstant le léger rattrapage une nouvelle fois constaté, la VSSE se taille encore la part du lion (environ 83 %) dans la mise en œuvre des méthodes particulières de renseignement.

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

	SGRS		VSSE		TOTAL
	Méthodes spécifiques	**Méthodes exceptionnelles**	**Méthodes spécifiques**	**Méthodes exceptionnelles**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445
2019	138	76	1781	449	2444
2020	146	51	1629	511	2337
2021	166	87	1220	350	1823
2022	253	172	1460	587	2472

Cela donne schématiquement :



Il ressort de ces chiffres que la baisse significative constatée en 2021 a été complètement inversée. Les chiffres globaux en termes de MRD reviennent aux niveaux de 2019-2020. Une ventilation des chiffres montre la poursuite de l'augmentation des méthodes spécifiques mises en œuvre par le SGRS en 2020 (de 166 en 2021 à 253 en 2022). On note également une augmentation extrêmement forte du nombre de méthodes exceptionnelles utilisées par le SGRS, même par rapport à 2019-2020 : il fait plus que doubler (de 87 à 172). Un mouvement similaire se dessine à la VSSE : le nombre de méthodes spécifiques déployées augmente de manière constante (de 1220 en 2021 à 1460 en 2022), mais l'augmentation est particulièrement notable en ce qui concerne le nombre de méthodes exceptionnelles (de 350 en 2021 à 587 en 2022).

II.1.2.2. Méthodes utilisées par le SGRS

Les méthodes spécifiques

Méthodes spécifiques (SGRS)	Nombre d'autorisations 2021	Nombre d'autorisations 2022
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)	12	38
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	1
S'infiltrer dans le monde virtuel sous couvert d'un faux nom ou d'une fausse qualité (art. 18/5/1 L.R&S)	NA	NA

Méthodes spécifiques (SGRS)	Nombre d'autorisations 2021	Nombre d'autorisations 2022
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 (art. 18/7 § 1er, 1° L.R&S)	6	12
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 § 1er, 2° L.R&S)	0	2
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 § 1er, 1°L.R&S)	75	100
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 § 1er, 2° L.R&S)	73	100
TOTAL	**166**	**253**

En ce qui concerne les méthodes spécifiques, ce sont le 'repérage des données d'appel d'un trafic de communications électroniques' (art. 18/8, § 1er, 1° L.R&S) et la 'prise de connaissance de données de localisation d'un trafic de communications électroniques' (art. 18/8, § 1er, 2° L.R&S) qui constituent la majorité des méthodes mises en œuvre. Comme toujours, ces méthodes, qui sont généralement déployées ensemble, ont remporté la palme (200 sur 253 méthodes spécifiques déployées). Par ailleurs, les observations dans des lieux accessibles au public à l'aide d'un moyen technique ont été trois fois plus nombreuses qu'en 2021 (de 12 à 38 en 2022).

Selon le SGRS, un certain nombre de méthodes n'ont pas été mises en œuvre par manque de personnel. En outre, le service a constaté qu'un certain nombre de méthodes spécifiques n'étaient pas suffisamment connues du personnel et, par conséquent, pas suffisamment utilisées. Pour y remédier, des briefings internes ont été organisés début 2022.

Les méthodes exceptionnelles

Méthodes exceptionnelles (SGRS)	Nombre d'autorisations 2021	Nombre d'autorisations 2022
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)	3	20
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)	2	10
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	2	4
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	8	19
S'introduire dans un système informatique (article 18/16 L.R&S)	14	24
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	60	95
TOTAL	**89**	**172**

On constate une hausse significative du nombre de méthodes exceptionnelles mises en œuvre par le SGRS. La forte augmentation en pourcentage (presque un doublement) s'explique essentiellement par l'augmentation du nombre d'intrusions dans un système informatique (art. 18/16 L.R&S) (de 14 en 2021 à 24 en 2022) et du nombre d'écoutes, de prises de connaissance et d'enregistrements de communications (art. 18/17 L.R&S) (de 60 en 2021 à 95 en 2022). De même, la méthode consistant à inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public et à inspecter le contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S) a connu une forte augmentation (de 2 à 10). La méthode exceptionnelle consistant à recourir à une personne morale afin de collecter des données (art. 18/13 L.R&S) n'a encore jamais été utilisée par le SGRS depuis l'entrée en vigueur de la Loi de 2010. En 2016, le même constat était déjà posé et expliqué par le fait que « *la procédure de création est trop lourde pour la mettre en œuvre pour un seul dossier* ».[148]

Le Comité a rappelé au SGRS l'obligation d'informer la Commission BIM toutes les deux semaines de la mise en œuvre de ces méthodes exceptionnelles (art. 18/10 § 1er, alinéa 3 L.R&S et art. 9 A.R. du 12 octobre 2010).[149] Une réunion

148 Exposé des motifs du projet de loi modifiant la loi du 30 novembre 1998, *Doc. Parl.*, Chambre, 2015-2016, n°54-2043/001, 11.

149 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 109, ('XII.II.3.3. Obligation d'information dans le cadre des méthodes exceptionnelles').

dite 'de quinzaine' a alors été mise en place. Les mesures sanitaires imposées dans le cadre de la crise sanitaire ont empêché la tenue de ces réunions. Elles ont repris au printemps 2022. Cela a permis de formaliser un meilleur suivi qualitatif des dossiers, tant par la Commission BIM que par le Comité permanent R.

Les missions et les menaces justifiant le recours aux méthodes ordinaires et particulières[150]

Le SGRS est autorisé à utiliser les méthodes spécifiques et exceptionnelles dans le cadre de six missions, compte tenu de différentes menaces.

1. La mission de renseignement (art. 11, 1° L.R&S)
   Le recueil, l'analyse et le traitement du renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir. Le recueil, l'analyse et le traitement du renseignement relatif à toute activité qui menace ou pourrait menacer les intérêts suivants :
   – l'intégrité du territoire national ou la survie de tout ou partie de la population ;
   – les plans de défense militaires ;
   – le potentiel économique et scientifique en rapport avec la défense ;
   – l'accomplissement des missions des Forces armées ;
   – la sécurité des ressortissants belges à l'étranger.
2. Veiller au maintien de la sécurité militaire (art. 11, 2° L.R&S)
   – la sécurité militaire du personnel relevant du ministre de la Défense nationale ;
   – les installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires ;
   – dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense 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 neutralisation, dans le cadre d'une crise nationale de cybersécurité, une cyberattaque de systèmes informatiques et de communications non gérés par le ministre de la Défense et l'identification des auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit international (art. 11 § 1er, 2° /1, L.R&S).

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

4. 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.
5. 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).
6. L'évaluation de la fiabilité des sources humaines ou de l'assurance de leur protection (art. 18 § 2, 18/1, 3° en 18/9 § 1er L.R&S).

Depuis 2017, la mise en œuvre de méthodes particulières n'est plus limitée au territoire belge (art. 18/1, 2° L.R&S). Cette possibilité n'a encore jamais été utilisée. Elle a toutefois été inscrite dans la loi parce que le SGRS la considérait comme une nécessité pour lui permettre de mener à bien ses missions à l'étranger (en particulier les missions mandatées par le Conseil de sécurité des Nations Unies).[151] Un examen plus approfondi doit permettre de déterminer si le SGRS n'a effectivement pas utilisé de méthodes MRD à l'étranger – ce qui annihilerait l'argument de l'exposé des motifs visant à modifier le champ d'application territorial des méthodes MRD – ou si le SGRS utilise des méthodes MRD à l'étranger sans pour autant recourir à la procédure MRD obligatoire. Le Comité vérifiera en 2023 si le SGRS utilise exclusivement la réglementation INT décrite à l'article 44 L.R&S. Cette initiative s'inscrit dans la philosophie de l'exposé des motifs de la Loi de 2017 qui stipule que *« Dans cinq ans, il sera procédé à une nouvelle évaluation de la situation pour voir si les prérogatives en faveur du SGRS sont praticables à l'étranger et si elles couvrent suffisamment les mandats des Nations Unies »*.

De même, aucune méthode particulière de renseignement n'a été mise en œuvre à la demande des services partenaires étrangers.[152] Cependant, selon le SGRS, les informations reçues des services étrangers peuvent être le déclencheur direct de la mise en œuvre d'une méthode particulière de renseignement.

La pratique montre que plusieurs menaces peuvent figurer dans une même autorisation. On peut constater une diminution de MRD mises en œuvre dans le cadre de la menace 'ingérence et organisations criminelles'. Il convient de noter la forte augmentation du nombre de méthodes exceptionnelles déployées dans le cadre de la menace 'espionnage' (de 120 en 2021 à 309 en 2022).

---

151 Exposé des motifs, *Doc. parl.* Chambre 2015-16, 54-2043/001.

152 Cela a parfois été le cas pour la mise en œuvre de 'méthodes ordinaires plus'(mais seulement s'il existe également une utilité identifiable pour le SGRS lui-même).

NATURE DE LA MENACE	NOMBRE EN 2021	NOMBRE EN 2022
Espionnage	120	309
Ingérence	16	4
Extrémisme	82	95
Terrorisme	9	0
Organisations criminelles	26	16
Autre	0	1
TOTAL	**253**	**425**

II.1.2.3. Méthodes utilisées par la VSSE

Les méthodes spécifiques

Méthodes spécifiques (VSSE)	Nombre d'autorisations 2021	Nombre d'autorisations 2022
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)	195	231
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)	33	23
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 (art. 18/7 § 1er, 1° L.R&S)	22	39
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 §1, 2° L.R&S)	2	3
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)	491	595

Méthodes spécifiques (VSSE)	Nombre d'autorisations 2021	Nombre d'autorisations 2022
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)	477	567
TOTAL	**1220**	**1460**

La forte baisse du nombre de méthodes spécifiques en 2021 s'est inversée, sans toutefois atteindre le niveau de 2020 avec 1629 autorisations. On constate une augmentation dans presque toutes les méthodes spécifiques.

Les méthodes exceptionnelles

Méthodes exceptionnelles (VSSE)	Nombre d'autorisations 2021	Nombre d'autorisations 2022
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	37
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)	11	23
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	13	22
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	73	108
S'introduire dans un système informatique (article 18/16 L.R&S)	61	67
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	192	330
TOTAL	**363**	**587**

À l'instar des méthodes spécifiques, le nombre de méthodes exceptionnelles déployées par la VSSE a connu une augmentation (de 363 en 2021 à 587 en 2022).

Les missions et les menaces justifiant le recours aux méthodes particulières

Le tableau suivant montre dans quel contexte de menaces (potentielles) la VSSE a mis en œuvre des méthodes spécifiques et exceptionnelles. Une méthode peut naturellement viser plusieurs menaces. La VSSE peut utiliser les méthodes spécifiques dans le contexte de toutes les menaces relevant de sa compétence (art. 8 L.R&S).

Il arrive que la menace potentielle ne soit pas connue à l'avance. C'est le cas, par exemple, lorsqu'il s'agit d'évaluer la fiabilité des sources humaines ou d'assurer leur protection (art. 18 § 2, 18/1, 3° et 18/9 § 1er 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 2021	NOMBRE EN 2022
Espionnage	478	612
Ingérence	121	325
Extrémisme	279	362
Prolifération	2	4
Organisations sectaires nuisibles	0	0
Terrorisme	690	715
Organisations criminelles	0	29
Suivi des activités des services étrangers en Belgique	(inclus dans les chiffres ci-dessus)	(inclus dans les chiffres ci-dessus)
TOTAL	**1570**	**2047**

Concernant la mise en œuvre de méthodes MRD en 2022, le tableau repris ci-dessus montre que la menace 'terrorisme' a légèrement augmenté (de 690 en 2021 à 715 en 2022) et demeure la priorité absolue de la VSSE, suivie par la menace 'espionnage' (612). Alors qu'en 2020, il était encore question d'une forte diminution du nombre de dossiers 'ingérence', une forte augmentation peut à nouveau être constatée (de 121 en 2021 à 325 en 2022). Dans la pratique, il n'est cependant pas toujours évident d'établir une distinction entre l'espionnage (recueillir clandestinement des données) et l'ingérence (influencer des processus décisionnels). La menace 'extrémisme-radicalisme' a également augmenté de manière remarquable (de 279 dossiers en 2021 à 362 dossiers en 2022). La menace 'organisations criminelles' réapparaît également dans les chiffres (29).[153]

Au niveau de la territorialité, la VSSE est autorisée à mettre œuvre des MRD *'sur et à partir du territoire du Royaume'* (art. 18/1, 1er L.R&S). Comme pour le

[153] *Ann.* Chambre, Commission commune Affaires Intérieures et Justice, 2022-2023, 24 octobre 2022, 10-11 (compte rendu intégral n° CRIV 55 COM 913).

SGRS, aucune méthode particulière de renseignement n'a été déployée à l'étranger par la VSSE. Le déploiement de telles méthodes en Belgique à la demande de services partenaires étrangers est également négligeable. Toutefois, sur la base d'informations reçues des services partenaires, il a été décidé de mettre en œuvre des méthodes particulières de renseignement.

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.
4. L'évaluation de la fiabilité des sources humaines ou de l'assurance de leur protection (art. 18 § 2, 18/1, 3° et 18/9 § 1er L.R&S).

Comme le SGRS, la VSSE combine plusieurs intérêts. On peut néanmoins mentionner que la 'sauvegarde des éléments essentiels du potentiel économique et scientifique' est un intérêt qui mobilise peu.

Pour rappel, 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.1.3. LE CONTRÔLE EXERCÉ PAR LE COMITÉ PERMANENT R

II.1.3.1. Les chiffres

Cette section porte sur le contrôle juridictionnel exercé par le Comité permanent R sur les méthodes de renseignement spécifiques et exceptionnelles. 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.

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 l'Autorité de protection des données (APD) ;
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 la base de l'article 18/10, § 3 L.R&S.

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

TYPE DE SAISINE	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
1. D'initiative	16	12	16	3	1	1	4	2	1	5
2. Autorité de protection des données	0	0	0	0	0	0	0	0	0	0
3. Plainte	0	0	0	1	0	0	0	0	0	0
4. Interdiction d'exploitation par la Commission BIM	5	5	11	19	15	10	12	9	8	9
5. Autorisation du ministre	2	1	0	0	0	0	0	0	0	0
6. Auteur d'avis préjudiciel	0	0	0	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**	**9**	**14**

Le nombre de décisions prises par le Comité est en hausse pour la première fois en deux ans, suite à l'augmentation du nombre de méthodes MRD. Les saisines sont passées de 9 à 14 et les méthodes ont augmenté de 650 unités entre 2021 et 2022. Il est à noter que l'augmentation du nombre de saisines et de méthodes est proportionnelle. La plupart des saisines sont cependant le résultat d'une suspension ordonnée par la Commission BIM (9 sur 14 saisines).

Une fois saisi, le Comité peut prendre plusieurs types 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	2014	2015	2016	2017	2018	2019	2020	2021	2022
Décisions préalables à la saisine									
1. Plainte frappée de nullité	0	0	0	0	0	0	0	0	0
2. Plainte manifestement non fondée	0	0	0	0	0	0	0	0	0
Décisions intermédiaires									
3. Suspension de la méthode	3	2	1	0	0	0	1	0	0
4. Information complémentaire de la Commission BIM	0	0	0	0	0	0	0	0	0
5. Information complémentaire du service de renseignement	1	1	4	0	0	0	1	1	2
6. Mission d'enquête confiée au Service d'Enquêtes R [154]	54	48	60	35	52	52	24	33	40
7. Audition des membres de la Commission BIM	0	2	0	0	0	0	0	0	0
8. Audition de membres des services de renseignement	0	2	0	0	0	1	1	0	0

[154] Le Comité demande au Service d'Enquêtes d'effectuer des recherches complémentaires et/ou de contacter le service concerné ou la Commission BIM.

9. Décision relative au secret de l'instruction	0	0	0	0	0	0	0	0	0
10. Informations sensibles lors de l'audition	0	0	0	0	0	0	0	0	0
Décisions finales									
11. Cessation de la méthode	3	3	6	9	4	11	10	5	9[155]
12. Cessation partielle de la méthode	10	13	4	6	6	4	0	3	3
13. Levée (partielle) de l'interdiction de la Commission BIM	0	4	11	0	0	0	0	0	0
14. Non compétent	0	0	0	0	0	0	0	0	0
15. Autorisation légale/Non-cessation de la méthode/Non-fondement	4	6	2	1	1	0	0	1	2
Avis préjudiciels									
16. Avis préjudiciel	0	0	0	0	0	0		0	0

II.1.3.2. La jurisprudence

La substance des décisions finales prises en 2022 par le Comité permanent R dans le cadre de son rôle juridictionnel en matière de contrôle des méthodes particulières de renseignement 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.

Photographies d'un lieu clos

Lors de la relecture d'un rapport d'observation à la suite de la mise en œuvre d'une méthode ordinaire, il est apparu que des photographies du jardin de l'intéressé avaient été prises et qu'une méthode spécifique aurait donc dû être demandée en vertu de l'article 18/4 L.R&S. Il s'agissait en effet de '*een woning met tuin die afgesloten is met een niet doorzichtige*

[155] Dans deux décisions, le Comité a soutenu la décision de la Commission BIM qui n'avait pas émis d'avis conforme sur un projet de décision de mise en œuvre d'une méthode exceptionnelle. Le Comité n'a pas décidé *stricto sensu* de mettre fin à la méthode puisque le service de renseignement concerné ne l'avait finalement pas autorisée.

omheining'. '*Enkele gemaakte foto's tonen aanwezige voorwerpen in de tuin die boven de omheining uitsteken*'[156], mais '*[d]eze voorwerpen zijn zichtbaar vanop de openbare weg, zonder hiervoor kunstgrepen te moeten uitvoeren*'.[157] Le Comité a fait valoir qu'il '*est incontestable que l'observation effectuée ne pouvait l'être que sur la base d'une BIM prise en vertu de l'article 18/4 §2 L.R&S, ce qui ne fut aucunement le cas, par défaut même de mise en œuvre d'une quelconque procédure BIM*'. Par conséquent, la méthode n'était pas légale (2021/11081).

Une erreur matérielle

Un service de renseignement souhaitait obtenir des informations sur la localisation en temps réel d'une cible par le biais de son numéro de GSM (2022/11294). Cependant, lors du lancement de cette méthode, un document erroné a été envoyé à la Commission BIM. Il s'agissait d' '*een niet-finale versie*'[158] qui contenait encore des '*ettelijke fouten met betrekking tot de gevraagde periode en de gevraagde gegevens*'[159]. Lorsque le service de renseignement s'en est aperçu, il a mis fin à la méthode. La Commission BIM a procédé à la suspension de la méthode et le Comité permanent R a ensuite constaté le non-respect des exigences légales.

Méthodes particulières en appui des interventions d'urgence à la suite d'inondations majeures

En réponse aux très graves inondations qui ont touché notre pays en juillet 2021, le service de renseignement militaire a décidé de procéder en urgence à la mise en œuvre de la méthode spécifique visée à l'article 18/3, § 3 et de la méthode exceptionnelle visée à l'article 18/11, § 1er L.R&S. En effet, le service souhaitait utiliser les images d'un système satellitaire, dont il est l'unique exploitant belge, dans le cadre de l'aide d'urgence. Il s'agissait évidemment de prendre des images de lieux accessibles au public et de lieux non accessibles au public mais soustraits à la vue, ainsi que de personnes et d'objets qui s'y trouvaient ou d'événements qui s'y déroulaient. Le Comité s'est saisi de ces dossiers (2021/10787 et 2021/10788) et a conclu, sur la base des éléments repris ci-dessous, que les méthodes spécifiques et exceptionnelles autorisées étaient légales, subsidiaires et proportionnelles.

Tout d'abord, le Comité a constaté que, sur la base des dispositions légales en question, des lieux pouvaient faire l'objet d'une méthode spécifique ou

---

156 '*une habitation dont le jardin est entouré d'une clôture non transparente.*' '*Certaines photos montrent des objets présents dans le jardin et qui dépassent de la clôture.*' (traduction libre).

157 '*Ces objets sont visibles de la voie publique, sans qu'il soit nécessaire de recourir à des artifices.*' (traduction libre).

158 '*une version non définitive*' (traduction libre).

159 '*plusieurs erreurs portant sur la période et les données requises*' (traduction libre).

exceptionnelle, sans qu'aucune restriction spatiale ne lui soit associée, compte tenu du respect des principes de proportionnalité.

La méthode spécifique concernait l'observation de lieux non accessibles au public et non soustraits à la vue. L'article 3, 12°/1 L.R&S décrit la notion de : « *lieu non accessible au public non soustrait à la vue* : *tout lieu auquel le public n'a pas accès et qui est visible de tous à partir de la voie publique sans moyen ou artifice, à l'exception de l'intérieur des bâtiments non accessibles au public* ». Cette notion inclut donc les dépendances des habitations (par exemple, les jardins soustraits à la vue par une haute haie). Le Comité a établi que le système satellitaire pouvait être qualifié de moyen technique au sens de l'article 3, 12°/1 L.R&S. Ce n'était toutefois nullement le cas dans le présent dossier, les images n'étant pas suffisamment détaillées.

En outre, le Comité a fait valoir que ni l'article 18/4, §§ 1er et 2 L.R&S, ni l'article 18/11, § 1er L.R&S ne précise la manière dont une observation doit se dérouler. Et le Comité d'ajouter que la collecte d'informations s'inscrivait dans le cadre de l'assistance nationale confiée aux Forces armées par la ministre de la Défense. Ce mandat était basé sur diverses dispositions légales.[160] Le Comité a également constaté que le déploiement du SGRS était fondé sur les articles 11, § 1er, 1° *in limine*, 13, alinéa 1er et 18/1, 2° L.R&S et sur l'article 35/1 de l'Arrêté royal du 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attritions de certaines autorités. La prise de photos satellites par le SGRS s'inscrivait donc dans le contexte d'une mission concrète d'appui en matière de renseignement à une opération militaire nationale en cours. L'exigence de subsidiarité a également été respectée, car les méthodes ordinaires et spécifiques n'ont pas suffi à obtenir les informations nécessaires. Il en va de même pour l'exigence de proportionnalité : compte tenu de la gravité et de l'étendue des dommages causés par les inondations et des dommages potentiels qui pouvaient encore en résulter, le Comité a estimé que l'utilisation des méthodes était proportionnée.

Une méthode sur un numéro erroné

Quelques mois après le lancement de la méthode spécifique impliquant la recherche de certaines données du trafic entrant et sortant d'un GSM, le service de renseignement concerné a constaté que le numéro ciblé avait été communiqué de manière erronée. Le service a mis fin à la méthode et a conservé séparément les données déjà collectées. La Commission BIM a été informée et a suspendu la

160 Art. 3, § 1er, 2°, b) de la Loi du 20 mai 1994 'relative aux périodes et aux positions des militaires du cadre de réserve, ainsi qu'à la mise en œuvre et à la mise en condition des Forces armées'; Art. 186, alinéa 4 de la Loi du 28 février 2007 'fixant le statut des militaires et candidats militaires du cadre actif des Forces armées'; Art. 6/1, alinéa 1er, 1°, et 6/2 de l'Arrêté royal du 6 juillet 1994 'portant détermination des formes d'engagement opérationnel, d'assistance et d'appui militaire, et des activités préparatoires en vue de la mise en œuvre des Forces armées'.

méthode, suspension que le Comité a confirmée. La méthode a été définitivement arrêtée et les données collectées ont dû être détruites (2021/11060).

Questions sur la proportionnalité d'une méthode mise en œuvre

Un service de renseignement souhaitait savoir si l'un des GSM appartenant officiellement à un membre de la famille de la cible n'était pas utilisé par ce dernier. Pour ce faire, le service voulait vérifier les données de trafic et de localisation de ces appareils sur une période de 12 mois. La Commission BIM a suspendu la méthode et a transmis le dossier pour décision au Comité, qui a estimé que la période de 12 mois n'était pas proportionnelle. Le Comité a établi que '*een periode van 2 maanden […] aangewezen lijkt*'[161]. Et le Comité d'ajouter que si nécessaire, cette période pouvait être prolongée par la suite. (2022/11256).

L"utilisation d'une méthode en dehors des limites de la décision

Un service de renseignement a décidé d'observer un bâtiment donné pendant six mois à compter de la notification de la décision à la Commission BIM. Le dispositif mis en place a toutefois continué à prendre des images pendant plusieurs jours. Le Comité a dès lors estimé que ces images n'étaient pas couvertes par la décision, qu'elles ne pouvaient pas être exploitées et qu'elles devaient être détruites (2022/10587).

Une erreur matérielle

Un service de renseignement voulait savoir, via une méthode exceptionnelle, quelles applications une cible utilisait et quels sites elle consultait avec son GSM. Cependant, lors de la mise en œuvre de la méthode, le service a procédé par erreur à la prise de connaissance du contenu de conversations. Il est intervenu dès qu'il s'est aperçu de l'erreur. La Commission BIM a été contrainte de suspendre la méthode et a ainsi saisi le Comité. Celui-ci a déclaré illégale la consultation du contenu et a ordonné la destruction des données obtenues illégalement (2022/11419).

L'utilisation insuffisamment différenciée d'une méthode spécifique

Un service de renseignement entendait obtenir les données téléphoniques de plusieurs dizaines de personnes répertoriées par l'OCAM comme répondant à un critère de menace bien défini. Le service de renseignement affirmait avoir besoin de ces données pour, entre autres, compléter les informations dont il disposait déjà

[161] '*une période de deux mois semble indiquée*' (traduction libre).

sur ces personnes. Ces données, qui donnent une image des contacts entretenus par les cibles, peuvent démontrer si la personne a toujours un profil problématique et si elle peut être engagée dans des activités menaçantes. En vertu de l'article 18/3, § 4 L.R&S, dans toute décision doivent figurer '*les circonstances de fait qui justifient la méthode spécifique, la motivation en matière de subsidiarité et de proportionnalité, en ce compris le lien entre*' les personnes et les menaces potentielles qui sont visées. Dans le cas spécifique, cependant, la motivation s'est en grande partie limitée à la référence aux critères d'inscription sur la liste de l'OCAM, alors qu'il s'agit d'une liste dynamique. '*Les prescrits de la Loi organique du 30 novembre 1998 […] imposent aux services d'individualiser toutes motivations dans le cadre de la mise en œuvre des méthodes spécifiques décidées (ou autres envisagées), ce tant au niveau du lien à effectuer entre la menace ciblée et l'individu concerné qu'au niveau de la subsidiarité et de la proportionnalité des mesures spécifiques décidées (ou autres envisagées).*' Outre le fait que la décision ne contenait aucune individualisation et n'apportait donc aucune précision particulière et concrète sur les intéressés, il est apparu que certaines personnes figuraient sur une liste établie sur la base d'un critère de menace différent. Se ralliant à l'avis de la Commission BIM, le Comité a conclu '*une insuffisance de justification voire un manque de contextualisation concernant la menace évoquée et une insuffisance de motivation concernant les liens à effectuer entre une telle menace potentielle et les personnes ciblées ainsi que concernant les éléments de proportionnalité*' (dossier 2022/11532).

Un problème de proportionnalité et de subsidiarité

L'introduction d'une plainte d'un fonctionnaire auprès du Comité a donné lieu à l'ouverture d'une enquête. Celle-ci a révélé que le service concerné avait ouvert une enquête de renseignement contre le fonctionnaire à la demande de l'employeur. À juste titre, puisqu'il y avait un risque de radicalisme au sens de la loi sur le renseignement. Mais il est rapidement apparu qu'une enquête plus approfondie n'était plus proportionnée. L'utilisation d'une méthode spécifique ne se justifiait donc plus à ce moment-là : '*il n'y avait pas de menace(s) imminente(s) nécessitant de procéder à quelconque enquête telle qu'effectuée et de mettre en œuvre les méthodes de recueil de données, l'une ordinaire et l'autre particulière - spécifique*'. Le Comité a établi que '*le principe de subsidiarité quant à la méthode particulière - spécifique - ainsi que sa finalité n'ont pas été respectés*', car certaines allégations contenues dans la décision BIM étaient manifestement erronées et n'étaient pas fondées sur les informations antérieures dont disposait le service. La méthode a dès lors été déclarée illégale (2019/8823).

Encore une erreur matérielle

Le lendemain du jour où un service de renseignement a procédé, via une méthode spécifique et exceptionnelle, à la prise de connaissance et à l'interception des communications passant par un GSM donné, il est apparu que l'un des trois opérateurs dont le concours a été requis s'était basé sur un numéro IMEI erroné. L'erreur a été immédiatement corrigée, mais les données de ce premier jour n'étaient naturellement pas couvertes par un mandat. La Commission BIM a suspendu la méthode sur ce point et le Comité a confirmé cette illégalité. Toutefois, un problème s'est posé lors de la destruction des données collectées via la méthode exceptionnelle. En effet, ces données étaient contenues dans un seul document, si bien qu'il n'était plus possible de déterminer quel fournisseur avait fourni quelles données. Par conséquent, le Comité a décidé : '*qu'en ce qui concerne les seules data, il appert, prima facie, qu'une discrimination ne pourrait être réalisée entre les data recueillies et transmises par les trois opérateurs, celles-ci étant reprises sur un document unique de synthèse sans possibilité d'identification des opérateurs les ayant recueillies. Il conviendrait, dès lors et en pareil cas, d'en interdire purement et simplement leur exploitation et de les faire détruire sans autre forme de procès (…).*' (2022/11825 et 2022/11826).

II.2. LA MISE EN ŒUVRE DES 'MÉTHODES ORDINAIRES PLUS' ET LE CONTRÔLE DE CELLES-CI

À l'origine, les méthodes ordinaires de renseignement étaient uniquement soumises au contrôle régulier du Comité. Toutefois, depuis plusieurs années, la loi sur le renseignement prévoit des méthodes ordinaires pour lesquelles le Comité est chargé d'une mission de contrôle particulière et/ou pour lesquelles le service de renseignement concerné se voit imposer une obligation supplémentaire de fournir des informations au Comité (ce que l'on appelle les 'méthodes ordinaires plus'). L'obligation de contrôle ou d'information est réglementée différemment pour chacune de ces méthodes, et ce, malgré le plaidoyer du Comité en faveur d'une uniformisation de cette obligation.[162]

[162] Cette division s'avère trop théorique pour certains et ne tient pas suffisamment compte de la réalité. Voir par exemple W. VAN LAETHEM, 'Enkele reflecties over tien jaar BIM-controle door het Vast Comité I', in VANDERBORGHT, J. (ed.), *o.c.*, 70-72. Adoptant un point de vue similaire, le Comité a cité, à titre d'exemple, l'article 16/3 L.R&S (collecte et traitement des données des passagers) et 16/4 L.R&S (collecte et traitement des images des caméras de police). Bien que ces deux pouvoirs d'enquête soient considérés comme des méthodes ordinaires, l'ingérence dans la vie privée dans ces méthodes est souvent plus importante que dans certaines méthodes de renseignement spécifiques, voire exceptionnelles. C'est certainement le cas de l'utilisation de caméras lorsque des caméras intelligentes ou des logiciels tels que l'ANPR sont utilisés. Voir COMITÉ PERMANENT R, Avis n° 001/CPR/2021 du 12 juillet 2021 (Modifications Loi sur le renseignement). Cet avis peut être consulté sur www.comiteri.be.

II.2.1. L'IDENTIFICATION DE L'ABONNÉ OU DE L'UTILISATEUR HABITUEL D'UN SERVICE OU D'UN MOYEN DE TÉLÉCOMMUNICATION (ART. 16/2 L.R&S)

L'identification de l'abonné ou de l'utilisateur habituel d'un service ou d'un moyen de télécommunication (par ex. un numéro de gsm ou une adresse IP[163]) est une méthode ordinaire lorsqu'elle est mise en œuvre via une réquisition adressée à un opérateur ou à un fournisseur de télécommunications ou via l'accès direct aux fichiers de leurs clients.[164] La réglementation prévoit l'obligation pour les services de renseignement de conserver un registre de toutes les identifications demandées et de toutes les identifications obtenues par accès direct.[165]

SGRS	Nombre d'autorisations 2021	Nombre d'autorisations 2022
Identification de l'abonné ou de l'utilisateur habituel' de télécommunications	420	601

VSSE	Nombre d'autorisations 2021	Nombre d'autorisations 2022
Identification de l'abonné ou de l'utilisateur habituel' de télécommunications	4080	5310

En ce qui concerne cette méthode, la loi n'a pas introduit de contrôle spécifique. Il était seulement stipulé que le Comité doit recevoir chaque mois la liste des identifications requises et des accès directs. Or, le Comité ne reçoit que le nombre de réquisitions. Le Comité s'est engagé à contrôler chaque année un échantillon de réquisitions.[166] Ce contrôle est effectué mensuellement. Il réclame parfois des compléments d'information de la part des services.

---

163 À partir de 2022, le nombre de réquisitions est également subdivisé en 'réquisitions IP' et 'réquisitions non IP'.

164 Lorsque l'identification se fait à l'aide d'un moyen technique (et donc pas via une réquisition adressée à un opérateur), la collecte reste une méthode spécifique (art. 18/7 § 1er L.R&S).

165 La possibilité créée à l'article 16/2, § 1er, dernier alinéa L.R&S pour les services de renseignement de requérir de telles données d'identification par le biais d'un accès direct aux fichiers clients des opérateurs et fournisseurs de télécommunications n'a pas eu d'effet jusqu'à présent.

166 COMITÉ PERMANENT R, *Rapport d'activités* 2017, 25, note de bas de page n°41. Ce contrôle a débuté en 2020. Le Comité a décidé d'inclure cette thématique dans l'enquête de contrôle qu'il a ouverte en 2019 sur l'application et le contrôle interne par les services de renseignement des méthodes et instruments qui venaient d'être introduits ou adaptés par le législateur et pour lesquels le Comité permanent R s'est vu confier un rôle de contrôle particulier.

En 2022, cette réglementation a été modifiée en ce sens que la VSSE et le SGRS peuvent également procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques en requérant le concours :

– des personnes ou institutions visées à l'article 5, § 1er, alinéa 1er, 3° à 22° de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces et des personnes ou institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec les valeurs virtuelles permettant d'échanger des moyens de paiement réglementés en valeurs virtuelles, sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée par un opérateur ou un fournisseur ;
– des autres personnes morales qui sont l'abonné d'un opérateur ou d'un fournisseur visé au paragraphe 1er ou qui souscrivent au nom et pour le compte de personnes physiques à un service de communications électroniques, sur la base des données qui ont été préalablement communiquées par un opérateur ou un fournisseur.

II.2.2. L'ACCÈS AUX DONNÉES PNR DE BELPIU (ART. 16/3 L.R&S ET ART. 27 DE LA LOI DU 25 DÉCEMBRE 2016)

Début 2017[167], la possibilité pour les services de renseignement d'accéder aux informations détenues par l'Unité d'Information des Passagers (BELPIU) via des 'recherches ciblées' a été mise en place. L'accès ne peut être accordé qu'après décision du dirigeant du service et *'de façon dûment motivée'*. Le Comité doit être informé et *'interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans des conditions qui ne respectent pas des dispositions légales'*. Aucune interdiction de ce type n'a été prononcée par le Comité en 2022.

La réglementation PNR permet également de réaliser une 'évaluation préalable', qui implique, d'une part la vérification automatique des données PNR saisies en regard des listes de noms ou des fichiers des services de renseignement et, d'autre part, la transmission d'informations sur la base des *'hits'* validés (art. 24 Loi PNR).

[167] Loi du 25 décembre 2016 (*M.B.* 25 janvier 2017).

Le Comité ne dispose d'aucune compétence particulière en la matière.

SGRS	Nombre d'autorisations 2021	Nombre d'autorisations 2022
Recherches ciblées de données PNR	29	33[168]

VSSE	Nombre d'autorisations 2021	Nombre d'autorisations 2022
Recherches ciblées de données PNR	98	221

Le recours aux recherches ciblées est en constante augmentation, en particulier à la VSSE. Le nombre d'autorisations pour des recherches ciblées dans les données des dossiers passagers (PNR) (art. 16/3 L.R&S) a plus que doublé (de 98 à 221). L'utilité de cette méthode ne cesse de croître, car le nombre de compagnies aériennes qui ont été intégrées a lui aussi augmenté de manière exponentielle.[169] [170]

II.2.3. L'UTILISATION DES IMAGES DES CAMÉRAS DE POLICE (ART. 16/4, § 2 L.R&S)

Les services de renseignement peuvent utiliser les images des caméras de police dans des conditions strictes. Ce faisant, le Comité s'est vu accorder des modalités

168 Les chiffres issus du rapport annuel 2022 du NTTC (National Travel Targeting Center) (p. 17) diffèrent légèrement : *« [n]otons également que les différentes sections du SGRS ont sollicité à 34 reprises le BelPIU pour effectuer des recherches historiques et que la VSSE a utilisé la même méthode 229 fois »*.

169 BelPIU affirme entre-temps approcher un taux de couverture de 100 %.

170 Toujours dans le rapport annuel 2022 du NTCC (p. 17), il est également constaté que *« [l]'année 2022 a vu une croissance de la collaboration entre la VSSE et le SGRS au sein du BelPIU. Concrètement, cela signifie que de nombreuses méthodes ont été partagées durant l'année et qu'en conséquence les résultats d'un service peuvent se retrouver comptabilisé dans les statistiques d'un autre. À cet égard, nous constatons que tous les chiffres sont en augmentation, tant du côté des sollicitations par les services que du côté des résultats engendrés. Ainsi, les cross matchs avec les bases de données ont généré 2.617 résultats pour le SGRS et 3.015 pour la VSSE et les listes de critères du SGRS ont généré 8.277 occurrences positives et celles de la VSSE en ont généré 4.473 ; ce qui représente un doublement des résultats par rapport à l'année précédente »*.

de contrôle particulières : un contrôle *a priori* [171] et un contrôle *a posteriori*.[172] [173] Une légère augmentation a été constatée en 2022.

SGRS	Nombre d'autorisations 2021	Nombre d'autorisations 2022
Utilisation d'images de caméras de police[174]	15	24

VSSE	Nombre d'autorisations 2021	Nombre d'autorisations 2022
Utilisation d'images de caméras de police	46	55

II.2.4. RÉQUISITION DE CERTAINES DONNÉES FINANCIÈRES (ART. 16/6 L.R&S)

Depuis août 2022, la VSSE et le SGRS peuvent requérir le concours :
- des personnes et institutions visées à l'article 5, paragraphe 1er, 3° à 22°, de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces ;
- des personnes et institutions qui, sur le territoire belge, mettent à disposition ou proposent des services en lien avec des valeurs virtuelles permettant d'échanger des moyens de paiement réglementés en valeurs virtuelles ;
- du point de contact central tenu par la Banque nationale de Belgique conformément à la loi du 8 juillet 2018 portant organisation d'un point de contact central des comptes et contrats financiers et portant extension de l'accès

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

172 *'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 d'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 des conditions qui ne respectent pas les dispositions 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 des conditions qui ne respectent pas les dispositions légales.'*

173 Début 2022, le Comité permanent R, en sa qualité d'Autorité de contrôle compétente, a formulé une décision à cet égard : COMITÉ PERMANENT R, Décision DPA n° VCI-DPA/2022/2 – Instruction de traitement concernant la récupération rétroactive d'images de caméras de police par les services de renseignement en vertu de l'article 16/4, § 2 L.R&S.

174 Le champ d'application de l'article 16/4 L.R&S (par ex. concernant les consultations de la Direction de l'information policière et des moyens ICT (DRI) de la Police fédérale) fait l'objet d'une analyse juridique (2021).

au fichier central des avis de saisie, de délégation, de cession, de règlement collectif de dettes et de prêt.

Cette collaboration se limite à :
– l'identification des produits et services dont la personne visée est le titulaire, le mandataire ou le bénéficiaire effectif ;
– l'identification des titulaires, des mandataires ou des bénéficiaires effectifs des produits et services.

Le dirigeant du service ou son délégué effectue la réquisition par écrit. La VSSE et le SGRS doivent tenir un registre de toutes les identifications requises et doivent transmettre chaque mois au Comité permanent R une liste des identifications requises. À cet égard, le Comité s'est vu attribuer la compétence d'interdire l'utilisation des données recueillies dans des conditions qui ne respectent pas les dispositions légales.

En 2022, le SGRS a émis 9 réquisitoires, tandis que la VSSE en a émis 20.

II.3. LE NOUVEAU RÔLE DU COMITÉ DANS LES MESURES DE PROTECTION ET D'APPUI

Par la loi du 14 juillet 2022[175], le Comité s'est vu confier des missions importantes dans le cadre des mesures de protection et d'appui qu'un service de renseignement peut mettre en œuvre dans l'exercice de ses missions.

II.3.1. LA COMMISSION D'INFRACTIONS PAR DES AGENTS, DES SOURCES HUMAINES ET DES PERSONNES QUI PRÊTENT LEUR CONCOURS (ART. 13/1, 13/1/1, 13/1/2 ET 13/4 L.R&S)

Les agents de renseignement ou les sources humaines peuvent, dans des conditions strictes, commettre des infractions pénales. L'une de ces conditions est généralement l'approbation donnée par la Commission BIM. En cas de refus de la Commission BIM, le dirigeant du service concerné peut saisir le Comité qui « *autorisera ou n'autorisera pas la commission de(s) (l') infraction(s) dans les plus brefs délais.* » Le Comité permanent R communique ensuite sa décision au dirigeant du service et à la Commission BIM.

Toutefois, si la Commission BIM n'a pas pris de décision dans le délai imparti, le dirigeant du service peut encore saisir le Comité, qui prend alors une décision dans

175 Loi du 14 juillet 2022 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, *M.B.* 5 août 2022.

les plus brefs délais. Le Comité est également destinataire de tous les documents établis dans ce cadre. Il est par ailleurs informé dans les plus brefs délais quand le dirigeant du service met lui-même fin à la mesure.

Si le Comité permanent R constate une illégalité, le dirigeant du service concerné en est informé par écrit. Ce dernier met fin dès que possible à la mesure prévue ou en cours, ce qu'il confirme ensuite par écrit.

Les conseillers et les collaborateurs du Comité permanent R sont exemptés de peine lorsqu'ils exercent leur contrôle dans le cadre de l'application de ces règles.

En 2022, la VSSE a utilisé cette méthode dans quatre dossiers. Pour sa part, le SGRS n'a pas eu recours à cette méthode.

II.3.2. FAUX NOM, FAUSSE QUALITÉ, IDENTITÉ FICTIVE ET QUALITÉ FICTIVE (ART. 13/2 L.R&S)

Un agent peut utiliser un nom ou une qualité fausse ou fictive pour des raisons de sécurité liées à la protection de sa personne ou de tiers. Tout usage actif d'une identité fictive doit être mentionné dans une liste transmise mensuellement au Comité permanent R. De même, toute création de documents officiels prouvant une identité ou une qualité fictive doit être notifiée au Comité. Cette réglementation est en vigueur depuis 2017.

En 2022, les listes ont été transmises mensuellement au Comité permanent R, et ce, conformément aux prescrits légaux.

II.3.3. LA CRÉATION D'UNE PERSONNE MORALE (ART. 13/3 L.R&S)

Les services de renseignement peuvent créer des personnes morales en l'appui de leurs opérations et, à leur profit, fabriquer et utiliser (ou faire fabriquer) de faux documents. Tout déploiement d'une personne morale en dehors du cas prévu à l'article 18/13 est mentionné dans une liste transmise mensuellement au Comité permanent R. Ce dispositif est également en vigueur depuis 2017.

En 2022, les listes ont été transmises mensuellement au Comité permanent R, et ce, conformément aux prescrits légaux.

II.4. CONTRÔLE SPÉCIFIQUE EN MATIÈRE DE DEMANDES DE CONSERVATION DES DONNÉES DANS LE SECTEUR DES TÉLÉCOMMUNICATIONS

Les données relatives à l'identification, au trafic et à la localisation jouent naturellement un rôle important dans le travail de renseignement. C'est en partie à cette fin que l'obligation de conserver les données a été créée à l'époque par l'article 126 de la Loi du 13 juin 2005 relative aux communications électroniques (LCE). Cette loi obligeait les fournisseurs de services de téléphonie publique et les opérateurs de réseaux publics de communications électroniques à conserver ces données pendant 12 mois. Mais dans son arrêt du 22 avril 2021, la Cour constitutionnelle a annulé cette loi sur la conservation des données.[176] La Cour a estimé que la conservation générale et indiscriminée de données relatives aux communications électroniques viole le droit au respect de la vie privée et porte atteinte à la protection des données à caractère personnel. La conservation des données doit être l'exception ; seule une conservation ciblée et proportionnée à la finalité poursuivie peut être autorisée.

Le législateur a répondu par la Loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités.[177]

En ce qui concerne la VSSE et le SGRS, cela s'est traduit d'abord par les articles 13/6 et 13/7 L.R&S.

L'article 13/6 L.R&S donne la possibilité aux deux services de requérir le concours d'un opérateur de réseaux de communications électroniques ou d'un fournisseur de services de communications électroniques pour procéder à :

- la conservation des données de trafic et de localisation de moyens de communications électroniques qui sont à sa disposition au moment de la réquisition ;
- la conservation des données de trafic et de localisation qu'il génère et traite à partir de la réquisition.

Cette réquisition doit être faite par écrit par le dirigeant du service ou son délégué et doit être motivée. La réquisition mentionne la nature des données de trafic et de localisation à conserver et les personnes, groupements, les zones géographiques, les moyens de communication et/ou le mode d'utilisation dont les données de trafic et de localisation doivent être conservées ainsi que le délai de conservation. Ce délai de conservation ou la durée de la mesure ne peut excéder six mois à compter de la date de la réquisition, sans préjudice de la possibilité de prolongation. Les services de renseignement et de sécurité doivent tenir un registre de toutes les réquisitions

176 Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.* 18 juillet 2016.

177 *M.B.* 8 août 2022.

de conservation. Chaque décision de réquisition est notifiée avec la motivation au Comité permanent R. Lorsqu'il constate une illégalité, le Comité permanent R met fin à la réquisition.

L'article 13/7 L.R&S permet de procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traitées par eux. Il doit cependant être question d'une menace réelle, grave et prévisible pour la sécurité nationale. L'utilisation de cette méthode est soumise à des conditions strictes. Elle requiert également l'accord écrit préalable de la Commission BIM, qui transmet immédiatement la demande du dirigeant du service et son accord éventuel au Comité permanent R. La réquisition approuvée doit être confirmée par arrêté royal. Si la Commission ou le Comité permanent R constate une illégalité, il est mis fin à la réquisition nonobstant la confirmation par arrêté royal.

En 2022, aucun des services de renseignement n'a fait usage de cette nouvelle méthode.

Par ailleurs, il y a lieu de faire référence à l'article 126/3, § 6 LCE, qui attribue également un rôle au Comité dans le contrôle de la définition des zones géographiques à l'intérieur desquelles la conservation des données peut être effectuée. Ainsi, le Comité sera le seul destinataire de la liste des bâtiments destinés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé. Cette liste est établie annuellement par la VSSE et le SGRS et est approuvée par le Conseil national de sécurité sur proposition du ministre de la Justice et du ministre de la Défense. La liste actualisée des autres zones visées aux paragraphes 3 à 5 de l'article 126/3 LCE où la conservation des données est obligatoire est mise à la disposition de l'Organe de contrôle de l'information policière (C.O.C.) et du Comité permanent R, chacun dans le cadre de ses compétences. L'Organe de contrôle de l'information policière et le Comité permanent R, chacun dans le cadre de ses compétences, peuvent formuler des recommandations concernant ces listes ou donner l'ordre motivé de retirer certaines zones géographiques de la liste. Cette réglementation n'est pas encore entrée en vigueur.[178]

II.5. CONSTATATIONS GÉNÉRALES

Pour l'année 2022 et par rapport à l'exercice précédent, le Comité permanent R constate une augmentation significative de l'utilisation par les deux services des méthodes particulières de renseignement.

---

178 Cette réglementation entrera en vigueur à la date fixée par le Roi par arrêté pris après avis du Conseil des ministres et au plus tard le 1er janvier 2027. En pratique, si le Roi ne décide rien, les services de renseignement devront établir leurs listes au plus tard le 1er janvier 2026 (art. 45 Loi du 20 juillet 2022).

Si la période Covid a pu être un facteur de ralentissement des activités, le retour à une situation sanitaire relativement normale a certainement facilité l'opérationnalisation des activités des deux services. En 2022, on en revient à des statistiques analogues à celles relevées depuis 2018.

Au cours de ses échanges avec les services à propos de cette tendance à la hausse, le Comité permanent R a été amené à constater que l'augmentation des activités des services coïncide également avec l'augmentation de leurs capacités, notamment à la suite de la fin des formations des agents et leur opérationnalisation effective.

À cet égard, tant le SGRS que la VSSE rappellent qu'une augmentation de la capacité opérationnelle, à la fois sur le plan quantitatif et qualitatif, entraîne logiquement une augmentation des dossiers et donc de l'utilisation des méthodes de renseignement, qu'elles soient ordinaires, spécifiques ou exceptionnelles.

Certaines problématiques comme, par exemple, la guerre en Ukraine ou les questions d'ingérence au sein du Parlement européen, ont également nécessité des investissements particuliers.

En lien avec ce dernier constat et sans préjudice de ce qui est communiqué dans les rapports d'activités des services – auxquels il est renvoyé –, le Comité permanent R constate qu'après une période qui a suivi les attentats de 2015-2016 et durant laquelle les menaces liées à l'extrémisme et au radicalisme ont mobilisé beaucoup de ressources, un rééquilibrage a eu lieu dans l'utilisation des méthodes particulières de renseignement au bénéfice de la lutte contre l'espionnage et l'ingérence.

Enfin, au sein de la VSSE, la mise en place d'une nouvelle méthodologie de travail permet certainement de déterminer plus efficacement des priorités d'enquête.

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

III.1. LES COMPÉTENCES DU SGRS ET LA MISSION DE CONTRÔLE DU COMITÉ PERMANENT R[179]

Dès 2017, la compétence du Service Général du Renseignement et de la Sécurité (SGRS) a été élargie dans le cadre des interceptions de sécurité.[180] Les interceptions pouvaient alors porter sur des communications *'émises ou reçues à l'étranger'*. Cette possibilité vaut pour presque toutes les missions du SGRS. Il est d'ailleurs intéressant d'observer que les descriptions des missions ont, elles aussi, été élargies. Le législateur a en même temps introduit deux autres méthodes, à savoir 'l'intrusion dans un système informatique' (art. 44/1 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S)) et 'la prise d'images animées' (art. 44/2 L.R&S). Par ailleurs, la manière dont le Comité peut contrôler ces méthodes a été modifiée.

Le contrôle *préalable* aux interceptions, prises d'images fixes ou animées s'effectue sur la base d'une liste établie annuellement.[181] Cela signifie qu'en plus du plan annuel d'interceptions, le SGRS doit également élaborer un plan d'intrusions et d'images.[182] 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

---

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

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

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

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

ouvrables et doit la communiquer au SGRS[183], qui transmet à son tour les listes pourvues de l'autorisation ministérielle au Comité permanent R.[184]

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

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

Que peut faire le Comité permanent R en cas d'irrégularité ? L'article 44/4 L.R&S stipule que *'le Comité permanent de contrôle des services de renseignement, sans préjudice des autres compétences attribuées à ce Comité par la loi du 18 juillet 1991, a le droit de faire cesser des interceptions, intrusions ou prises d'images en cours lorsqu'il apparaît que celles-ci ne respectent pas les dispositions légales ou l'autorisation [ministérielle]. Il ordonne l'interdiction d'exploiter les données recueillies illégalement et leur destruction, selon les modalités à fixer par le Roi.*' Le Comité permanent R tient à souligner une fois encore[185] qu'un tel Arrêté royal n'a toujours pas été pris.[186] Aussi, le Comité réitère sa recommandation d'y remédier au plus vite.

---

183 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.

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

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

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

III.2. LES CONTRÔLES EFFECTUÉS EN 2022

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

L'ensemble des plans relatifs aux interceptions, aux intrusions et aux prises d'images pour l'année 2022 a été remis au Comité permanent R le 23 décembre 2021.

Le Comité a pu constater que les plans pour l'année 2022 respectent effectivement les prescrits légaux.

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

En 2022, le Comité permanent R n'a pas effectué de visite des installations à partir desquelles sont effectuées les interceptions, intrusions et prises d'image.
Ces divers contrôles feront l'objet d'un plan d'actions pour 2023, tenant compte de la création, en octobre 2022, de la nouvelle composante Cyber Command placée sous le commandement du SGRS.

Etant donné que cette nouvelle composante est annoncée comme devant permettre d'assurer une « *approche intégrée de la sécurité de l'information et du renseignement* »[187] dans tout l'espace cyber, le Comité permanent R veillera à adapter son contrôle des dispositions particulières visées aux articles 44 à 44/5 inclus L.R&S en conséquence de l'importante réorganisation entamée par le SGRS.

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

En 2022, le Comité permanent R a constaté avoir reçu les « *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°* ».

[187] J. MATRICHE, « Cyberespace, le nouveau champ de bataille de l'armée belge », *Le Soir*, 18 octobre 2022.

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

IV.1. INTRODUCTION

Le Règlement Général sur la Protection des Données 2016/679 (RGPD)[188] et la Directive 2016/680 (Directive)[189] règlent la manière dont les acteurs publics et privés doivent opérer lorsqu'ils collectent, sauvegardent, conservent et communiquent des données à caractère personnel. Les deux instruments européens ont donné lieu à quelques modifications de loi substantielles au niveau national : en décembre 2017, l'Autorité de protection des données (APD)[190] a été créée et en juillet 2018, une nouvelle Loi relative à la protection des données (LPD) a été votée.[191] Cette loi modifie à son tour la L.Contrôle du 18 juillet 1991. Le Comité permanent R a, en effet, été désigné comme autorité de contrôle compétente pour les traitements de données à caractère personnel qui relèvent de la 'sécurité nationale'.

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

188 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.

189 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.

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

191 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.

et de renseignement et de l'Organe de contrôle pour l'analyse de la menace (L.Contrôle).[192]

L'article 35 §3 L.Contrôle énonce que le '*Comité permanent R fait rapport annuellement à la Chambre des représentants sur les avis rendus en sa qualité d'autorité de protection des données, sur les enquêtes effectuées et mesures prises en cette même qualité ainsi que sur sa collaboration avec les autres autorités de protection des données*'. Ce chapitre répond à cette obligation. Il aborde :

- les contrôles effectués par le Comité – seul ou avec l'Organe de contrôle de l'information policière (C.O.C.) ou le Comité P – à la demande de citoyens qui souhaitent exercer leur droit d'accès indirect à leur 'dossier' dans l'un des services contrôlés par le Comité ;
- les avis rendus par le Comité concernant la protection des données.

IV.2. LE TRAITEMENT DES REQUÊTES INDIVIDUELLES

Le Comité permanent R est compétent pour le traitement des requêtes individuelles relatives aux traitements de données à caractère personnel par les personnes et les services susmentionnés ainsi que leurs sous-traitants (art. 34 L.Contrôle et articles 79, 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. Il peut encore se plaindre de l'éventuel non-respect des règles de protection des données par un responsable du traitement relevant de la compétence du Comité.[193]

Pour être recevable, une requête doit être écrite, datée, signée et motivée (art. 51/2 L.Contrôle).[194] 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.

Le tableau suivant donne un aperçu des dossiers traités (ouverts et/ou clôturés) en 2022. Les colonnes du tableau ventilent les requêtes selon que la compétence du Comité permanent R est exclusive ou conjointe avec d'autres autorités de

192 Pour plus de détails, voir COMITÉ PERMANENT R, *Rapport d'activités 2018*, pp. 75-86.

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

194 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 les articles 80, 114, 146 et 174 LPD).

contrôle.[195] Il convient de noter que, dans le tableau ci-dessous, une seule et même plainte peut constituer plusieurs « dossiers » selon les services visés.[196]

Tableau 1. Le traitement des requêtes individuelles[197]

2022	Comité permanent R		Comités permanents R et P	Comités permanents R et P et le C.O.C.	Total
1. Dossiers ouverts en 2022	23		4	0	27
2. Requêtes irrecevables en 2022	3		0	0	3
3. Requêtes recevables en 2022	20		4	0	24
	c. VSSE	17			
	c. SGRS	1			
	c. VSSE&SGRS	2			
4. Dossiers en cours en 2022	25[198]		6[199]	0	31

[195] Le tableau n'indique donc pas les hypothèses dans lesquelles une coopération a pu se réaliser avec une autre autorité de contrôle, le C.O.C. par exemple, lorsque les compétences de chaque autorité de contrôle sont distinctes.

[196] Par exemple, une plainte contre l'OCAM et la VSSE sera comptabilisée à la fois dans les dossiers traités conjointement par les Comités permanents P et R pour le volet OCAM de l'enquête et dans les dossiers traités exclusivement par le Comité permanent R pour les devoirs d'enquêtes portant sur la VSSE.

[197] La ligne 1 indique le nombre de dossiers ouverts en 2022. Les lignes 2 et 3 répartissent les requêtes introduites en 2022 selon la décision d'irrecevabilité ou de recevabilité. Pour les dossiers traités uniquement par le Comité permanent R, la ligne 3 précise encore le nombre de requêtes (introduites en 2022) recevables selon les services visés. Les lignes 4 et 5 précisent l'état d'avancement des dossiers traités en 2022 (toujours en cours ou clôturés). Enfin, la ligne 6 indique le nombre de dossiers pour lesquels des mesures correctives ont été exigées par le Comité.

[198] Dont 2 dossiers ouverts en 2021.

[199] Dont 2 dossiers ouverts en 2021.

2022	Comité permanent R	Comités permanents R et P	Comités permanents R et P et le C.O.C.	Total
5. Dossiers clôturés en 2022[200]	13[201]	2[202]	3[203]	18
6. Mesures correctives	4	0	0	4
7. Nombre total de requêtes traitées	38	8	3	49

Il peut être relevé que dans 93 % des requêtes traitées en 2022, les personnes concernées allèguent[204] une interférence concrète dans leurs droits et libertés causée par, ou du moins liée à, un traitement de données d'un responsable du traitement relevant de la compétence du Comité permanent R. Une telle interférence existerait par exemple dans le cadre d'une demande d'acquisition de la nationalité ou de titre de séjour à l'occasion de laquelle un service de renseignement communique des informations au Ministère public, lorsque la personne concernée allègue faire l'objet de contrôles réguliers de police, lorsqu'elle constate que l'accès à un territoire lui est refusé, lorsque des données d'un service de renseignement ont été utilisées dans une procédure judiciaire pénale, etc.

Comme en 2021, le Comité a ainsi eu à traiter en 2022 plusieurs requêtes déposées dans le cadre de procédures de demande de nationalité ou de droit de séjour. Confrontés à une décision négative motivée sur la base d'informations fournies par la Sûreté de l'Etat (VSSE), le Service Général du Renseignement et de la Sécurité (SGRS) et/ou l'Organe de coordination pour l'analyse de la menace (OCAM), les requérants s'adressent (entre autres) au Comité permanent R pour un contrôle du traitement de leurs données personnelles.

---

200 Par le passé, le Comité permanent R comptabilisait un dossier comme clôturé lorsqu'il avait pu constater que les mesures correctives qu'il avait exigées avaient été mises en œuvre. En 2022, des échanges entre le Comité et les services de renseignement à propos de mesures correctives exigées dans différents dossiers ont mis en lumière les retards que pouvait parfois prendre l'exécution de ces mesures. Désormais, un dossier est considéré comme clôturé lorsque le requérant a été informé des conclusions du Comité et que les éventuelles mesures correctives ont été ordonnées par courrier au(x) service(s) concerné(s). Des doublons sont donc possibles entre les chiffres de 2021 et 2022 (ligne 6).

201 Dont 1 dossier ouvert en 2019, 1 dossier ouvert en 2020 et 6 dossiers ouverts en 2021.

202 Dont 1 dossier ouvert en 2020 et 1 dossier ouvert en 2021.

203 Ouverts en 2020.

204 Il est à noter que dans plusieurs dossiers, ces interférences ne sont pas seulement alléguées par les personnes concernées mais bien étayées par elles et avérées (s'agissant par exemple, de la communication de notes d'analyse dont disposent les personnes concernées dans le cadre des procédures où ces notes sont utilisées par les autorités publiques). Dans d'autres cas, ces allégations sont des suspicions, plus ou moins, voire non, étayées en faits.

Les 7 % restant de requêtes se composent de demandes d'exercice indirect de droits, sans précision particulière ou grief concret. Typiquement, la personne concernée se demande si des données sont traitées à son sujet et si le traitement de celles-ci est conforme à la réglementation applicable (accès indirect).

Ce déséquilibre (93-7%)[205] n'est pas surprenant dès lors que la réponse fournie à la personne concernée exerçant ses droits ne lui apprend rien sur ce qu'il en est du traitement (éventuel) de ses données à caractère personnel par les services relevant de la compétence du Comité. Ce n'est que lorsque la personne concernée suspecte ou subit concrètement l'effet d'un tel traitement de données, qu'elle verra un intérêt à s'adresser au Comité permanent R pour qu'il réalise les vérifications nécessaires, dans l'espoir d'obtenir une amélioration de sa situation.

Enfin, notons qu'en 2022, le Comité permanent R, en sa qualité d'autorité de contrôle, a ordonné des mesures correctives à l'égard des services de renseignement concernés dans quatre dossiers (art. 51/3 L.Contrôle). Selon les dossiers, il peut s'agir d'exiger la rectification voire la suppression de données à caractère personnel, la notification de la décision du Comité aux partenaires et/ou aux autorités ou encore la diffusion de la décision au sein du service concerné.

IV.3. LES AVIS

Le Comité peut rendre un avis « *sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant des orientations politiques des ministres compétents* » dans deux cas : lorsque la loi impose son avis ou à la demande de la Chambre des représentants ou du ministre compétent (art. 33, alinéa 8 L. Contrôle). Ce genre d'avis porte spécifiquement sur la problématique du traitement de données et doit donc être distingué de la compétence d'avis générale qui porte, par exemple, sur l'efficacité et la coordination (cf. Chapitre VI. Avis). 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.

En 2022, le Comité a rendu quatre avis en cette qualité :

- Avis 001/CPR/2022 du 20 avril 2022 portant sur « *la sûreté maritime* » ;
- Avis 002/CPR/2022 du 29 juin 2022 portant sur « *l'accès à la banque de données E-PV* » ;
- Avis 003/CPR/2022 du 29 juin 2022 portant sur « *la protection des données en matière de transfert de données à caractère personnel de l'Office des Etrangers à la VSSE et au SGRS* » ;
- Avis 004/CPR/2022 du 29 juin 2022 portant sur « *le filtrage des investissements directs étrangers et le rôle de la VSSE et du SGRS en la matière* ».

[205] En 2021, ce déséquilibre était de 85-15%.

Ces avis sont résumés dans le Chapitre VI et consultables, dans leur intégralité, sur le site internet du Comité.[206]

IV.4. LA NOTIFICATION D'UNE POTENTIELLE BRÈCHE DE SÉCURITÉ

Les services contrôlés par le Comité permanent R doivent conserver ou mettre à la disposition du Comité toute une série de données[207]. Le responsable du traitement doit ainsi notifier toute brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance (articles 89, 122, 155 et 180 LPD).

En 2022, aucune brèche de sécurité (« *data breach* »)[208] n'a été signalée au Comité.

206 www.comiteri.be.

207 Chaque service n'est pas tenu de conserver ou tenir à disposition du Comité toutes les données mentionnées ici. La Commission BIM ne doit ainsi pas communiquer d'informations au Comité.

208 Article 26, 11° LPD : « 'brèche de sécurité' : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données ». En pratique et en droit hors du contexte de la LPD, il est plutôt fait référence à des « violations de données » ou « data breaches ».

CHAPITRE V.
LE CONTRÔLE DES BANQUES DE DONNÉES COMMUNES

La création de la banque de données commune '*foreign terrorist fighters*' par les ministres de l'Intérieur et de la Justice remonte à 2016. Cette banque de données commune a été modifiée en 2018 : on parle désormais de la banque de données commune '*terrorist fighters*' (BDC TF). Celle-ci comprend, outre la catégorie générale des '*foreign terrorist fighters*', une catégorie visant les '*homegrown terrorist fighters*'. Toujours en 2018, une (nouvelle) banque de données commune distincte a été créée pour les 'propagandistes de haine' (BDC PH). Par un arrêté royal pris fin 2019, deux nouvelles catégories ont encore été ajoutées à la BDC TF, à savoir les 'extrémistes potentiellement violents' (EPV) ainsi que les 'personnes condamnées pour terrorisme' (PCT).

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

Aucune évolution législative ou réglementaire n'est intervenue depuis le dernier rapport[209] du C.O.C. et du Comité permanent R en la matière.

En février 2022, une nouvelle version des BDC TF et HP a été mise en production. Cette version présente une interface sensiblement modifiée, ainsi que de nouvelles fonctionnalités.

V.1. LA MISSION DE CONTRÔLE ET L'OBJET DU CONTRÔLE

Pour l'année 2022, le C.O.C. et le Comité permanent R ont décidé d'axer leur contrôle conjoint sur le suivi de certaines recommandations antérieures et sur l'utilisation des banques de données communes par les services de sécurité et de renseignement. Une forme de suivi des recommandations de l'enquête de contrôle

[209] C.O.C. et COMITÉ PERMANENT R, *Rapport concernant le contrôle conjoint des Banques de données communes Terrorist Fighters et Prédicateurs de haine par le Comité permanent R et l'Organe de contrôle de l'information policière*, 2020, 33 p. (Diffusion restreinte (A.R. 20 mars 2000)). Le rapport a été approuvé par les autorités de contrôle le 12 août 2021.

concernant la radicalisation d'un militaire de la Défense réalisée en 2021[210] a également été intégrée au contrôle.

Le contrôle a été annoncé aux services concernés, à savoir la Police fédérale, la Sureté de l'Etat (VSSE) et le Service Général du Renseignement et de la Sécurité (SGRS) par courrier. Ces services ont été interrogés par courrier et une extraction des données de journalisation concernant les traitements effectués par les deux services de renseignement et de sécurité a été demandée à la Police fédérale.
Le rapport est planifié pour le premier semestre de 2023.

V.2. LA MISSION D'AVIS

La Loi sur la fonction de police (LFP) prévoit également l'obligation de recueillir l'avis conjoint du Comité permanent R et du C.O.C. dans différentes hypothèses.

Ainsi, préalablement à sa création, les ministres de l'Intérieur et de la Justice doivent déclarer la banque de données commune ainsi que les modalités de traitement, dont celles relatives à l'enregistrement des données, et les différentes catégories et types de données à caractère personnel et d'informations traitées, au Comité permanent R et au C.O.C. À leur tour, le Comité et le C.O.C. doivent émettre conjointement un avis (art.44/11/3*bis* § 3 LFP). Par ailleurs, pour chaque banque de données commune, un Arrêté royal délibéré en Conseil des ministres détermine, après avis des deux instances précitées, les règles de responsabilités en matière de protection des données à caractère personnel des organes, services, autorités et organismes traitant des données, les règles en matière de sécurité des traitements, les règles d'utilisation, de conservation et d'effacement des données (art.44/11/3*bis* § 4 LFP). En outre, des modalités complémentaires de gestion des banques de données communes peuvent être déterminées par un arrêté royal délibéré en Conseil des ministres, toujours après un avis du Comité permanent R et du C.O.C. (art.44/11/3*bis* § 8 LFP). Enfin, la fonction d'avis s'exerce également en ce qui concerne tout projet d'Arrêté royal instaurant ou modifiant les accès aux banques de données communes (art.44/11/3*ter* §§ 2 à 4).

Le Comité permanent R et le C.O.C. n'ont pas été sollicités en 2022 dans ce contexte.

[210] Enquête de contrôle du Comité permanent R concernant, d'une part, la détection et le suivi de la radicalisation d'un militaire de la Défense par les deux services de renseignement, et d'autre part, leur collaboration portant notamment sur l'échange d'information avec leurs partenaires, y compris la Défense, 1er juillet 2021 (www.comiteri.be).

CHAPITRE VI.
AVIS

L'article 33 de la Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (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* ».

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 relative aux banques de données communes, et ce conjointement avec l'Organe de contrôle de l'information policière (C.O.C.).

En 2022, l'avis du Comité permanent R a été sollicité à sept reprises.[211] À trois reprises, des ministres ont adressé une demande d'avis directement au Comité : la ministre de la Fonction publique concernant la réglementation relative aux lanceurs d'alerte du secteur public (VI.5) et la ministre de la Défense à propos du screening des (candidats) membres de la Défense (VI.6). Pour cet avis, la ministre a également, pour la première fois, sollicité le président de l'Organe de recours en matière d'habilitations, attestations et avis de sécurité. La ministre de l'Intérieur a également adressé une demande d'avis aux Comités permanents P et R concernant la Direction Evaluation de l'intégrité pour les pouvoirs publics (DEIPP).[212]

À quatre autres reprises, la demande d'avis a été soumise au Comité permanent R par l'intermédiaire de l'Autorité de protection de données (ADP) : un avis pour le ministre de la Justice et de la Mer du Nord sur un projet de loi concernant la sûreté maritime (VI.1), un avis pour le secrétaire d'Etat à l'Asile et à la Migration concernant le transfert de données entre l'Office des Etrangers et les services de renseignement (VI.3) et deux avis pour le ministre de l'Economie et du Travail

---

211 Le Comité est de plus en plus sollicité sur la base de l'article 33 L.Contrôle; le temps consacré à la formulation d'avis a par conséquent considérablement augmenté.

212 Suite à l'approbation par le Conseil des ministres, le 14 septembre 2022, du projet de loi relatif à « l'approche administrative communale, à la mise en place d'une enquête d'intégrité communale et portant création d'une Direction chargée de l'Évaluation de l'Intégrité pour les pouvoirs publics », la ministre de l'Intérieur a formulé une nouvelle demande d'avis. Les Comités permanents P et R ont décidé de renvoyer à un avis précédent (17 septembre 2020) sur ce sujet (cf. www.comiteri.be). Cet avis n'est pas repris dans le présent chapitre.

concernant, d'une part, l'accès à la banque de données e-PV (VI.2) et, d'autre part, le filtrage des investissements directs étrangers (VI.4).

Les avis sont résumés, en ordre chronologique, dans le présent chapitre. Ils sont consultables, dans leur intégralité, sur le site internet du Comité.[213]

VI.1. AVIS SUR LA SÛRETÉ MARITIME[214]

Fin février 2022, l'Autorité de protection des données a transmis au Comité permanent R une demande d'avis du ministre de la Justice et de la Mer du Nord à propos de l'avant-projet de loi modifiant la Loi du 8 mai 2019 introduisant le Code belge de la navigation.

L'avant-projet y établissait que la composition et le fonctionnement de l'Autorité Nationale de Sûreté Maritime (ANSM) sont fixés par arrêté royal. L'exposé des motifs précisait toutefois que « *(l)es services suivants feront déjà partie de l'ANSM : DG Navigation, NCCN, OCAM, Police fédérale/Police de la Navigation, Douanes et Accises, Défense, SGRS et Sûreté de l'État* ». Le Comité constatait donc que la VSSE, le SGRS et l'OCAM étaient mentionnés expressément comme membres de l'ANSM. En ce qui concerne la VSSE et le SGRS, cette adhésion s'inscrit dans la lignée de participations similaires à des plateformes de concertation en charge de la sécurité dans le domaine 'mobilité et transport', plus précisément au Comité fédéral pour la Sûreté du Transport ferroviaire[215] et au Comité national de sûreté de l'aviation civile.[216] Mais l'avant-projet stipulait également que la composition et le fonctionnement des Comités locaux de la Sûreté maritime (CLSM) sont déterminés par le Roi. Ici aussi, l'exposé des motifs précisait qu' « *(u)n CLSM sera composé d'au moins des représentants de la Police fédérale/Police de la navigation, de la police locale, des douanes et accises, de la DG Navigation, de la défense, du SGRS et des représentants des entités régionales exploitant les ports ou les voies navigable* ». Le Comité s'étonnait par contre que l'exposé des motifs prévoyait également la participation du SGRS aux Comités locaux de la Sûreté maritime.

Le Comité recommandait en outre de supprimer un autre projet d'article, selon lequel « *(l)'ANSM peut agir en tant qu'officier de sécurité aux fins de la demande des habilitations de sécurité visées au paragraphe 1er* ». En effet, le Comité rappelait au gouvernement que la fonction d'« officier de sécurité » visée par la Loi du 11 décembre 1998 (article 13, 1°) est une personne physique. Dans le cadre de la demande d'habilitation de sécurité, cet officier de sécurité fait office de lien entre

213 www.comiteri.be.

214 Avis n° 001/CPR/2022 du 20 avril 2022 portant sur la sûreté maritime, 5 p.

215 *Cf.* article 4 de l'arrêté royal du 26 janvier 2006 relatif à la création d'un Comité fédéral pour la Sûreté du Transport ferroviaire et portant diverses mesures pour la sûreté du transport intermodal.

216 *Cf.* article 3 de l'arrêté royal du 20 juillet 1971 relatif à la création d'un Comité national de sûreté de l'aviation civile et de comités locaux de sûreté d'aéroports.

l'autorité à laquelle il appartient et l'Autorité nationale de sécurité (ANS) chargée de délivrer les habilitations de sécurité.

L'avis du Comité rappelait également que la plateforme digitale ISPS[217] utilisée pour « *le stockage, le suivi et l'approbation de toutes les évaluations de la sûreté […]* » et pour « *l'échange d'informations entre les acteurs concernés* » ne pouvait contenir de données classifiées provenant de la VSSE, du SGRS et de l'OCAM. Quant à l'utilisation de cette plateforme pour « *la mise à jour de la liste des membres de l'ANSM* », le Comité insistait sur le caractère sensible du nom des membres de la VSSE, du SGRS et de l'OCAM. Il recommandait que les agents concernés ne soient identifiés que par le numéro d'identification fourni par leur service.

Enfin, l'avant-projet chargeait la VSSE, le SGRS et l'OCAM – en tant que membres de l'ANSM – « *du contrôle du respect du Règlement ISPS […]*» du Code belge de la Navigation et « *(d)es arrêtés d'exécution y afférents* ». Le Comité exprimait toutefois un avis négatif vis-à-vis d'une telle mission pour la VSSE, le SGRS et l'OCAM. La VSSE et le SGRS sont des services de renseignement et de sécurité et l'OCAM, un organe d'analyse de la menace. Une mission de contrôle du respect des lois pénales et administratives et de détection des infractions est en contradiction avec leurs missions actuelles. Les éventuels manquements des services concernés dans l'exercice de leurs missions de renseignement et de sécurité doivent logiquement être signalés au parquet sur la base de l'obligation de dénonciation incombant notamment aux fonctionnaires publics, telle que visée à l'article 29 CIC.

Depuis, la Loi du 13 octobre 2022 modifiant le Code belge de la Navigation concernant la sûreté maritime a été publiée[218] et est entrée en vigueur le 1er janvier 2023.

VI.2. AVIS SUR L'ACCÈS À LA BANQUE DE DONNÉES E-PV

Le Comité permanent R a été sollicité en mai 2022 par l'Autorité de protection de données pour une demande d'avis du ministre de l'Economie et du Travail sur l'avant-projet de loi modifiant le Code pénal social (ci-après CPS) en vue de la mise en place de la plateforme eDossier.[219] L'avant-projet de loi prévoyait, entre autres, l'accès de la VSSE et du SGRS à la base de données e-PV qui rassemble les procès-verbaux d'infraction des inspecteurs sociaux.

---

217 *International Ship and Port Facility Security.*

218 *M.B.*, 26 octobre 2022.

219 Avis n° 002/CPR/2022 du 29 juin 2022 portant sur l'accès à la banque de données e-PV, 10 p.

VI.2.1. LÉGITIMATION D'UN DROIT D'ACCÈS

Le Comité approuve la mise en place d'un droit d'accès à la base de données e-PV pour la VSSE, le SGRS et, dans le cadre des questions abordées ci-dessous[220], la Police fédérale.[221] En effet, le Comité est d'avis qu'un tel droit d'accès est non seulement important pour effectuer des vérifications de sécurité (par la VSSE, le SGRS et la Police fédérale pour le compte de l'ANS) mais peut aussi être un instrument important pour mener à bien les (autres) missions de renseignement et de sécurité de la VSSE et du SGRS.

VI.2.2. RÈGLEMENT PARTICULIER SUR LE DROIT D'ACCÈS DES SERVICES DE RENSEIGNEMENT

Dans son avis, le Comité commençait par rappeler que l'article 14 L.R&S règle le flux d'informations des autorités judiciaires et administratives vers la VSSE et le SGRS. Cette disposition stipule notamment que : « *(d)ans le respect de la législation en vigueur, les services de renseignement et de sécurité peuvent selon les modalités générales fixées par le Roi, avoir accès aux banques de données du secteur public utiles à l'exécution de leurs missions* » (Article 14, dernier alinéa L.R&S). Le législateur y indique également que dans l'hypothèse où la VSSE et/ou le SGRS dispose d'un droit d'accès à une base de données publique, certaines dispositions particulières doivent être prises en considération par le Roi.

Ces règles particulières ont été précisées par arrêté royal en 2019.[222] Elles prévoient, entre autres, la tenue, au sein des services de renseignement et de sécurité, d'un registre des personnes habilitées à accéder à la banque de données en question ainsi que des traitements effectués par les services. Ces règles s'appliquent donc également à un éventuel accès du SGRS et de la VSSE à la banque de données e-PV.

---

220 Le Comité se limite à l'application de la Loi Classification, règlement dans lequel le législateur l'a désigné comme l'autorité compétente en matière de protection des données.

221 Le Comité rappelle que la nécessité d'un tel droit d'accès avait déjà été confirmée pour ces trois services par arrêté royal, dans le cadre et aux fins des vérifications de sécurité effectuées par l'Autorité nationale de sécurité (ANS) – voir Article 3, dernier alinéa AR 8 mai 2018 *juncto* article 21 AR 24 mars 2000 portant exécution de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.

222 Arrêté royal du 2 octobre 2019 modifiant l'arrêté royal du 12 octobre 2010 portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'arrêté royal du 3 juillet 2016 portant exécution de l'article 21 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

VI.2.3. PROJET D'ARTICLE 100/10, § 5 CPS

La création d'un droit d'accès pour la VSSE, le SGRS et, en ce qui concerne l'exécution des vérifications de sécurité, la Police fédérale, devrait être incluse dans le projet d'article 100/10, § 5 CPS. Dans son avis, le Comité suggérait de compléter le projet d'article par une référence à la L.R&S afin que l'accès aux données de la banque de données e-PV soit étendu aux services de renseignement et de sécurité.

Le Comité insistait également sur l'exposé des motifs de l'article 17, 4° du projet de loi qui justifie le remplacement de l'article 100/10, § 5 CPS comme suit : « *Il s'agit de délimiter l'accès aux données relatives à la banque de données epv pour un traitement légitime et proportionnel au regard de la ou des finalités appropriées et reposant sur une base légale afin de se conformer aux exigences de la réglementation relative à la protection des données selon les catégories de données traitées* ».

Le Comité constatait ainsi le choix du législateur d'intégrer les règles en matière de protection des données relatives à la VSSE et au SGRS dans la Loi du 30 juillet 2018 relative à la protection des données (LPD)[223], plutôt que dans la Loi Renseignement.

Les articles 76 et 110 LPD disposent que « *(d)ans l'intérêt de l'exercice de leurs missions* », la VSSE, le SGRS et, notamment en ce qui concerne, entre autres, les vérifications de sécurité, la Police fédérale « *traitent 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.* ».

Contrairement à la Loi (abrogée) du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (*juncto* article 14 Loi Classification), les services concernés peuvent donc désormais traiter les données relatives à la santé dans le cadre des vérifications et enquêtes de sécurité. Le Comité rappelait néanmoins que cela doit se faire dans le respect des exigences de qualité juridique auxquelles tout traitement de données à caractère personnel doit répondre de manière cumulative (cf. articles 75 et 109 LPD).

[223] Les dispositions relatives à la protection des données applicables lors des missions de renseignement et de sécurité de la VSSE et du SGRS sont énumérées aux articles 72 à 104 LPD (titre 3, sous-titre 1). Celles qui sont d'application lors de l'exécution des vérifications de sécurité figurent aux articles 106 à 137 LPD (titre 3, sous-titre 3).

VI.3. AVIS SUR LA PROTECTION DES DONNÉES EN MATIÈRE DE TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL DE L'OFFICE DES ÉTRANGERS À LA VSSE ET AU SGRS

En juin 2022, le Comité permanent R a été sollicité par l'Autorité de protection de données à la demande du Secrétaire d'Etat à l'Asile et à la Migration pour rendre un avis concernant l'avant-projet de loi relatif aux traitements de données à caractère personnel par la Direction générale Office des étrangers du SPF Intérieur (OE).[224]

VI.3.1. LE TRANSFERT DE DONNÉES DE L'OE À LA VSSE ET/OU AU SGRS

Le Comité a pu constater que le projet de loi contenait une large énumération des catégories de données à caractère personnel qui peuvent être traitées par l'OE. En vertu du projet, l'OE peut transférer ces données respectivement à la VSSE et au SGRS. Un tel transfert de données à caractère personnel doit avoir lieu, selon les dispositions concernées, « *aux fins de a) l'accomplissement de ses missions légales* » – c'est-à-dire les missions de la VSSE ou du SGRS – et/ou « *b) l'évaluation par l'Office des étrangers de la menace pour l'ordre public et la sécurité nationale* ». L'exposé des motifs (pp. 66 et 67) de ces dispositions précise que : « *Les communications de données à caractère personnel avec la Sûreté de l'État permettent de vérifier si un étranger est susceptible de porter atteinte à l'ordre public et/ou à la sécurité nationale* ».

VI.3.2. LA COMMUNICATION PAR LA VSSE ET/OU LE SGRS AUX SERVICES DE RENSEIGNEMENT ÉTRANGERS DE DONNÉES ÉMANANT DE L'OE

Dans son avis, le Comité rappelait que les données à caractère personnel disponibles à la VSSE et au SGRS ne peuvent être transférées à des pays non membres de l'Union européenne ou à des organisations internationales que dans des conditions limitées (cf. articles 126 et 127 de la Loi relative à la protection des données[225]). De même, les données à caractère personnel obtenues auprès de l'Office des étrangers ne peuvent pas être transférées vers des pays tiers et sont soumises à un régime restrictif.

---

224 Avis n° 003/CPR/2022 du 29 juin 2022 portant sur la protection des données en matière de transfert de données à caractère personnel de l'Office des Etrangers à la VSSE et au SGRS, 5 p.

225 Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD).

En outre, les articles 19, alinéa 1er et 20 § 3 L.R&S constituent le cadre juridique de la coopération (inter)nationale et de l'échange d'informations. L'article 19, alinéa 1er, L.R&S règle la compétence générale de communication et de transfert de renseignement à des instances tierces.[226] Toutefois, en 1998, le législateur lui-même a estimé que cette disposition était insuffisante. Par conséquent, l'article 20 § 3 L.R&S prescrit que le Conseil national de sécurité (CNS), entre autres, doit préciser les modalités de la coopération internationale et de l'échange d'informations.

Par la Directive du 30 septembre 2016, le Conseil national de sécurité a (partiellement) rempli cette obligation légale.[227] La directive du CNS règle notamment les modalités du transfert international de données à caractère personnel par la VSSE et le SGRS.[228]

Au regard du respect de l'article 8.2 CEDH concernant le droit au respect de la vie privée, le Comité appelait à inscrire les principes de base de la Directive du Conseil national de sécurité dans une loi. Le Comité conseillait dès lors d'associer l'installation de l'article 11, § 1er, 32° et 33° du projet de loi à une telle élaboration.

En sa qualité d'autorité de protection des données dans le domaine de la sécurité nationale, le Comité invitait le gouvernement et les deux services de renseignement à œuvrer à l'élaboration d'un projet de loi visant à remédier à la situation actuelle, afin que les échanges d'informations au niveau international par les services de renseignement puissent à nouveau se dérouler conformément aux traités.[229]

---

226 Article 19, alinéa 1er L.R&S : « *Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11* ».

227 La Directive du 30 septembre 2016 du Conseil national de sécurité relative aux relations de la Sûreté de l'État (VSSE) et du Service Général du Renseignement et de Sécurité (SGRS) avec les services de renseignement étrangers.

228 Il a été décidé de classifier (au niveau 'Confidentiel') cette directive du CNS. Le Comité ne comprend pas pourquoi ce document doit être classifié. En effet, il ne contient ni des données et méthodologies opérationnelles ni d'autres types de données sensibles. En outre, étant donné que la directive du CNS fait partie du cadre juridique d'évaluation de l'action internationale des services de renseignement et de sécurité, le Comité estime qu'il n'y a aucune raison de classifier un tel document de manière permanente.

229 Voir l'avis du Comité permanent R du 28 septembre 2020 sur la Proposition de loi 'modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en vue d'instaurer des notes d'évaluation pour la collaboration avec les services de renseignement et de sécurité étrangers' (www.comiteri.be).

VI.4. AVIS SUR LE FILTRAGE DES INVESTISSEMENTS DIRECTS ÉTRANGERS ET LE RÔLE DE LA VSSE ET DU SGRS EN LA MATIÈRE

En juin 2022, à la demande du ministre du Travail et de l'Economie par l'intermédiaire de l'APD, le Comité permanent R a rendu un avis sur l'avant-projet de loi portant approbation de l'accord de coopération visant à instaurer un mécanisme de filtrage des investissements directs étrangers.[230] L'Accord de coopération a pour but de sauvegarder la sécurité nationale, l'ordre public et les intérêts stratégiques des entités fédérées dans le cadre de leurs compétences matérielles par le filtrage de certains investissements directs étrangers.

Plus spécifiquement, l'avant-projet de loi portait sur les traitements de données à caractère personnel effectués par la VSSE et/ou le SGRS. L'article 13 de l'Accord de coopération, prévoit en effet que les deux services de renseignement et de sécurité (parmi d'autres services publics) soient consultés dans le cadre des procédures de vérification et de filtrage des investissements étrangers.[231]

Dans son avis, le Comité relevait que ni le texte de l'Accord de coopération lui-même ni les documents joints par le demandeur d'avis n'apportent de clarté quant à la nature et à la portée de l'enquête de filtrage que doivent effectuer la VSSE/le SGRS avant de formuler un avis.

Or, le Comité identifiait plusieurs questions dont les réponses détermineront la nature et la portée de l'enquête de filtrage finale effectuée par le Comité de filtrage interfédéral, et donc l'étendue du contrôle exercé par les autorités belges sur les investissements directs étrangers visés. Par exemple :

- Ne prévoit-on qu'une vérification de la base de données des services de renseignement ?
- Les informations et les données à caractère personnel dont disposent les services de renseignement doivent-elles être mises à jour et adaptées lorsqu'elles sont jugées insuffisantes au regard de l'évaluation d'un investissement direct étranger ?
- Attend-on des services de renseignement qu'ils mènent une enquête complète sur le terrain ? Dans l'affirmative, quels devoirs d'enquête et quels objectifs d'enquête sont attendus concrètement ?

---

230 Avis n° 004/CPR/2022 du 29 juin 2022 portant sur le filtrage des investissements directs étrangers et le rôle de la VSSE et du SGRS en la matière, 6 p.

231 Le SGRS doit ainsi être consulté lorsque les investisseurs étrangers sont « *1° actif(s) dans les secteurs liés à la défense ; 2° actif(s) dans le secteur des biens à double usage au sens de l'article 2, paragraphe 1, du Règlement (CE) n° 428/2009 du Conseil du 5 mai 2009 instituant un régime communautaire de contrôle des exportations, des transferts, du courtage et du transit de biens à double usage ; 3° candidat(s), soumissionnaire(s) ou adjudicataire(s) d'un marché passé ou à passer par ou au nom de la Défense belge ou de l'OTAN incluant un accès à leurs installations* ». Pour sa part, l'avis de la VSSE est exigé lorsque « *l'investissement porte sur les missions légales visées à l'article 7,1° et 3°/1 de la loi du 30 novembre 1998 relative à la des services de renseignement et de sécurité* ».

- En cas d'enquête sur le terrain menée par les services de renseignement, quelles personnes physiques d'une société étrangère doivent faire l'objet d'une enquête (par ex., les membres du conseil d'administration, les personnes qui assurent la gestion journalière, les membres de l'assemblée générale, etc.) ?
- En termes de contenu : les services de renseignement sont-ils chargés, par exemple, de détecter toute structure d'entreprise dissimulée ? Les parties prenantes, par exemple, doivent-elles également être détectées et faire l'objet d'une enquête ?
- Au niveau de la procédure : quels actes d'enquête la VSSE et/ou le SGRS doivent-ils effectuer à cet égard (par ex., échange d'informations avec des partenaires nationaux tels que les autorités fiscales, échange d'informations avec des partenaires étrangers tels que les services de renseignement d'autres États membres de l'UE, *social media intelligence*, etc.) ?

Le Comité recommandait que ces questions fassent l'objet d'un débat parlementaire.

Enfin, le Comité relevait également les similitudes entre la procédure de filtrage décrite dans l'Accord de coopération et les procédures existantes décrites dans la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. Une différence notable entre les deux procédures réside toutefois dans le fait qu'un avis négatif de l'ANS peut faire l'objet d'un recours auprès d'une juridiction administrative spécialement établie à cet effet, c'est-à-dire l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. Le Comité constatait que cette importante garantie procédurale ne figurait pas dans l'Accord de coopération. Or, la protection juridique des personnes physiques et/ou morales qui ont fait l'objet d'un contrôle exige qu'un niveau équivalent de protection juridique soit mis en place entre les deux procédures. De l'avis du Comité, en tant qu'instance de recours naturelle pour les litiges en matière de screening et de sécurité, l'Organe de recours est l'instance appropriée auprès de laquelle introduire un recours contre un avis négatif émis par le Comité de filtrage interfédéral.

Le 2 décembre 2022, le Conseil des ministres a approuvé en deuxième lecture l'avant-projet de loi portant assentiment de l'accord de coopération du 30 novembre 2022 entre l'Etat fédéral et les entités visant à instaurer un mécanisme de filtrage des investissements directs étrangers. Le texte a été adopté en séance plénière de la Chambre des Représentants le 9 février 2023.

VI.5. AVIS SUR LA RÉGLEMENTATION RELATIVE AUX LANCEURS D'ALERTE DU SECTEUR PUBLIC

A la demande de la ministre de la Fonction publique, le Comité permanent R rendu un avis concernant l'avant-projet de loi relative aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et de la police intégrée.[232]

En tant qu'« *organismes du secteur public fédéral* » (projet d'article 6, 1° et 2°), la VSSE et le SGRS entrent dans le champ d'application de ce projet de loi. Le Comité recommandait toutefois que le projet de loi indique également précisément ce qui n'entre *pas* dans son champ d'application.

En ce qui concerne les services précités, le projet d'article 4, § 1er, 1° exclut les activités liées à *« la sécurité nationale »* tandis que le projet d'article 3, § 3, stipule également que « *(l)a présente loi ne porte pas atteinte aux dispositions de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité* ».

L'exposé des motifs de l'avant-projet de loi précisait toutefois que la future loi s'appliquera aux « *atteintes à l'intégrité commises à l'occasion des activités dans l'exécution des missions des services de renseignement et de sécurité* ». Si le Comité souscrit pleinement à l'importance d'instaurer un mécanisme de dénonciation d'atteintes à l'intégrité dans les services de renseignement, il pointait l'impossibilité, dans la pratique, d'établir une distinction claire entre les atteintes à l'intégrité commises *en dehors* de l'exercice des missions de ces services et les atteintes à l'intégrité commises *pendant* l'exercice de celles-ci.

Plus généralement, le Comité constatait que les procédures, les conditions de protection et les modalités de notification proposées dans le projet de loi n'étaient pas adaptées à la nature spécifique et aux modalités d'exécution des activités d'un service de renseignement, non seulement en ce qui concerne les activités liées à la mission (qui n'entrent pas dans le champ d'application du projet de loi) mais également en ce qui concerne les activités dites secondaires, non liées à la mission (qui, elles, entrent dans le champ d'application du projet de loi).

En outre, l'absence d'un système en cascade pour le signalement d'une atteinte à l'intégrité présumée dans la proposition d'article 7, § 1er, alinéa 1er, 2° (c'est-à-dire d'abord un signalement interne, puis un éventuel signalement externe, et seulement ensuite une éventuelle divulgation publique) signifiait, selon le Comité, que la protection des informations classifiées ne pourrait pas être garantie dans la pratique.

Enfin, le Comité soulignait que le manque de clarté entourant la distinction entre les deux réglementations ne profite pas au lanceur d'alerte lui-même. Un lanceur d'alerte ne pourra bénéficier de l'immunité en cas de divulgation que

232 Avis n° 005/CPR/2022 du 30 août 2022 portant sur la réglementation relative aux lanceurs d'alerte du secteur public, 7 p.

si son choix s'est initialement porté sur la réglementation adéquate (à savoir la réglementation reprise dans le projet de loi soumis pour avis *vs.* la réglementation en matière de sécurité nationale). Pour le Comité, cette distinction n'était pas claire dans le projet de loi discuté. On pouvait dès lors difficilement attendre de l'auteur d'un signalement qu'il opère un tel choix.

Pour ces raisons, le Comité recommandait de donner la priorité à l'élaboration, dans les meilleurs délais, du projet de loi déjà annoncé dans l'exposé des motifs, qui règle le statut des lanceurs d'alerte en ce qui concerne les atteintes à l'intégrité dans le domaine de la 'sécurité nationale'. En ce qui concerne spécifiquement le présent projet de loi, le Comité recommandait vivement que les services de renseignement (c'est-à-dire la VSSE et le SGRS) et l'OCAM soient retirés du champ d'application du projet de loi.

La Loi du 8 décembre 2022 réglant les canaux de signalement et la protection des lanceurs d'alerte dans le secteur public a été publiée au Moniteur belge le 23 décembre 2022 et est entrée en vigueur le 2 janvier 2023.[233]

VI.6. AVIS SUR LE SCREENING DES (CANDIDATS) MEMBRES DE LA DÉFENSE ET LA PROCÉDURE GÉNÉRALE DE VÉRIFICATION ET CONTENTIEUX ADMINISTRATIF

Le Comité permanent R a rendu, à la ministre de la Défense, un avis sur une série de projets d'amendements gouvernementaux au projet de loi portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.[234] Le projet d'amendements vise notamment à instaurer l'obligation pour le personnel de la Défense de se soumettre à une vérification de sécurité.[235] La demande d'avis a été introduite fin juillet 2022 auprès du président de l'Organe de recours en matière d'habilitations, attestations et avis de sécurité, qui est le président du Comité permanent R.

L'avis rendu traite de questions qui se rapportent à la compétence de l'Organe de recours ainsi que de questions relatives aux compétences du Comité permament

---

233 Loi du 8 décembre 2022 relative aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée (1), *M.B.*, 23 décembre 2022.

234 Avis n° 001/CPR-PrBOR/2022 du 14 septembre 2022 relatif au screening des (candidats) membres de la Défense, 30 p.

235 Le projet d'article 22*sexies*/2 (amendement 4) dispose que *« (à) moins qu'elle ne soit titulaire d'une habilitation de sécurité, toute personne civile ou militaire du cadre actif ou du cadre de réserve occupant une fonction ou une emploi au sein du Ministère de la Défense, toute personne candidate à une telle fonction ou à un tel emploi, tout militaire détaché en Dehors* (sic) *du Ministère de la Défense, et tout agent civil du Ministère de la Défense mis temporairement à la disposition d'un autre service est soumis à la vérification de sécurité visée à l'article 22sexies (…)* ».

R. C'est pourquoi, en fonction des éléments discutés, les appellations « le président de l'Organe de recours » et « Comité permanent R » sont précisées dans l'avis.[236]

Parmi les remarques formulées dans l'avis, le président de l'Organe de recours a notamment suggéré de modifier le projet sur une série de points afin d'apporter des clarifications (concernant le champ d'application de l'obligation de vérification de sécurité, les avis de sécurité pour lesquels le collège au sein du SGRS serait amené à statuer, les intérêts à protéger par l'imposition de pareille vérification de sécurité, …). Des modifications textuelles ont également été demandées afin de veiller au respect de l'article 109, 4° de la loi du 30 juillet 2018 relative à la protection des données (LPD) qui impose que les données à caractère personnel mobilisées dans le cadre d'une vérification de sécurité soient exactes et mises à jour.

Le président de l'Organe de recours a également constaté que l'introduction d'une procédure de vérification particulière entraine une inégalité de traitement entre les personnes soumises à la procédure générale de vérification existante et celles soumises à la procédure de vérification particulière pour la Défense que les amendements visent à instaurer. Le président de l'Organe de recours a relevé que certaines différences de traitement n'étaient pas (suffisamment) justifiées, et a, de ce fait, formulé des propositions visant à aligner les deux procédures.

Le président de l'Organe de recours a également plaidé pour des modifications dans la L.Org.recours visant à ancrer légalement la jurisprudence de la Cour constitutionnelle selon laquelle l'Organe de recours est une juridiction administrative de pleine juridiction et les avis de sécurité de l'Organe de recours revêtent un caractère contraignant. Des remarques additionnelles ont été formulées concernant la procédure de recours devant l'Organe de recours (notamment la question de la comparution personnelle du requérant en audience).

Le Comité permanent R a par ailleurs formulé une série de remarques concernant les nouvelles incriminations que le projet de loi vise à instaurer et qui ont trait à l'usage inapproprié d'informations classifiées et leur divulgation.

Le Comité a enfin relevé l'existence d'un problème légistique dans la modification de la L.R&S et a plaidé pour une rectification de l'article 4 de la Loi du 14 juillet 2022 au Moniteur belge.

Le projet de loi portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité a été adopté en séance plénière de la Chambre des Représentants le 9 février 2023.

[236] Pour un aperçu de l'ensemble des remarques formulées, il est renvoyé à l'avis intégral disponible sur le site internet du Comité permanent R.

CHAPITRE VII.
LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Le Service d'Enquêtes R du Comité effectue également sur ordre des autorités judiciaires des enquêtes sur les membres des services de renseignement et de sécurité et de l'Organe de coordination pour l'analyse de la menace (OCAM)[237] suspectés d'avoir commis un crime et/ou un délit. Cette compétence est décrite à l'article 40, alinéa 3 de la L.Contrôle.

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le chef du Service d'Enquêtes R sont soumis à l'autorité du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a aucune autorité sur eux. Le président du Comité doit cependant veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle. La raison en est évidente : le Comité a beaucoup d'autres missions légales. Celles-ci pourraient être mises en péril si les dossiers judiciaires nécessitaient un investissement trop conséquent. Le président peut, le cas échéant, se concerter avec les autorités judiciaires quant à la participation des membres du Service d'Enquêtes R à des enquêtes pénales (art. 61*bis* L.Contrôle).

Lorsque le Service d'Enquêtes R effectue des enquêtes pénales, le chef du Service d'Enquêtes R 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 2022, le Service d'Enquêtes R a effectué des devoirs d'enquête dans le cadre de trois dossiers répressifs, sous l'autorité respectivement du substitut du Procureur du Roi de Hal-Vilvorde et du juge d'instruction de Bruxelles, du substitut du Procureur du Roi de Bruxelles et du Parquet fédéral. Seize procès-verbaux ont été dressés dans ce cadre. Étaient visées les infractions suivantes : la 'violation du secret professionnel' par un membre d'un service de renseignement (le Service d'Enquêtes était assisté par la Police judiciaire fédérale), le 'non-respect de la réglementation en matière des habilitations de sécurité' et enfin, la plainte

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

d'un membre d'un service de renseignement pour 'harcèlement' dans le cadre d'une enquête ouverte antérieurement (2021).

Outre les procès-verbaux dressés dans le cadre de ces trois dossiers répressifs, un procès-verbal supplémentaire a été dressé suite à une perquisition effectuée dans le cadre d'une enquête judiciaire sous l'autorité du juge d'instruction de Nivelles. Enfin, un procès-verbal a été établi et adressé au procureur du Roi de Bruxelles sur la base de l'article 29 du Code d'instruction criminelle.

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 renseignement rédige un rapport d'information et le communique dans les quinze jours au chef du Service d'enquêtes R*'. En 2022, le Service d'Enquêtes R n'a reçu aucun signalement en ce sens.

CHAPITRE VIII.
EXPERTISE ET CONTACTS EXTERNES

VIII.1. EXPERT DANS DIFFÉRENTS FORUMS

En 2022, les membres du Comité permanent R et son personnel ont été consultés à plusieurs reprises en tant qu'experts par des institutions publiques et privées nationales et étrangères :

- Le greffier faisant fonction du Comité permanent R a été invité à présenter le fonctionnement du Comité dans le cadre du cours « *Intelligence* » du Master en relations internationales et diplomatie (Université d'Anvers) ;
- Des livres et des articles rédigés par des collaborateurs du Comité ont été publiés dans diverses revues scientifiques et de vulgarisation[238] ;
- Le Président du Comité permanent R a été invité, mi-mai 2022, par la Faculté de Droit, de Science Politique et de Criminologie de l'Université de Liège à présenter la méthodologie des enquêtes de contrôle aux participants à la formation organisée dans le cadre du Certificat d'Université en Analyse du Renseignement ;
- Des échanges ont eu lieu avec des personnes issues du monde académique (Uppsala University, Suède) sur la jurisprudence de la Cour de justice de l'Union européenne ;
- Le greffier faisant fonction a été invité à faire une présentation sur le cadre légal des avis de sécurité en Belgique lors d'une journée d'étude organisée par la Fédération des entreprises belge (FEB) ;
- Le chef du Service d'Enquêtes a participé à une session de formation pour les personnes nouvellement recrutées au sein du SGRS ;

[238] W. VAN LAETHEM, *Handboek Veiligheidsscreenings*, Politeia, Brussel, 2022, 177 p.; B. VERSCHAEVE, 'Het Incident Response Team van de Staatveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht', *Politie en Recht*, 1, 2022, 3-20; C. THOMAS, *BePolitix*, www.absp.be/blog ('La 'liste OCAM' ou l'ancrage de l'organe de coordination au sein du champ antiterroriste belge').

- En mars 2022, une collaboratrice a présenté aux collaborateurs de l'OCAM les résultats de sa recherche doctorale sur l'organe de coordination et l'organisation de la lutte antiterroriste en Belgique[239] ;
- Fin mai, le Comité a participé à l'évaluation UNCTAD[240] « *Law Enforcement – Oversight of Counter-terrorism activities of Law Enforcement Bodies* » ;
- Le greffier faisant fonction a été invité en septembre à faire une présentation sur les screenings de sécurité dans le cadre d'une journée d'étude organisée à huit clos par l'Université d'Anvers (*Security screenings in Europe: A Comparative Analysis*) ;
- Toujours en septembre, le greffier faisant fonction a été invité par la maison d'édition Politeia pour présenter son *Handboek Veiligheidscreenings* (Provinciehuis Vlaams-Brabant, Leuven) ;
- Enfin, en septembre 2022, une collaboratrice a participé à la *Pan-European Conference on International Relations* organisée par la *European International Studies Association* à Athènes.[241]

VIII.2. PROTOCOLE DE COOPÉRATION AVEC LES MÉDIATEURS FÉDÉRAUX

La Loi du 15 septembre 2013[242] désigne les Médiateurs fédéraux comme point de contact central des atteintes suspectées à l'intégrité au sein des autorités administratives fédérales. En septembre 2021, le 'Protocole de coopération du 7 octobre 2021 pour les relations entre les Médiateurs fédéraux et le Comité permanent de contrôle des services de renseignement et de sécurité dans le cadre de la loi du 15 septembre 2013' a été conclu. Le protocole vise à réglementer les modalités de coopération entre les Médiateurs fédéraux et le Comité lorsqu'une atteinte suspectée à l'intégrité dans l'un des deux services de renseignement est signalée aux Médiateurs.

Le cas échéant, les Médiateurs fédéraux peuvent demander au Comité permanent R de désigner un membre du Service d'Enquêtes pour assister le Centre Intégrité - un point de contact central au sein des Médiateurs fédéraux - en tant qu'expert dans la conduite de l'enquête. Les Médiateurs fédéraux n'ont pas eu recours à cette possibilité en 2022. Des accords ont également été conclus dans le protocole concernant les moyens d'investigation, le secret professionnel, la confidentialité et l'échange de bonnes pratiques.

---

239 C. THOMAS, "'Une menace possible et vraisemblable'. Dire et faire la sécurité : l'Organe de Coordination pour l'Analyse de la Menace et la structuration du champ antiterroriste belge", Université Saint-Louis – Bruxelles, décembre 2021.

240 https://unctad.org/about/evaluation.

241 Le titre de l'intervention était : "*Looking beyond traditional intelligence services: CUTA and the fight against terrorism in Belgium*".

242 Loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel, *M.B.* 14 octobre 2013.

Toutefois, la Loi du 8 décembre 2022 relative aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée a été publiée le 23 décembre 2022 au Moniteur belge. Les auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée bénéficient désormais d'une protection conforme à la directive européenne sur les lanceurs d'alerte (Directive 2019/1937). Avec cette loi, le législateur fédéral a en effet transposé ces dispositions en droit interne.[243]

La Loi octroie au Comité permanent R une nouvelle compétence : « *le canal de signalement externe pour les atteintes à l'intégrité au sein du Service général du Renseignement et de la Sécurité ou de la Sûreté de l'Etat est institué auprès du Comité permanent R* ».[244]

VIII.3. COLLABORATION AVEC L'INSTITUT FÉDÉRAL DES 'DROITS DE L'HOMME'

Par le biais d'un protocole de coopération, toutes les institutions participantes (c.à.d. les organismes sectoriels pour la promotion et la protection des droits humains, dont le Comité permanent R) ont accepté d'échanger des pratiques et des méthodes, d'examiner des questions communes et de promouvoir la coopération mutuelle. Des réunions de concertations informelles se tiennent au sein de la Plateforme des droits de l'Homme dont l'Institut Fédéral pour la protection et la promotion des Droits Humains (IFDH) assure la coordination depuis septembre 2022.[245] Le Comité n'a pas participé activement à la Plateforme des droits de l'Homme en 2022.

VIII.4. UNE INITIATIVE MULTINATIONALE EN MATIÈRE D'ÉCHANGE D'INFORMATIONS

La multiplication des échanges de données au niveau international entre les services de renseignement et de sécurité pose un certain nombre de défis aux organes de contrôle nationaux. Les organes de contrôle de (au départ) cinq pays européens (la Belgique, le Danemark, les Pays-Bas, la Norvège et la Suisse) se concertent depuis quelques années afin de relever ces défis, en identifiant des méthodes de travail qui leur permettraient de limiter le risque de lacunes dans le contrôle *(International Overisght Working Group (IOWG))*.

---

243 Le champ d'application ne concerne pas la sécurité nationale.

244 Le canal de signalement externe pour les atteintes à l'intégrité au sein de l'OCAM est institué auprès du Comité permanent P.

245 Depuis février 2023, les Médiateurs fédéraux assurent le secrétariat de la Plateforme des droits de l'Homme.

En mars 2022, une réunion « *staff meeting* » de l'IOWG s'est tenue à Berne, pour la première fois en présentiel depuis le déclenchement de la crise sanitaire. Après une brève présentation par les délégations des derniers développements intervenus au sein de leurs organismes respectifs, les discussions ont principalement porté sur l'avenir et les objectifs de l'IOWG, la plateforme en ligne, les publications des organes de contrôle et le modèle d'analyse de risques présenté par les hôtes suisses de l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens). En octobre 2022, une « *Charter of the Intelligence Oversight Working Group* », non contraignante, a été signée à Londres et l'adhésion des organes de contrôle suédois[246] à l'IOWG a été formellement acceptée.

VIII.5. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

En octobre 2022 s'est tenue, à Londres, la quatrième *European Intelligence Oversight Conference*. Cette conférence, organisée par l'*Investigatory Powers Commissioner's Office (IPCO)*, était articulée en panels autour de thèmes tels que '*Accountablility and Communication – reporting and sharing information with the public*', '*Co-operation across the oversight community in building technological competence*', '*Metrics of Privacy*', '*Saveguards of information from sensitive professions*', '*Sharing information between states*' et '*Development of European jurisprudence and the role of the Council of Europe*'.

Le Président du Comité permanent R a également participé, en juin, à Berlin au troisième workshop de la *European Intelligence Oversight Network* (EION), avec pour thème '*the governance of intelligence services*' *use of commercially available data*' et, en novembre, à l'*International Intelligence Oversight Forum 2022* (IIOF) à Strasbourg, avec notamment pour thème l'article 11 de la Convention 108+ et l'impact du conflit ukrainien sur le contrôle des services de renseignement.

Prévue en 2022, l'arrivée d'un stagiaire suisse de l'Autorité de surveillance indépendante des activités de renseignement (AS-Rens) a finalement été postposée.

Enfin, le Comité permanent R a accueilli, fin juin, une délégation de la Haute Autorité hellénique pour la sauvegarde de l'intimité des communications (ADAE). Lors de cette visite de deux jours, le Comité a présenté à la délégation grecque le système institutionnel et sécuritaire belge ainsi que les missions légales du Comité du système de contrôle à travers toute une série de présentations, suivies de discussions et d'un partage d'expériences avec le Comité au sens large. Par ailleurs, la Présidente de la Chambre et de la Commission de suivi a reçu la délégation grecque, le Comité et plusieurs de ses collaborateurs pour un échange de vues.

---

246 A savoir le *Swedisch Foreign Intelligence Inspectorate (Statens inspektion av försvarunderättelse-verksamhet (SIUN))* et le *Swedish Board of Inventions (Statens uppfinnarnämnd (SUN))*.

CHAPITRE IX.
L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ[247]

Ce chapitre reprend le rapport d'activités approuvé lors de la réunion de mai 2023 par l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité (ci-après l'Organe de recours) ainsi qu'un certain nombre de remarques et suggestions du président de cette juridiction.

IX.1. LE RAPPORT D'ACTIVITÉS DE L'ORGANE DE RECOURS

IX.1.1. INTRODUCTION

L'Organe de recours est, en Belgique, l'unique juridiction administrative compétente pour les contentieux portant sur des décisions administratives dans divers domaines : les habilitations de sécurité, les attestations de sécurité 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.[248]

L'Organe de recours est composé du président du Comité permanent R, de la présidente du Comité permanent P et du président de la Chambre contentieuse de l'Autorité de protection des données. Les trois présidents peuvent être remplacés en cas d'empêchement par un membre-conseiller effectif de l'institution à laquelle appartient le président concerné.

---

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

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

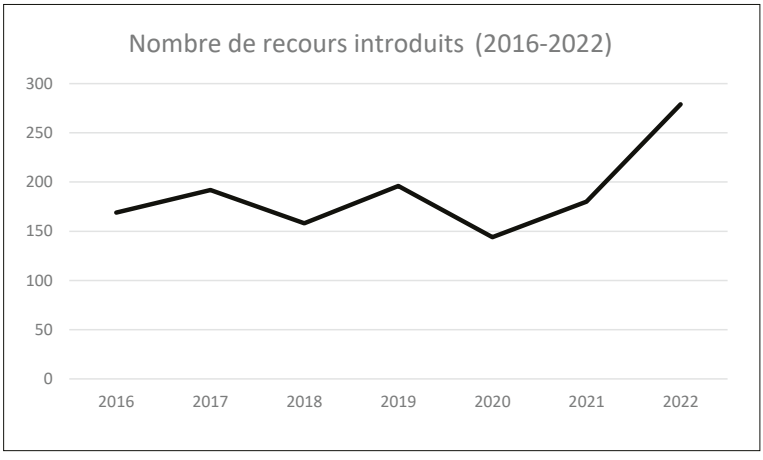
Le président du Comité permanent R assure la présidence de l'Organe de recours. La fonction de greffier est exercée par le greffier du Comité permanent R et le personnel du greffe est le personnel affecté par le Comité. La composition de l'Organe de recours apporte une contribution multidisciplinaire à la délibération de chaque dossier.

Il convient de noter qu'en ce qui concerne les recours, l'administration et le suivi sont entièrement assurés par le Comité permanent R. En effet, le Comité met à disposition toutes les personnes et ressources nécessaires pour assurer l'administration, la correspondance, la tenue des audiences et la rédaction des décisions. Il s'agit, d'une part, de la mise à disposition du président et de ses membres suppléants, de son greffier mais aussi des juristes comme 'greffiers assumés' et du personnel administratif qui forment le greffe de cette juridiction administrative. D'autre part, le Comité permanent R prend en charge, sur son budget, les frais de locaux et de fonctionnement de l'Organe de recours.

IX.1.2. LE DÉTAIL DES CHIFFRES

Cette section reprend les chiffres relatifs à la nature des décisions contestées, la qualité des autorités compétentes et des requérants, ainsi que la nature des décisions de l'Organe de recours dans le cadre des différentes procédures de recours. À des fins de comparaison, les chiffres des six années précédentes sont également repris. En 2022, 279 recours ont été introduits, soit une forte augmentation par rapport à 2021 (180 recours introduits) et 2020 (144 recours introduits). L'Organe de recours a tenu des audiences au rythme minimum de deux par mois. En 2022, il a tenu 41 audiences dont 4 audiences avec des membres des autorités de sécurité.[249]
Au total, 224 décisions finales ont été prises.

Tableau 1. Nombre de recours introduits (2016-2022)



[249] Dont 12 audiences en néerlandais et 29 en français.

Tableau 2. Nombre de recours introduits vs. Nombre de décisions rendues (2016-2022)

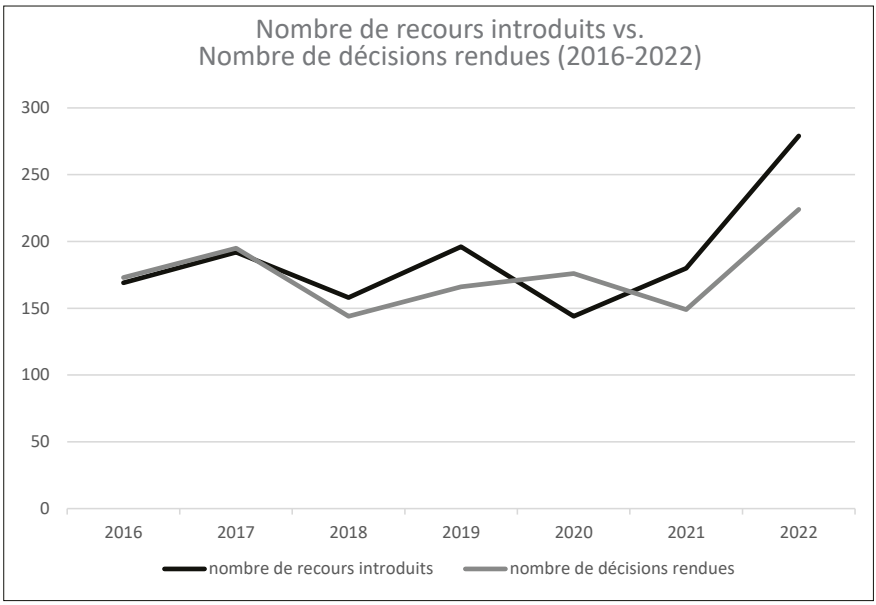


Tableau 3. Autorités de sécurité et autorités de vérification[250] concernées (2016-2022)

	2016	2017	2018	2019	2020	2021	2022
Autorité nationale de sécurité	92	129	113	114	91	86	183
Sûreté de l'État	0	0	0	0	0	4	2
Service Général du Renseignement et de la Sécurité	68	53	32	61	41	84	76
Agence fédérale de Contrôle nucléaire	8	7	10	17	7	6	12
Police fédérale	1	3	3	3	4	0	1
Police locale	0	0	0	1	1	0	5
TOTAL	169	192	158	196	144	180	279

[250] Les « autorités de vérification » sont les autorités compétentes pour la délivrance d'attestations et d'avis de sécurité, comme par exemple la Police fédérale et l'Agence fédérale de Contrôle nucléaire.

Le graphique ci-dessous visualise la répartition des autorités de sécurité et des autorités de vérification concernées par un recours en 2022.

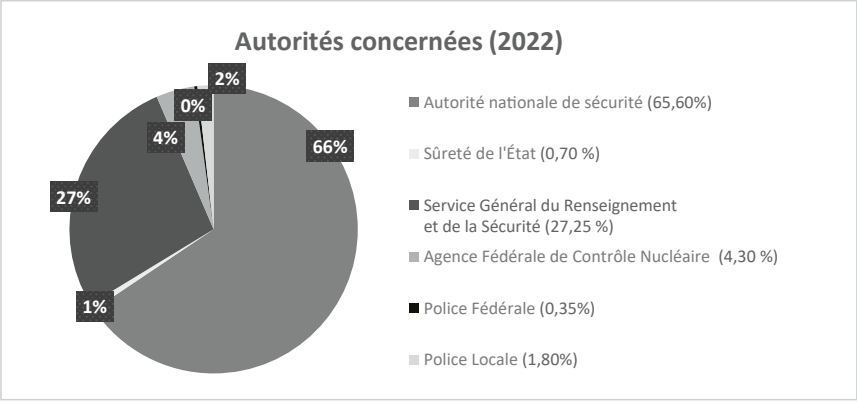


Tableau 4. Nature des décisions contestées

	2016	2017	2018	2019	2020	2021	2022
Habilitations de sécurité (art. 12 et s. L.C&HS)							
Confidentiel	5	1	2	5	0	2	5
Secret	38	33	31	39	27	50	64
Très secret	7	6	3	7	5	8	14
Refus	28	30	26	39	23	37	47
Retrait	9	7	4	16	8	17	15
Refus et retrait	0	0	0	0	0	4	3
Habilitation pour une durée limitée	4	1	1	3	0	1	0
Habilitation pour un niveau inférieur	1	0	0	0	0	0	1
Pas de décision dans les délais	7	2	5	0	0	1	17
Pas de décision dans les nouveaux délais	1	0	0	0	0	0	0
Autres					1[251]		
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	**50**	**40**	**36**	**51**	**32**	**60**	**83**
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)							
Refus	1	3	3	1	0	3	2
Retrait	0	0	0	0	0	0	0
Pas de décision dans les délais	0	0	0	0	0	0	0

251 'Mise en garde du requérant'. Une personne s'était vue octroyer l'habilitation de sécurité pour cinq ans avec une mise en garde et est allée en recours contre cette mise en garde.

	2016	2017	2018	2019	2020	2021	2022
Attestations de sécurité lieu ou événement (art. 22*bis*, al.2 L.C&HS)							
Refus	9	20	15	12	6	2	21
Retrait	0	0	0	0	0	0	2
Pas de décision dans le délai	0	0	0	0	0	1	2
Attestations de sécurité lieu secteur nucléaire (art. 8*bis* L.C&HS)							
Refus	7	7	11	17	7	6	12
Retrait	1	0	0	0	0	0	0
Pas de décision dans le délai	0	0	1	0	0	0	0
Avis de sécurité (art. 22*quinquies* L.C&HS)							
Avis négatif	101	122	92	115	99	108	157
Pas d'avis	0	0	0	0	0	0	0
Révocation d'avis positif	0	0	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	0	0
Refus de l'ANS d'effectuer des vérifications pour des attestations de sécurité	0	0	0	0	0	0	0
Décision d'une autorité administrative d'exiger des avis de sécurité	0	0	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des avis de sécurité	0	0	0	0	0	0	0
SOUS-TOTAL ATTESTATIONS ET AVIS	**119**	**152**	**122**	**145**	**112**	**120**	**196**
TOTAL DÉCISIONS CONTESTÉES	**169**	**192**	**158**	**196**	**144**	**180**	**279**

Tableau 5. Nature du requérant

	2016	2017	2018	2019	2020	2021	2022
Fonctionnaire	2	4	5	4	8	16	47
(candidat) Militaire	23	20	8	27	39	81	69
Particulier	139	164	140	163	95	80	157
Personne morale	5	4	5	2	2	3	6

Le graphique ci-dessous visualise la répartition 'nature du requérant' en 2022.

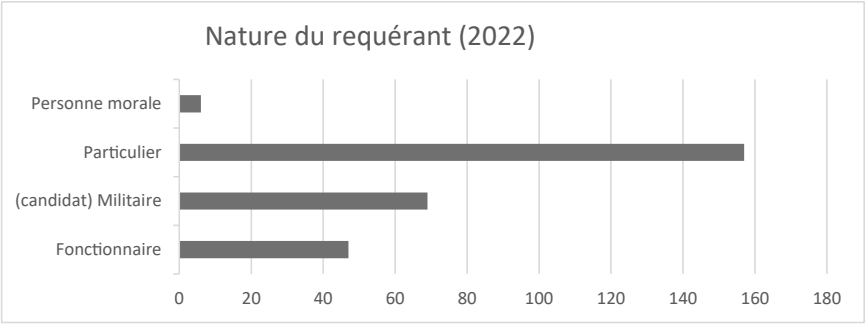


Tableau 6. Langue du requérant

	2016	2017	2018	2019	2020	2021	2022
Français	99	115	83	101	83	86	201[252]
Néerlandais	70	77	75	95	61	94	123[253]
Allemand	0	0	0	0	0	0	0
Autre langue	0	0	0	0	0	0	0

Tableau 7. Actes du greffe

	2016	2017	2018	2019	2020	2021	2022
Demande du dossier complet (1)	167	191	154	191	141	180	279
Demande d'informations complémentaires (2) et rappels adressés aux autorités de sécurité et de vérification (3)	23	36	12	39	41	45	146[254]

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

252 181 dossiers francophones en 2022 et 20 dossiers francophones des années antérieures mais traités en 2022.

253 98 dossiers néerlandophones en 2022 et 25 dossiers néerlandophones des années antérieures mais traités en 2022.

254 Dont 76 demandes d'informations complémentaires et 70 rappels adressés aux autorités de sécurité.

(2) L'Organe de recours peut également demander tout complément d'informations qu'il juge nécessaire pendant la procédure. Dans la pratique, le greffe se charge de demander aux autorités de compléter les dossiers.
(3) L'art. 6 de l'AR Org.recours prévoit les délais pour la communication des dossiers par les autorités de sécurité et de vérification. Ces délais prennent cours lorsque le greffier transmet une copie du recours à l'autorité de sécurité ou de vérification concernée. Ils varient selon la nature de l'acte attaqué. Ainsi, l'autorité de sécurité ou de vérification doit communiquer son dossier dans les 15 jours en ce qui concerne les habilitations de sécurité, dans les 5 jours en matière d'attestations de sécurité et dans les 10 jours si le recours porte sur un avis de sécurité. Lorsque ces délais ne sont pas respectés, le greffe prend les contacts nécessaires. Ces données sont comptabilisées à partir de 2019.

Tableau 8. Actes juridictionnels interlocutoires pris par l'Organe de recours [255]

	2016	2017	2018	2019	2020	2021	2022
Audition d'un membre d'une autorité (1)	10	0	1	6	1	4	12
Décision du président (2)	0	0	0	0	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (3)	54	80	72	77	50	77	118
Décisions avant dire droit (4)	/	/	/	9	9	19	28

(1) L'Organe de recours peut décider d'entendre les membres des services de renseignement et de police ou des autorités de sécurité ou de vérification qui ont participé à l'enquête ou à la vérification de sécurité.
(2) Le président de l'Organe de recours peut décider de permettre au membre du service de renseignement de garder secrètes certaines données pendant son audition.
(3) Si le service de renseignement ou de police concerné le demande, l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant.
(4) Il peut s'agir par exemple d'une décision de jonction de deux dossiers ou de demander un complément d'informations à propos de la situation d'un dossier judiciaire. Ces données sont comptabilisées à partir de 2019.

[255] Le nombre d'"actes juridictionnels interlocutoires' (tableau 6), les 'manières dont les requérants font usage de leurs droits de défense' (tableau 7), ou encore la 'nature des décisions de l'Organe de recours' (tableau 8) ne correspondent pas nécessairement au nombre de requêtes introduites (voir tableaux 1 à 4). En effet, certains dossiers ont par exemple déjà été ouverts en 2021, alors que la décision n'a été rendue qu'en 2022.

Tableau 9. Manière dont le requérant fait usage de ses droits de défense

	2016	2017	2018	2019	2020	2021	2022
Consultation du dossier par le requérant et/ou l'avocat	87	105	69	96	96	97	136
Audition du requérant (assisté ou non d'un avocat)[256]	127	158	111	143	135	151	192

Tableau 10. Nature des décisions de l'Organe de recours

	2016	2017	2018	2019	2020	2021	2022
Habilitations de sécurité (art. 12 et s. L.C&HS)							
Recours irrecevable	0	3	0	1	1	0	2
Recours sans objet	7	0	4	3	3	3	5
Recours non fondé	18	13	12	12	16	11	20
Recours fondé (avec octroi partiel ou complet)	24	24	12	25	14	17	31
Devoir d'enquête complémentaire par l'autorité	2	0	1	1	2	1	1
Délai supplémentaire pour l'autorité	2	1	1	0	3	0	3
Donne acte de retrait de recours	0	0	3	2	2	11	2
Attestations de sécurité documents classifiés (art. 22*bis*, al.1 L.C&HS)							
Recours irrecevable	0	1	0	0	0	0	0
Recours sans objet	0	1	0	0	0	0	0
Recours non fondé	1	0	1	1	0	2	0
Recours fondé (avec octroi)	1	1	0	3	0	2	1
Donne acte de retrait de recours	-	-	-	1	0	0	0
Attestations de sécurité pour lieux ou événements (art. 22*bis*, al.2 L.C&HS)							
Recours irrecevable	0	1	2	4	2	0	4
Recours sans objet	0	1	0	0	0	0	1
Recours non fondé	2	12	2	4	4	1	6
Recours fondé (avec octroi)	4	7	3	4	1	0	9

[256] La L.Org.recours prévoit l'assistance d'un avocat à l'audience mais pas la représentation par ce dernier. À noter que, dans le cadre de certains dossiers, le requérant (assisté ou non de son avocat) est auditionné à plusieurs reprises.

	2016	2017	2018	2019	2020	2021	2022
Donne acte de retrait de recours	0	1	2	0	0	0	2
Attestations de sécurité pour le secteur nucléaire (art. 8*bis* §2 L.C&HS)							
Recours irrecevable	1	1	0	1	0	0	0
Recours sans objet	1	0	1	0	0	0	1
Recours non fondé	0	1	1	5	2	2	6
Recours fondé (avec octroi)	7	5	6	7	4	6	5
Donne acte de retrait de recours	-	-	2	0	0	0	0
Avis de sécurité (art. 22*quinquies* L.C&HS)							
Organe de recours non compétent	0	20[257]	12	0	0	0	0
Recours irrecevable	15	10	3	7	8	3	18
Recours sans objet	0	1	3	1	6	4	11
Confirmation de l'avis négatif	42	49	46	40	51	47	59
Réformation en avis positif	46	41	27	43	52	34	37
Donne acte de retrait de recours	0	1	0	1	5	5	4
Recours contre des actes normatifs d'une autorité administrative (art. 12 L. Org.recours)	0	0	0	0	0	0	0
TOTAL	**173**	**195**	**144**	**166**	**176**	**149**	**228**

IX.2. REMARQUES ET SUGGESTIONS DU PRÉSIDENT DE L'ORGANE DE RECOURS

1. Le 9 février 2023, la Chambre a adopté le projet de loi portant modification de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité.[258]

   À la suite de l'entrée en vigueur de la loi, le 31 décembre 2023, la Sûreté de l'État exercera les compétences de l'Autorité nationale de sécurité et sera dorénavant chargée de la délivrance, la modification, la suspension et le retrait des habilitations de sécurité, mis à part pour la Défense. La Police fédérale

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

[258] 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 2022-2023, n° 55-2443/009.

exercera une compétence générale en matière de délivrance, de modification, de suspension et du retrait des avis de sécurité.

Ces changements d'autorités de sécurité auront certainement un impact sur le fonctionnement de la juridiction. Le temps permettra à chacun d'en analyser les effets. Nul doute qu'à l'occasion des prochains rapports annuels, un bilan pourra être réalisé.

2. En 2022, à l'occasion de deux recours, l'Organe de recours a été amené à examiner des questions relatives à l'enquête de sécurité en matière d'habilitation de sécurité. A chaque fois, le citoyen soulevait des problèmes de légalité de l'interview réalisée par les services de renseignement. L'Organe de recours a rappelé à ces occasions qu'il appartenait dorénavant aux services, d'une part, de faire parapher l'interview par le demandeur d'habilitation de sécurité et, d'autre part, en cas de méconnaissance d'une des langues nationales, de faire assister la personne concernée par un interprète.

3. L'Organe de recours a pris acte de la volonté du gouvernement d'étendre le principe des vérifications de sécurité pour l'octroi d'avis de sécurité à tous les collaborateurs de la Défense, à un rythme quinquennal.[259] Outre cette adaptation législative, le ministre de la Justice a également fait savoir que d'autres modifications seraient initiées pour les 16.000 personnes travaillant dans le secteur portuaire. Ces modifications ont des conséquences pour le devenir de l'Organe de recours. A aucun moment, les textes n'ont appréhendé cette question de la charge de travail. Pourtant, il est important de permettre aux membres du greffe de travailler dans de bonnes conditions.

4. L'Organe de recours précise que l'évolution du contentieux qui lui sera soumis n'a pas été pris en compte à ce jour par la Chambre, compétente en ce qui concerne le budget de l'institution via le Comité permanent R. En décembre 2022, alors que l'Organe de recours sollicitait, rien que pour l'accroissement en 2022 de 50% du contentieux, une augmentation de cadre de 2 unités (une secrétaire et un juriste), la Chambre a marqué son accord pour l'engagement d'un juriste. La charge administrative ne cesse d'évoluer et l'augmentation du contentieux pose problème.

5. L'absence de digitalisation de la juridiction, qui a été sollicitée auprès de la Chambre, constitue assurément un autre problème. Il est dénoncé depuis des années mais sans effet. De la même manière, le projet de proposition de loi préparé pour simplifier la procédure et améliorer l'accès du justiciable reste sans suite. Ainsi, le citoyen se voit toujours confronté à des délais de recours de huit

259 Voir l'avis rendu à ce sujet par le Comité (VI.6. Screening des (candidats) membres de la Défense – Procédure générale de vérification et contentieux administratif particulier).

jours, des procédures lourdes qui ne répondent plus aux exigences modernes d'accessibilité à la justice. Est-il normal que les particuliers et leurs avocats, qui interviennent dorénavant dans deux dossiers sur trois, ne puissent consulter leur dossier à distance ?

6. Nous devons relever que notre demande de pouvoir bénéficier de la franchise postale a été relayé, par la présidente de la Chambre, auprès du ministre compétent mais sans succès. L'Organe de recours est toujours tenu, par la loi, d'envoyer tous ses courriers par lettre recommandée à la poste. La loi ne lui permet pas de recourir au mail. Il en a résulté, en 2022, une dépense de plus de 15.000 euros pour les frais de poste.

Enfin, je veux remercier tous les collaborateurs de l'Organe de recours : greffier, greffiers assumés, juristes, secrétaires et toutes les personnes qui permettent que les justiciables reçoivent sans délai leur décision. Je souligne les qualités humaines et la disponibilité du greffe car le justiciable, lorsqu'il s'adresse par téléphone ou par mail au greffe, bénéficie d'une réelle écoute et reçoit une réponse adéquate à ses interrogations. Les quarante-et-une audiences tenues en 2022 n'ont pas pu se tenir sans l'aide essentielle de nos collègues Présidents et membres des Comité permanent P et de la Chambre contentieuse de l'Autorité de protection des données. Je remercie aussi le conseiller Pieter-Alexander De Brock qui a présidé la chambre néerlandophone de l'Organe de recours.

CHAPITRE X.
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

X.1. LA COMPOSITION DU COMITÉ PERMANENT R

La composition du Comité est restée identique en 2022 : Serge Lipszyc (F), premier substitut de l'auditeur du travail près l'auditorat du travail de Liège, a continué à remplir sa mission de président. Pieter-Alexander De Brock (N)[260], fonctionnaire, et Thibaut Vandamme (F), substitut du procureur du Roi de l'arrondissement du Luxembourg, ont eux aussi poursuivi l'exercice de leur mandat de conseiller.

La Chambre a par contre procédé à la nomination du nouveau greffier[261], en la personne de Frédéric Givron (F), qui a prêté serment le 26 avril 2022.[262]

En 2022, le Président du Comité permanent R a envoyé deux courriers à la Présidente de la Chambre des représentants afin de solliciter une extension du cadre du personnel. Le premier courrier, daté du 8 juin 2022, a été envoyé par le Comité en tant qu'Autorité de protection des données, et le second l'a été le 2 août 2022, afin d'obtenir des renforts pour l'Organe de recours de matière d'habilitations, d'attestations et d'avis de sécurité. Nonobstant l'investissement de la Chambre dans le cadre des objectifs de synergies, auxquels le Comité a maintenu son soutien, le Comité a, en effet, jugé nécessaire de solliciter un renfort.[263] Il n'est en effet pas en mesure de mener à bien toutes les missions légales ni de répondre

---

260 Comité permanent de contrôle des services de renseignement et de sécurité - nomination du second suppléant du membre néerlandophone - Filip Vanneste (*C.R.I.*, Chambre, 2021-2022, 29 mars 2022, PLEN 171, p. 67).

261 Le 19 mai 2022, en application de l'article 20, deuxième alinéa du Règlement d'ordre intérieur du Comité permanent R, la Chambre a octroyé à Wouter De Ridder, ancien greffier, le titre honorifique de sa fonction (*C.R.I.*, Chambre, 2021-2022, 19 mai 2022, PLEN 181, p. 58).

262 Nomination du greffier du Comité permanent de contrôle des services de renseignements et de sécurité, *Doc. parl.*, Chambre, 2021-2022, n° 55-2597/1 et résultat du scrutin (*C.R.I.*, Chambre, 2021-2022, 29 mars 2022, PLEN 171, p. 75).

263 En ce sens, deux offres d'emploi ont été publiées : le recrutement pour l'entrée en service immédiate et la constitution d'une réserve de recrutement d'un(e) secrétaire francophone statutaire (m/f/x) (niv. B) (*M.B.* 6 septembre 2022) et le recrutement, par détachement, et la constitution d'une réserve de recrutement de commissaires-auditeurs/trices francophones et néerlandophones (m/f/x), dotés de connaissances particulières en ICT/Data, pour le Service d'Enquêtes du Comité permanent R (*M.B.* 12 juillet 2022).

de manière adéquate aux différentes demandes formulées par la Chambre. Le 15 décembre 2022, la Commission de la Comptabilité de la Chambre des représentants a approuvé l'augmentation du cadre du personnel du Comité permanent R. Sur les sept équivalents temps plein (ETP) demandés par le Comité, la Commission a accordé une extension de cadre de deux ETP (un(e) juriste et un(e) enquêteur(rice)) à partir du 1er avril 2023.[264]

X.2. LE PROJET 'RIBORN'

À l'entame de 2022, le Comité permanent R a lancé, avec l'appui du SPF BOSA, un projet visant l'amélioration de l'organisation sur la base d'une vision partagée et la consultation de ses principaux partenaires[265] dans une vision à 360°.

Ce projet dénommé 'RIborn', a mobilisé les énergies tout au long de l'année, comme en témoignent les réunions qui se sont tenues à intervalles réguliers. Un workshop a été organisé en juin 2022 au sein des locaux du SPF BOSA. Concernant ce volet interne du projet, le SPF BOSA a livré un rapport de synthèse de la consultation des collaborateurs reprenant treize objectifs d'amélioration. Les membres du Comité, Président et Conseillers, ont ensuite effectué, dans le courant du dernier trimestre de l'année, un exercice visant à transformer ces objectifs d'amélioration en projets ou plans d'actions et à les prioriser. Le projet devrait être achevé en 2023.

En outre, le Comité permanent R a souhaité consulter ses principaux partenaires externes en vue d'améliorer la collaboration. À l'issue d'une réflexion approfondie basée sur des critères précis (nature, intérêt et fréquence des relations), douze partenaires[266] ont été retenus. À ce stade, neuf partenaires ont été sollicités par l'équipe de projet au cours de trois vagues successives.

---

264 Cour des comptes, Cour constitutionnelle, Conseil supérieur de la Justice, Comité Permanent de contrôle des services de police, Comité Permanent de contrôle des services de renseignement et de sécurité, Médiateurs fédéraux, Autorité de protection des données, Commissions de nomination pour le notariat, Commission BIM, Organe de contrôle de l'information policière, Commission fédérale de déontologie, Conseil central de surveillance pénitentiaire, Institut fédéral des droits humains - Travaux des groupes de travail dans le cadre du projet de synergie - Comptes de l'année budgétaire 2021 - Ajustements budgétaires de l'année budgétaire 2022 - Propositions budgétaires pour l'année budgétaire 2023, *Doc. parl.*, Chambre 2022-2023, n° 55-3050/001, pp. 70 et suivantes. Le budget a été validé en séance plénière de la Chambre des représentants le 22 décembre 2022.

265 '*Samenwerkingsovereenkomst. Opstellen van een nieuwe organisatie-gedragen visie en actieplan voor het Vast Comité van Toezicht op de Inlichtingen- en veiligheidsdiensten*' (10 janvier 2022).

266 La VSSE, le SGRS, l'OCAM, la Commission BIM, l'ANS, le Comité permanent P, le C.O.C., l'APD et le Collège des Procureurs Généraux, le Ministre de la Justice, la Ministre de la Défense et la Présidente de la Chambre et de la Commission de suivi P et R.

X.3. RÉUNIONS AVEC LA COMMISSION DE SUIVI

La composition de la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de Contrôle des services de renseignement et de sécurité (la Commission de suivi) a connu quelques changements en 2022. En étaient membres avec voix délibérative Peter Buysrogge (N-VA), Yngvild Ingels (N-VA), Julie Chanson/Gilles Vanden Burre (Ecolo-Groen), Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Denis Ducarme (MR), Servais Verherstraeten (CD&V), Nabil Boukili (PVDA-PTB), Tim Vandenput (Open Vld) et Bert Moyaers (Vooruit). La Présidente de la Chambre, Eliane Tillieux (PS), assume la présidence de la Commission. Georges Dallemagne (Les Engagés) participe en tant que membre sans voix délibérative.

Dans le courant de l'année 2022, quatre réunions ont eu lieu à huis clos avec la Commission de suivi pour discuter des enquêtes de contrôle que le Comité permanent R avait clôturées. La Commission s'est également penchée sur le fonctionnement interne du Comité permanent R.

Le *Rapport d'activités 2021* du Comité permanent R a été discuté lors de la réunion de la Commission de suivi du 8 juin 2022.[267] Une série de thématiques ont particulièrement retenu l'attention de la Présidente et des Députés, parmi lesquelles le suivi des recommandations de la commission d'enquêtes 'Attentats', le suivi des mandataires politiques, le screening régulier des militaires, le suivi des détenus condamnés pour terrorisme ou encore la sécurité de l'État. En guise de conclusion, la Commission a pris *'acte du Rapport d'Activités 2021 du Comité permanent R et souscrit à ses recommandations*'.[268]

X.4. COLLABORATION ET RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

L'article 52 L.Contrôle prévoit qu'au minimum deux réunions se tiennent annuellement entre le Comité permanent R et le Comité permanent P. Étant donné notamment l'absence de nouvelles enquêtes communes, seule une réunion formelle s'est tenue le 12 octobre 2022.

---

267 La Commission se réfère à cet effet à l'article 66*bis*, § 3,1° L.Contrôle, tel que modifié par la loi du 6 janvier 2014 modifiant diverses lois de réformes institutionnelles, *M.B.* 31 janvier 2014.

268 *Doc. parl.* , Chambre 2021-22, 55-2745/001, 30 juin 2022 (Rapport d'activités 2021 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).

En 2021, les deux Comités avaient chargé leurs Services d'enquêtes respectifs de préparer des procédures de travail pour le traitement des plaintes et des enquêtes de contrôle conjointes. En 2022, la finalisation de la procédure commune de traitement des plaintes a pu être actée. Quant à la seconde, elle est toujours en cours d'élaboration.

Enfin, le Comité permanent P continue à fournir son appui dans le cadre de l'accès du service d'Enquêtes R à la Banque de données nationale générale (BNG), notamment via la transmission des informations nécessaires suite aux mises à jour techniques et le coaching ponctuel d'une personne de référence quand cela s'avère nécessaire.[269, 270]

X.5. LE '*DATA PROTECTION OFFICER*' AU COMITÉ

En mai 2018, le Comité permanent R a désigné un *Data Protection Officer* (DPO) ou délégué à la protection des données pour les traitements de données à caractère personnel en vertu du 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 (Règlement Général sur la Protection des Données ou RGPD) et la 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 et 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. Le DPO exerce également cette fonction pour plusieurs autres institutions à dotation.

En 2022, outre les tâches statutaires telles que l'information et la sensibilisation du personnel à la protection des données, l'accent a été mis sur le partage de conseils concernant une série de traitements de données à caractère personnel dans le

269 L'engagement, en juin 2021, d'un commissaire auditeur ayant un profil judiciaire et une expérience en gestion de l'information policière a renforcé la capacité et les compétences internes d'utilisation de la BNG au sein du service d'Enquêtes R.

270 En octobre 2017, le Comité permanent R a signé un protocole d'accord avec la Police fédérale concernant l'application de l'arrêté royal du 30 octobre 2015 relatif à l'accès direct du Comité permanent de contrôle des services de renseignement et de sécurité et de son Service d'enquêtes aux données et informations de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police (*M.B.* 20 novembre 2015).

cadre de la gestion du personnel et de l'administration.[271] L'objectif est également de fournir des informations encore plus ciblées aux membres du personnel sur le traitement de leurs données à caractère personnel par le Comité permanent R en tant que responsable de traitement.

X.6. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Le budget 2022 du Comité permanent R a été fixé à 5,215 millions d'euros, un montant identique à celui de 2021.[272]

Les sources de financement attribuées par la Chambre des représentants[273] sont les suivantes : 74,93 % au titre du budget de dotation, 21,53 % de boni de 2020 et 3,54 % du boni (hypothétique) de 2021.

L'exécution du budget 2021 a produit un boni comptable de 1,616 millions d'euros, représentant la différence entre le budget approuvé et les dépenses constatées.

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

Le dégagement d'un boni comptable considérable provient essentiellement de l'écart temporel existant entre l'approbation des budgets et l'entrée effective en service du personnel à cause de la longueur des procédures de recrutement et de l'obtention des habilitations de sécurité requises. Cela, cumulé au gel du budget affecté au projet de digitalisation décidé par la Chambre, a généré un boni important.

---

271 Le délégué à la protection des données a notamment fourni un avis interne sur la surveillance caméra suite auquel un registre a été établi et la notification a été formalisée conformément à la nouvelle « loi Caméras » (Loi du 30 juillet 2018 modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, en vue d'améliorer la cohérence du texte et sa conformité avec le Règlement général sur la protection des données (RGPD), *M.B.* 31 août 2018).

272 *C.R.I.* Chambre 2021-22, PLEN 154, 17.

273 *Doc. parl.* Chambre 2021-22, 55-2368/001, 44-45.

X.7. MISE EN ŒUVRE DES RECOMMANDATIONS DE L'AUDIT DE LA COUR DES COMPTES

À la demande de la Commission de la Comptabilité de la Chambre des représentants, la Cour des comptes a, dès 2017, initié une enquête sur les institutions à dotation, conjointement à Ernst & Young. Le rapport d'audit, transmis fin mars 2018, reprenait des recommandations concernant les 'missions' des neuf institutions à dotation concernées par l'audit, dont le Comité permanent R.[274]

En avril 2021, un accord avait été trouvé au sein de la Commission de la Comptabilité sur les synergies à initier entre les institutions concernées. Il s'agissait notamment de mettre en place un centre de services partagés. Il a également été décidé d'harmoniser les statuts du personnel et les barèmes des institutions concernées ainsi que de rationaliser le parc automobile des institutions.

Les travaux se sont poursuivis en 2022, notamment avec une proposition de loi relative à l'harmonisation des statuts. Le Comité a organisé des réunions internes afin d'informer ses collaborateurs et, dans la mesure du possible, de répondre à leurs questions et préoccupations.

Dans le cadre de l'installation envisagée de la Commission BIM dans une section des locaux du Comité permanent R, le Comité a fourni à la Chambre une estimation des coûts que cette installation engendrerait.

X.8. FORMATIONS

Compte tenu de l'intérêt pour l'organisation, le Comité permanent R encourage ses membres et ses collaborateurs à suivre des formations générales (en informatique, en management, etc.) ou propres au secteur, ou encore à participer à des conférences. En 2022, plusieurs membres du personnel ont assisté aux journées d'étude et participé aux formations reprises dans le tableau ci-dessous.

274 *Doc. parl.* Chambre 2018-19, 54-3418/003.

DATE	TITRE	ORGANISATION	LIEU
26-27 janvier 2022	Intelligence, surveillance & oversight: tracing connections & contestations	GUARDINT	En ligne
Mars – avril 2022	Formation Personne de confiance (N)	IDEWE	Louvain
12 mai 2022	Fusion Conference : La communication polarisante en tant que vecteur de radicalisation	Institut Egmont et Organe de coordination pour l'analyse de la menace (OCAM)	Bruxelles
19 mai 2022	Extreme Right: what are the risks for Belgium?	Royal Higher Institute for Defense	Bruxelles
Mai – juin 2022	Formation Personne de confiance (F)	Securex	Bruxelles
14 juin 2022	Public Security Exhibition 2022	British Embassy Brussels & ADS Group	Bruxelles
1-4 septembre 2022	Pan-European Conference on International Relations	European International Studies Association	Athènes
5-9 septembre 2022	Formation de rappel pour les réservistes de la Défense	Ecole du Renseignement et de la Sécurité	Heverlee
5 octobre 2022	Utilisation d'armes et exercices de tir	Défense	Leopoldsburg
10 octobre 2022	Utilisation d'armes et exercices de tir	Défense	Bruxelles
28 octobre 2022	Rétention des données	Groupe de Recherche en matière Pénale et Criminelle (GREPEC) de l'Université Saint-Louis à Bruxelles & Vrije Universiteit Brussel	Bruxelles
Septembre – décembre 2022	Hautes Etudes de sécurité et de défense (4e cycle)	Institut royal supérieur de défense	Bruxelles
Septembre – décembre 2022	Formation IT	VSSE	Bruxelles
Novembre - décembre	Formation IT	VSSE	Bruxelles
5 décembre 2022	Fusion Conference : Retour sur 5 années de CSIL-R. Bonnes pratiques, leçons et défis	Institut Egmont et Organe de coordination pour l'analyse de la menace (OCAM)	Bruxelles

En octobre 2022, une collaboratrice a également présenté en interne les résultats de sa recherche doctorale sur l'OCAM et l'organisation de la lutte antiterroriste en Belgique.

CHAPITRE XI.
RECOMMANDATIONS

À la lumière des enquêtes de contrôle, des contrôles et des inspections clôturés en 2022, le Comité permanent R formule les recommandations reprises ci-après. Ces recommandations portent à la fois sur la coordination et l'efficacité des services de renseignement, de l'Organe de coordination pour l'analyse de la menace (OCAM) et des services d'appui et sur l'optimalisation des possibilités d'enquête du Comité permanent R.[275]

XI.1. RECOMMANDATIONS RELATIVES À LA COORDINATION ET À L'EFFICACITÉ DES SERVICES DE RENSEIGNEMENT, DE L'OCAM ET DES SERVICES D'APPUI

XI.1.1. RENFORCER L'ÉCHANGE D'INFORMATIONS ENTRE LA VSSE ET LES ÉTABLISSEMENTS PÉNITENTIAIRES[276]

Le Comité invite le ministre de la Justice à organiser de manière régulière des sessions d'information au sein de chaque établissement pénitentiaire afin de veiller à ce que toutes les prisons soient sensibilisées à l'importance et à l'intérêt de l'échange d'informations avec la VSSE.

[275] En 2022, aucune recommandation relative à la protection des droits que la Constitution et la loi confère aux personnes n'a été formulée.

[276] Les recommandations reprises aux points XI.2.1 à XI.2.8. sont issues de l'enquête sur le suivi par la VSSE des condamnés pour terrorisme qui ont été libérés (Chapitre I.1.).

XI.1.2. INVESTIR DANS UN DIALOGUE CONSTRUCTIF AVEC LES ACTEURS SOCIO-PRÉVENTIFS

Le Comité recommande à la VSSE d'élaborer un plan d'action visant à investir dans ses relations avec les acteurs socio-préventifs[277], non pas dans l'unique but de récolter de l'information mais d'obvier tout sentiment de méfiance, en engageant une réflexion plus large sur le phénomène de radicalisation en prison et ses ressorts psycho-sociaux.

XI.1.3. OPÉRATIONNALISATION ET ÉVALUATION DU PROJET PILOTE AUTOUR DES COORDINATEURS DE SÉCURITÉ AU SEIN DES PRISONS

Lancé en décembre 2021, le projet pilote de la Direction Générale Établissements pénitenciaires (DG EPI) autour des coordinateurs de sécurité[278] ne pourra être évalué qu'à moyen terme. Si le Comité juge le projet prometteur, il conviendra d'évaluer, d'une part, la compatibilité d'une telle fonction avec des tâches de management et, d'autre part, les modalités de la coopération avec la VSSE. Le Comité encourage dès lors une concertation entre la VSSE et la DG EPI quant à l'opérationnalisation des missions et la formation des coordinateurs de sécurité. Le Comité invite le ministre de la Justice à lui remettre un rapport d'évaluation du projet pilote au premier semestre 2024.

XI.1.4. SIGNATURE DU (NOUVEAU) PROTOCOLE D'ACCORD VSSE – DG EPI[279]

Le Comité invite le ministre de la Justice à clarifier, dans le protocole d'accord entre la VSSE et la DG EPI, la coopération concrète entre la VSSE et les coordinateurs de sécurité, et à prendre toutes les mesures nécessaires visant la finalisation, d'ici la fin 2022, du protocole en discussion depuis 2016.

---

277 Il s'agit par exemple d'enseignants, de collaborateurs des centres PMS, de professionnels du secteur du bien-être et de la santé, de consultants d'un service public de l'emploi, de travailleurs du secteur de la jeunesse,…

278 Il s'agit de collaborateurs de la DG EPI qui agissent comme point de contact pour la Sûreté de l'Etat.

279 Dans la préface du rapport annuel de la VSSE, l'Administratrice générale a.i. fait reference à un accord conclu avec la DG EPI qui « *règle, entre autres, le contenu et les dispositions légales concernant la circulation de l'information entre les deux services* ». In VSSE, *Intelligence report 2021-2022* (www.vsse.be).

XI.1.5. PRUDENCE DANS L'ÉCHANGE DE DONNÉES AVEC DES PARTENAIRES ÉTRANGERS

Le Comité invite la VSSE à faire preuve de prudence dans le partage, avec certains partenaires étrangers, de la liste des détenus inscrits dans la banque de données commune *Terrorist Fighters* (BDC TF) et arrivant à fond de peine. Le Comité appelle en outre à une plus grande attention au respect du droit à l'oubli des détenus ayant purgé leur peine et qui ne constituent plus une menace aux yeux des services belges. Le Comité rappelle également que l'extraction de listes des BDC est soumise à des dispositions légales strictes et cumulatives.[280]

XI.1.6. UNE COOPÉRATION RENFORCÉE ENTRE LE SGRS ET LA VSSE DANS LE CADRE DU SUIVI DES (ANCIENS) DÉTENUS CONDAMNÉS POUR TERRORISME ET/OU RADICALISÉS

Le Comité attire l'attention du SGRS sur son interprétation très restrictive de sa compétence dans le cadre du suivi des (anciens) détenus terro et/ou radicalisés. Le Comité recommande de maintenir et de renforcer davantage les contacts existants avec la VSSE au sein de la plateforme CT afin de s'assurer que le champ d'action du SGRS, avant tout théorique, ne laisse aucune brèche dans le suivi des (anciens) détenus terro et/ou radicalisés.

XI.1.7. ACCÈS DU SGRS AU LOGICIEL SIDIS SUITE DE LA DG EPI

Le Comité invite les ministres de la Défense et de la Justice à adopter un arrêté royal afin de rendre effectif l'accès du SGRS à SIDIS Suite. Le Comité recommande au SGRS d'ensuite prévoir des procédures internes quant à l'accès et aux modalités d'utilisation de ce logiciel.

---

[280] Voir COMITÉ PERMANENT R, *Rapport d'activités 2018,* p. 96 ('VI.2.4. L'information des bourgmestres et la transmission (d'extraits) des cartes d'information ou de listes à des instances tierces') et *Rapport d'activités 2019*, pp. 88-89 ('VI.2.2.6. La transmission des listes').

XI.1.8. SOUTENIR LA RECHERCHE SCIENTIFIQUE SUR LA RÉCIDIVE TERRORISTE

Les contours et facteurs de la récidive terroriste demeurent flous. Le Comité encourage le ministre de la Justice à soutenir les projets de recherche scientifique sur cette matière afin d'obtenir une meilleure image du phénomène de récidivisme chez les individus condamnés pour terrorisme. Partagés avec les services de renseignement, les résultats de ces recherches permettront d'adapter leur stratégie et leurs moyens aux besoins réels.

XI.1.9. DES DIRECTIVES POLITIQUES RELATIVES AUX ACTIVITÉS DE RENSEIGNEMENT À L'ÉTRANGER[281]

Le Comité souligne que tout déploiement de capacités de renseignement supplémentaires à l'étranger doit être mûrement réfléchi, compte tenu des nombreux risques liés à leur mise en œuvre. Ainsi, la collecte de renseignements à l'étranger comporte des risques pour les relations internationales de la Belgique. Il convient, dès lors, que les coûts-bénéfices d'une éventuelle opération de collecte à l'étranger fasse l'objet d'une évaluation et d'un arbitrage par le Gouvernement. Dans cette éventualité, les compétences de plusieurs Ministres étant concernées, le Comité permanent R recommande que le Conseil National de Sécurité se saisisse de la question et détermine la manière avec laquelle les activités de renseignements à l'étranger et leur impact sur les relations internationales doivent d'être coordonnées.

XI.1.10. ÉVITER LES DOUBLONS DANS LES ACTIVITÉS INTERNATIONALES

Le Comité recommande d'intégrer le développement de toute activité à l'étranger dans l'approche globale du SGRS dans la mesure du possible, et ce afin d'éviter les interférences et la duplication des activités.

XI.1.11. DES SYNERGIES ET COMPLÉMENTARITÉS DANS LE DÉPLOIEMENT D'UN RÉSEAU D'OFFICIERS DE LIAISON

Le Comité réaffirme qu'il considère que le déploiement d'officiers de liaison – tant au niveau opérationnel qu'au niveau diplomatique – constitue une valeur

[281] Les recommandations reprises aux points XI.2.9 à XI.2.11. sont issues de l'enquête sur les capacités de renseignement internationales pour la VSSE (Chapitre I.2.).

ajoutée évidente. Le développement d'un tel réseau mérite l'attention de la VSSE. Cependant, le déploiement d'officiers de liaison doit se faire dans un contexte de complémentarité et de synergies avec les partenaires nationaux, en l'occurrence le SGRS et la Police fédérale.[282]

XI.1.12. UNE TASKFORCE ET UN PLAN NATIONAL DE SÉCURITÉ DIGITALE[283]

Afin d'améliorer sa position d'information à l'égard des menaces digitales, et donc la prévention et la réaction face à ces menaces, le Comité permanent R invite le gouvernement à créer, dans les six mois, une Taskforce nationale intégrale et intégrée sur le modèle d'autres taskforces déjà créées pour des situations de crise. Il pourra s'agir d'un organe stratégique et politique spécifique qui élaborera des recommandations afin de prévenir et lutter efficacement contre les menaces digitales. Cette Taskforce sera également chargée d'établir un Plan National de Sécurité Digitale sur le modèle des autres plans nationaux développés en matière de sécurité.

XI.1.13. DES ANALYSES DE RISQUES RÉGULIÈRES QUANT À L'USAGE DE *REMOTE INFECTION TECHNOLOGIES*

Le Comité permanent R estime que les deux services de renseignement et de sécurité doivent être plus attentifs aux menaces que les nouvelles possibilités technologiques peuvent représenter en termes de captation de données et d'espionnage économique et politique, même si ces risques émanent de pays avec lesquels ils entretiennent des relations stratégiques. À cet égard, le Comité recommande que les deux services de renseignement procèdent régulièrement à des analyses de risques en portant une attention particulière aux risques liés à la présence de nombreuses institutions internationales sur le territoire belge.

---

[282] A cet égard, voir le protocole d'accord signé en septembre 2020 entre la Police fédérale et la VSSE qui règle les modalités de la coopération entre la Sûreté de l'Etat et les officiers de liaison de la police belge à l'étranger.

[283] Les recommandations reprises aux points XI.2.12 à XI.2.15. sont issues de l'enquête sur l'utilisation du logiciel Pegasus (Chapitre I.5.).

XI.1.14. LE DÉVELOPPEMENT D'OUTILS PROPRES ET COMMUNS À LA VSSE ET AU SGRS

En vue d'une plus grande coordination et de davantage d'efficacité, les deux services de renseignement et de sécurité belges devraient mutualiser leurs capacités techniques/technologiques telles que les *Remote Infection Technologies*. Le Comité permanent R invite les ministres de la Justice et de la Défense à investir dans le développement d'outils propres. Le Comité recommande qu'en cas de recours à des partenaires, un contrôle renforcé de légalité et de subsidiarité soit organisé.

XI.2. RECOMMANDATIONS RELATIVES À L'EFFICACITÉ DU CONTRÔLE

XI.2.1. LA CAPACITÉ DE CONTRÔLE DU COMITÉ PERMANENT R[284]

Le Comité permanent R recommande de voir ses capacités adaptées au renforcement en capacités humaines des services de renseignement afin de lui permettre de répondre à l'ensemble de ses missions légales, ce qui n'est plus le cas aujourd'hui.

[284] Voir notamment Chapitre 'I.5. Enquête de contrôle à la suite des révélations sur l'utilisation du logiciel Pegasus'.

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 2022 AU 31 DÉCEMBRE 2022)

Loi du 9 décembre 2021 portant assentiment à l'accord entre le Royaume de Belgique et le Royaume d'Espagne sur l'échange et la protection mutuelle des informations classifiées, fait à Bruxelles le 15 octobre 2015, *M.B.* 21 février 2022

Loi du 9 décembre 2021 portant assentiment à la convention multilatérale pour la mise en oeuvre des mesures relatives aux conventions fiscales pour prévenir l'érosion de la base d'imposition et le transfert de bénéfices et à la note explicative, faites à Paris le 24 novembre 2016, *M.B.* 4 mars 2022

Loi du 9 décembre 2021 portant assentiment à l'accord entre le Royaume de Belgique et la République de Finlande concernant la protection réciproque des informations classifiées, fait à Helsinki le 20 juillet 2016, *M.B.* 22 mars 2022

Loi du 26 mai 2016 portant assentiment à la Convention de coopération entre le gouvernement du Royaume de Belgique et le gouvernement du Royaume du Maroc en matière de lutte contre la criminalité organisée et le terrorisme, faite à Bruxelles le 18 février 2014, *M.B.* 20 mai 2022

Loi du 14 juillet 2022 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, *M.B.* 5 août 2022

Loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité, *M.B.* 5 août 2022

Loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, *M.B.* 8 août 2022

Loi du 20 juillet 2022 modifiant la loi du 23 mai 2017 de programmation militaire des investissements pour la période 2016-2030, *M.B.* 2 septembre 2022

Loi du 11 septembre 2022 visant à introduire des règles générales de déclassification des pièces classifiées (nouvel intitulé), *M.B.* 27 septembre 2022

Loi du 31 mai 2022 modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace, *M.B.* 19 octobre 2022

Loi du 13 octobre 2022 modifiant le Code belge de la Navigation concernant la sûreté maritime, *M.B.* 26 octobre 2022

Loi du 25 avril 2022 modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace en ce qui concerne l'obligation, pour le Service d'Enquêtes du Comité P, d'informer l'autorité disciplinaire compétente de l'existence d'une faute disciplinaire éventuelle lorsqu'il agit dans le cadre d'une enquête pénale, *M.B.* 28 novembre 2022

Loi du 8 décembre 2022 relatif aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée, *M.B.* 23 décembre 2022

Loi du 26 décembre 2022 contenant le budget général des dépenses pour l'année budgétaire 2023, *M.B.* 30 décembre 2022

A.R. du 14 mars 2022 relatif aux services postaux, *M.B.* 18 mars 2022

A.R. du 29 mars 2022 modifiant l'arrêté royal du 22 décembre 2020 portant création du Conseil national de sécurité, du Comité stratégique du Renseignement et de la Sécurité et du Comité de coordination du Renseignement et de la Sécurité, *M.B.* 7 avril 2022

A.R. du 29 mars 2022 modifiant l'arrêté royal du 13 décembre 2006 portant le statut des agents des services extérieurs de la Sûreté de l'État, *M.B.* 27 avril 2022

A.R. du 14 juin 2022 modifiant l'arrêté ministériel du 29 juillet 1987 portant création des comités de concertation de base pour le service public fédéral Justice et désignation de leurs présidents et abrogeant l'arrêté ministériel du 24 octobre 2014 portant composition du Comité de concertation de base du Moniteur belge, *M.B.* 25 juillet 2022

A.R. du 16 octobre 2022 portant exécution de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité, et modifiant l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, *M.B.* 24 octobre 2022

A.R. du 30 juillet 2022 relatif à l'octroi d'une allocation relative à la lutte contre le terrorisme et l'extrémisme destinée à la mise en oeuvre d'une politique locale de sécurité et de prévention pour l'année 2022, *M.B.* 24 octobre 2022

A.R. du 30 juillet 2022 relatif à l'octroi d'une allocation destinée à la mise en oeuvre d'une politique locale de sécurité et de prévention pour l'année 2022, *M.B.* 24 octobre 2022

A.R. du 2 octobre 2022 modifiant l'arrêté royal du 4 juillet 2014 fixant le statut de certains agents civils du département d'état-major renseignement et sécurité des forces armées, *M.B.* 29 novembre 2022

A.M. du 16 juin 2022 déterminant l'équipement réglementaire des agents de la Sûreté de l'État et fixant les dispositions particulières relatives à la détention, au port et à la garde de l'armement, *M.B.* 19 octobre 2022

Extrait de l'arrêt n° 158/2021 du 18 novembre 2021, n° du rôle : 6672, en cause : le recours en annulation de la loi du 1er septembre 2016 'portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité', introduit par P. Van Assche et autres, *M.B.* 17 février 2022

Sûreté de l'État - désignation temporaire par arrêté ministériel du 18 mai 2022 : madame Francisca BOSTYN, Conseillère générale au Service Public Fédéral Justice, nommée à titre définitif dans la classe A4, est désignée à titre temporaire pour exercer les fonctions d'administrateur général de la Sûreté de l'État, à partir du 2 mai 2022, *M.B.* 27 mai 2022

Rapport d'activités 2021 du Comité permanent de contrôle des services de renseignement et de sécurité, rapport, *M.B.* 30 juin 2022

Recrutement, par détachement, et constitution d'une réserve de recrutement de commissaires-auditeurs/trices francophones et néerlandophones (m/f/x), dotés de connaissances particulières en ICT/Data, pour le Service d'Enquêtes du Comité permanent R, *M.B.* 12 juillet 2022

Avis prescrit par l'article 3*quater* de l'arrêté du Régent du 23 août 1948 déterminant la procédure devant la section du contentieux administratif du Conseil d'État L'A.S.B.L.

Syndicat de la Police Belge 'Sypol.be' a sollicité l'annulation de l'arrêté royal du 29 mars 2022 modifiant l'arrêté royal du 13 décembre 2006 portant le statut des agents des services extérieurs de la Sûreté de l'Etat, *M.B.* 10 août 2022

Comité permanent de contrôle des services de renseignement et de sécurité - recrutement pour l'entrée en service immédiate et constitution d'une réserve de recrutement d'un(e) secrétaire francophone statutaire (m/f/x) (niv. B), *M.B.* 6 septembre 2022

Extrait de l'arrêt n° 33/2022 du 10 mars 2022, numéro du rôle : 7330. En cause : le recours en annulation partielle de la loi du 22 mai 2019 'modifiant diverses dispositions en ce qui concerne la gestion de l'information policière', introduit par l'ASBL 'Ligue des droits humains', *M.B.* 18 novembre 2022

Sélection comparatives, épreuves préalables des sélections comparatives et résultats des sélections comparatives de :

- Data officers (m/f/x) (niveau B) néerlandophones pour la Sûreté de l'État - numéro de sélection : ANG21452, *M.B.* 13 janvier 2022
- Data officers (m/f/x) (niveau B) francophones pour la Sûreté de l'État - numéro de sélection : AFG21328, *M.B.* 13 janvier 2022
- Surveillance officers (m/f/x) (niveau B) néerlandophones pour la Sûreté de l'État - numéro de sélection : ANG21457, *M.B.* 13 janvier 2022
- Technical officers (m/f/x) (niveau B) néerlandophones pour la Sûreté de l'État - numéro de sélection : ANG21458, *M.B.* 13 janvier 2022
- Surveillance officers (m/f/x) (niveau B) francophones pour la Sûreté de l'État - numéro de sélection : AFG21332, *M.B.* 13 janvier 2022
- Technical officers (m/f/x) (niveau B) francophones pour la Sûreté de l'État - numéro de sélection : AFG21333, *M.B.* 13 janvier 2022
- Analystes habilitations de sécurité (m/f/x) (niveau A1) néerlandophones pour le Ministère de la Défense - numéro de sélection : ANG22016, *M.B.* 18 janvier 2022
- Experts ICT pour le Laboratoire de Cyberdéfense (m/f/x) (niveau B), francophones, pour le Ministère de la Défense - numéro de sélection : AFG22133, *M.B.* 2 mai 2022
- Résultat de la sélection comparative de Surveillance officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'Etat - numéro de sélection : AFG21332, *M.B.* 15 juin 2022
- Résultat de la sélection comparative de Technical Officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'Etat - numéro de sélection : AFG21333, *M.B.* 15 juin 2022
- Résultat de la sélection comparative de Data Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'Etat - numéro de sélection : ANG21452, *M.B.* 15 juin 2022
- Support Officers (m/f/x) (niveau C), francophones, pour la Sûreté de l'Etat - numéro de sélection : AFG22248, *M.B.* 29 août 2022
- Masters (m/f/x) (niveau A1), francophones, pour la Sûreté de l'Etat - numéro de sélection : AFG22249, *M.B.* 29 août 2022
- Support Officers (m/f/x) (niveau C), néerlandophones, pour le la Sûreté de l'État - numéro de sélection : ANG22350, *M.B.* 29 août 2022
- Masters (m/f/x) (niveau A1), néerlandophones, pour le la Sûreté de l'Etat - numéro de sélection : ANG22351, *M.B.* 29 août 2022
- Bacheliers (m/f/x) (niveau B) néerlandophones pour le la Sûreté de l'État - numéro de sélection : ANG22386, *M.B.* 19 septembre 2022
- Bacheliers (m/f/x) (niveau B) francophones pour la Sûreté de l'État - numéro de sélection : AFG22268, *M.B.* 19 septembre 2022

- Psychologues (m/f/x) (niveau A1), francophones, pour la Sûreté de l'État - numéro de sélection : AFG22337, *M.B.* 28 octobre 2022
- Résultat de la sélection comparative de Masters (m/f/x) (niveau A1) francophones pour la Sûreté de l'Etat - numéro de sélection : AFG22249, *M.B.* 9 novembre 2022
- Résultat de la sélection comparative de Masters (m/f/x) (niveau A1) néerlandophones pour la Sûreté de l'Etat - numéro de sélection : ANG22351, *M.B.* 9 novembre 2022, *M.B.* 9 novembre 2022
- Résultat de la sélection comparative de Bacheliers (m/f/x) (niveau B) francophones pour la Sûreté de l'Etat - numéro de sélection : AFG22268, *M.B.* 16 novembre 2022
- Résultat de la sélection comparative de Bacheliers (m/f/x) (niveau B) néerlandophones pour la Sûreté de l'Etat - numéro de sélection : ANG22386, *M.B.* 16 novembre 2022

ANNEXE B
APERÇU DES PRINCIPALES PROPOSITIONS DE LOIS, DES PROJETS DE LOIS, DES RÉSOLUTIONS, MOTIONS D'ORDRE 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 2022 AU 31 DÉCEMBRE 2022)

Sénat

Demande d'établissement d'un rapport d'information relatif à la lutte contre les ingérences de puissances étrangères visant à saper les fondements de l'état de droit démocratique, Doc. parl., Sénat, 2021-2022, n° 7-344/1 et *Ann. parl.*, Sénat, 2021-2022, 29 avril 2022, n° 7-28, p. 15

Proposition de résolution relative à une obligation de déclaration pour les universités et les entreprises qui collaborent avec des régimes autoritaires dans des secteurs critiques, Doc. parl., Sénat, 2021-2022, n° 7-373/1

Chambre des représentants

Proposition de loi visant à fixer des règles générales de déclassification pour les pièces classifiées, Doc. parl., Chambre, 2021-2022, n° 55-0732/3

Comité permanent de contrôle des services de renseignements et de sécurité - nomination du second suppléant du membre néerlandophone - candidatures introduites, *C.R.I.*, Chambre, 2021-2022, 13 janvier 2022, PLEN 157, p. 86

Proposition de loi modifiant la loi du 29 juillet 1934 interdisant les milices privées en vue d'interdire les groupements non démocratiques, proposition de loi incriminant l'appartenance ou la collaboration avec un groupement qui prône la discrimination ou la ségrégation, proposition de loi modifiant la loi du 29 juillet 1934 interdisant les milices privées, afin que les interdictions prévues par cette loi soient élargies pour viser les associations incitant à la haine, à la discrimination ou à la violence, et permettant leur dissolution par le pouvoir exécutif, Doc. parl., Chambre, 2021-2022, n° 55-0943/3

Proposition de loi modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace en ce qui concerne l'obligation, pour le Service d'Enquêtes du Comité P, d'informer l'autorité disciplinaire compétente de l'existence d'une faute disciplinaire éventuelle

lorsqu'il agit dans le cadre d'une enquête judiciaire, Doc. parl., Chambre, 2021-2022, n° 55-1985/5

Projet de loi introduisant des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G, Doc. parl., Chambre, 2021-2022, n° 55-2317/8

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, 2021-2022, n° 55-2443/1

Projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace, Doc. parl., Chambre, 2021-2022, n° 55-2495/1 à 55-2495/10

Projet de loi portant assentiment à l'accord entre le gouvernement du Royaume de Belgique et le gouvernement de la République italienne concernant l'échange et la protection mutuelle des informations classifiées, fait à Rome le 31 janvier 2017, Doc. parl., Chambre, 2021-2022, n° 55-2555/1

Proposition de loi modifiant le Code pénal en ce qui concerne la mise à disposition du tribunal de l'application des peines, Doc. parl., Chambre, 2021-2022, n° 55-2571/1

Projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, Doc. parl., Chambre, 2021-2022, nos 55-2572/1 à 55-2572/7 et discussion générale (*C.R.I.*, Chambre, 2021-2022, 7 juillet 2022, PLEN 192, p. 44)

Proposition de résolution visant à renforcer la lutte contre les groupements extrémistes, Doc. parl., Chambre, 2021-2022, n° 55-2585/1

Nomination du greffier du Comité permanent de contrôle des services de renseignements et de sécurité, Doc. parl., Chambre, 2021-2022, n° 55-2597/1 et résultat du scrutin (*C.R.I.*, Chambre, 2021-2022, 29 mars 2022, PLEN 171, p. 75)

Comité permanent de contrôle des services de renseignements et de sécurité - nomination du second suppléant du membre néerlandophone (*C.R.I.*, Chambre, 2021-2022, 29 mars 2022, PLEN 171, p. 67)

Proposition de loi modifiant diverses lois en ce qui concerne la délimitation de l'infraction d'incitation à la haine, Doc. parl., Chambre, 2021-2022, n° 55K2606/1

Proposition de résolution visant à porter le budget de la Défense belge à 2 % du produit intérieur brut d'ici 2030, Doc. parl., Chambre, 2021-2022, n° 55K2619/1

Proposition de loi modifiant la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques en ce qui concerne l'utilisation obligatoire de réseaux unidirectionnels, Doc. parl., Chambre, 2021-2022, n° 55K2635/1

Comité permanent de contrôle des services de renseignements et de sécurité - titre honorifique (*C.R.I.*, Chambre, 2021-2022, 19 mai 2022, PLEN 181, p. 58)

Projet de loi relatif à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité, Doc. parl., Chambre, 2021-2022, nos 55K2693/1 à 55K2693/3 et 55K2693/5 et (*C.R.I.*, Chambre, 2021-2022, 14 juillet 2022, PLEN 195, p. 23)

Projet de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, Doc. parl., Chambre, 2021-2022, nos 55K2706/1 à 55K2706/6 et discussion générale (*C.R.I.*, Chambre, 2021-2022, 7 juillet 2022, PLEN 192, p. 53)

Projet de loi modifiant le Code belge de la Navigation concernant la sûreté maritime, Doc. parl., Chambre, 2021-2022, n° 55K2734/1

Projet de loi modifiant la loi du 23 mai 2017 de programmation militaire des investissements pour la période 2016-2030, Doc. parl., Chambre, 2021-2022, nos 2737/1, 2737/3 et 2737/4, discussion générale (*C.R.I.*, Chambre, 2021-2022, 13 juillet 2022, PLEN 194, p. 22) et amendement réservé au projet de loi (*C.R.I.*, Chambre, 2021-2022, 14 juli 2022, PLEN 195, p. 68)

Proposition de loi visant à fixer des règles générales de déclassification pour les pièces classifiées, Doc. parl., Chambre, 2021-22 nos 55K2739/001 à 55K2739/006, discussion générale (*C.R.I.*, Chambre, 2021-2022, 19 juillet 2022, PLEN 196, p. 22), amendements et articles réservés (*C.R.I.*, Chambre, 2021-2022, 20 juillet 2022, PLEN 201, p. 51) et ensemble de la proposition de loi (*C.R.I.*, Chambre, 2021-2022, 20 juillet 2022, PLEN 201, p. 52)

Rapport d'activités 2021du Comité permanent de contrôle des services de renseignement et de sécurité - rapport, Doc. parl., Chambre, 2021-2022, no 55K2745/1

Proposition de résolution visant à promouvoir une politique de cybersécurité plus performante pour soutenir nos entreprises et nos organisations dans la lutte contre la cybercriminalité, Doc. parl., Chambre, 2021-2022, no 55K2771/1

Projet de loi portant assentiment aux actes internationaux suivants: 1) la convention entre le Royaume de Belgique et la République d'Inde sur l'entraide judiciaire en matière pénale, faite à Bruxelles le 16 septembre 2021, et 2) le traité entre le Royaume de Belgique et les Émirats arabes unis sur l'entraide judiciaire en matière pénale, fait à Abu Dhabi le 9 décembre 2021, et 3) le traité entre le Royaume de Belgique et les Émirats arabes unis sur l'extradition, fait à Abu Dhabi le 9 décembre 2021, et 4) le traité entre le Royaume de Belgique et la République islamique d'Iran sur le transfèrement de personnes condamnées, fait à Bruxelles le 11 mars 2022, et 5) le protocole du 22 novembre 2017 portant amendement du Protocole additionnel à la Convention sur le transfèrement des personnes condamnées, signé le 7 avril 2022 à Strasbourg (2784/1-4) - discussion générale (*C.R.I.*, Chambre, 2021-2022, 19 juillet 2022, PLEN 197, p. 1) et (*C.R.I.*, Chambre, 2021-2022, 20 juillet 2022, PLEN 201, p. 48)

Projet de loi modifiant la loi du 3 décembre 2017 portant création de l'Autorité de protection des données, Doc. parl., Chambre, 2021-2022, no 55K2793/1

Projet de loi portant assentiment à l'accord entre le Royaume de Belgique et le Royaume des Pays-Bas concernant l'échange et la protection mutuelle des informations classifiées, fait à Bruxelles le 5 novembre 2019, Doc. parl., Chambre, 2021-2022, no 55K2796/1

Projet de loi portant assentiment à l'accord entre le gouvernement du Royaume de Belgique et le gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord concernant la protection des informations classifiées, fait à Bruxelles le 1er décembre 2020, Doc. parl., Chambre, 2021-22, no 55K2797/1

Proposition de loi modifiant, en vue d'interdire le financement étranger de partis politiques, la loi du 4 juillet 1989 relative à la limitation et au contrôle des dépenses électorales engagées pour l'élection de la Chambre des représentants, ainsi qu'au financement et à la comptabilité ouverte des partis politiques, Doc. parl., Chambre, 2021-22, no 55K2905/1

Projet de loi relatif aux canaux de signalement et à la protection des auteurs de signalement d'atteintes à l'intégrité dans les organismes du secteur public fédéral et au sein de la police intégrée, Doc. parl., Chambre, 2021-2022, no 55K2952/1

Proposition de loi modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace, afin de charger le Comité P d'effectuer chaque année un contrôle par échantillonnage du traitement des plaintes et dénonciations, Doc. parl., Chambre, 2021-2022, no 55K2963/1

Proposition de loi modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace, afin d'élargir l'obligation de signaler les crimes et délits commis par un collègue aux cas de décès, de blessures graves et d'incidents de tir, Parl. St. Kamer 2021-22, no 55K2964/1

Proposition de résolution relative à la lutte efficace et effective contre l'influence étrangère et la mise à mal de notre démocratie, Doc. parl., Chambre, 2021-2022, no 55K3045/1

Cour des comptes, Cour constitutionnelle, Conseil supérieur de la Justice, Comité Permanent de contrôle des services de police, Comité Permanent de contrôle des

services de renseignement et de sécurité, Médiateurs fédéraux, Autorité de protection des données, Commissions de nomination pour le notariat, Commission BIM, Organe de contrôle de l'information policière, Commission fédérale de déontologie, Conseil central de surveillance pénitentiaire, Institut fédéral des droits humains - travaux des groupes de travail dans le cadre du projet de synergie - comptes de l'année budgétaire 2021 - ajustements budgétaires de l'année budgétaire 2022 - propositions budgétaires pour l'année budgétaire 2023, Doc. parl., Chambre, 2021-2022, nos 55K3050/1 à 55K3050/3 et (*C.R.I.*, Chambre, 2022-2023, 22 décembre 2022, PLEN 226, p. 44)

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 2022 AU 31 DÉCEMBRE 2022)

Sénat

Question écrite de R. Daems au ministre de la Justice sur les 'services de sécurité - méthodes spécifiques - méthodes exceptionnelles - interception de données transitant par câble - captures de données à des moments précis - écoute de données - collecte - autorisation - vie privée - statistiques et tendances' (Sénat, 2021-2022, 30 mars 2022, Q. nº 7-1542)

Question écrite de R. Daems à la ministre de la Défense sur les 'services de sécurité - méthodes spécifiques - méthodes exceptionnelles - interception de données transitant par câble - captures de données à des moments précis - écoute de données - collecte - autorisation - vie privée - statistiques et tendances' (Sénat, 2021-2022, 30 mars 2022, Q. nº 7-1543)

Question écrite de R. Daems à la ministre de l'Intérieur sur les 'services de sécurité - méthodes spécifiques - méthodes exceptionnelles - interception de données transitant par câble - captures de données à des moments précis - écoute de données - collecte - autorisation - vie privée - statistiques et tendances' (Sénat, 2021-2022, 30 mars 2022, Q. nº 7-1544)

Question écrite d'E. Ampe à la ministre de la Justice sur 'guerre en Ukraine - antivirus 'Kaspersky' - risques potentiels pour la sécurité - acteurs étrangers - piratage - approche au sein des services publics et des services de sécurité - mesures' (Sénat, 2021-2022, 5 avril 2022, Q. nº 7-1570)

Question écrite d'E. Ampe à la ministre de la Défense sur 'guerre en Ukraine - antivirus 'Kaspersky' - risques potentiels pour la sécurité - acteurs étrangers - piratage - approche au sein des services publics et des services de sécurité - mesures' (Sénat, 2021-2022, 5 avril 2022, Q. no 7-1571)

Question écrite d'E. Ampe à la ministre de l'Intérieur sur 'guerre en Ukraine - antivirus 'Kaspersky' - risques potentiels pour la sécurité - acteurs étrangers - piratage - approche au sein des services publics et des services de sécurité - mesures' (Sénat, 2021-2022, 5 avril 2022, Q. no 7-1572)

Question écrite de S. Coenegrachts à la ministre de la Justice sur 'guerre en Ukraine - églises orthodoxes russes - menaces - chiffres et tendances - Sûreté de l'État - mesures' (Sénat, 2021-2022, 5 avril 2022, Q. nº 7-1581)

Question écrite de S. Coenegrachts à la ministre de l'Intérieur sur 'Citrix - grave vulnérabilité - risques en matière de sécurité - piratage - serveurs et ordinateurs - entreprises - services publics et de sécurité - protection - directives - mesures' (Sénat, 2021-2022, 5 avril 2022, Q. nº 7-1582)

Question écrite de R. Daems à la ministre de la Défense sur 'guerre en Ukraine - églises orthodoxes russes - menaces - chiffres et tendances - Sûreté de l'État - mesures' (Sénat, 2021-2022, 5 mai 2022, Q. nº 7-1600)

Question écrite de L. Gahouchi au ministre de la Justice sur 'Institut national des droits humains - approche interfédérale - accord de coopération - état d'avancement - bureau de l'agent du gouvernement auprès de la Cour européenne des droits de l'homme - coordination - cadre du personnel - statut A - demande d'accréditation' (Sénat, 2021-2022, 11 mai 2022, Q. nº 7-1617)

Question écrite d'E. Ampe à la ministre de l'Intérieur sur les 'caméras - Chine - espionnage - acteurs étrangers - vie privée - chiffres et tendances' (Sénat, 2021-2022, 2 juin 2022, Q. nº 7-1646)

Question écrite d'E. Ampe au ministre de la Justice sur les 'cyberattaques - acteurs étatiques - vie privée - cybersécurité - chiffres et tendances' (Sénat, 2021-2022, 2 juin 2022, Q. nº 7-1651)

Question écrite d'E. Ampe au secrétaire d'État à la Digitalisation sur les 'cyberattaques - acteurs étatiques - vie privée - cybersécurité - chiffres et tendances' (Sénat, 2021-2022, 2 juin 2022, Q. nº 7-1653)

Question écrite de T. Ongena à la ministre de la Défense sur 'Défense - applications de messagerie instantanée - utilisation - risques pour la sécurité - piratage - acteurs étatiques - chiffres et tendances - interdiction éventuelle - autres mesures' (Sénat, 2021-2022, 2 juin 2022, Q. nº 7-1668)

Chambre des représentants

Questions jointes de Ph. Pivin et G. Dallemagne au ministre de la Justice sur 'l'ordonnance du tribunal de l'entreprise concernant l'Exécutif des Musulmans de Belgique' (*C.R.I.*, Chambre, 2021-2022, 12 janvier 2022, COM 652, p. 58, Q. nºs 23785C et 23837C)

Question de M. Freilich à la ministre de l'Intérieur sur 'l'approche du Dark web' (*Q.R.*, Chambre, 2021-2022, 13 janvier 2022, nº 74, p. 316, Q. nº 961)

Question d'O. Depoortere à la ministre de l'Intérieur sur le 'Comité permanent de contrôle des services de police - rapport annuel 2020' (*Q.R.*, Chambre, 2021-2022, 13 janvier 2022, nº 74, p. 330, Q. nº 966)

Question de Th. Francken au secrétaire d'État à l'Asile et la Migration sur 'les contrôles de sécurité dans le cadre de l'opération en Afghanistan' (*Q.R.*, Chambre, 2021-2022, 13 janvier 2022, nº 74, p. 406, Q. nº 437)

Question de S. Loones au ministre de la Justice sur 'les attentats de 2017 en Espagne' (*C.R.I.*, Chambre, 2021-2022, 19 janvier 2022, COM 663, p. 41, Q. nº 23908C)

Question d'Y. Ingels au ministre de la Justice sur les 'Belgian secure communications' (*Q.R.*, Chambre, 2021-2022, 24 janvier 2022, nº 75, p. 241, Q. nº 897)

Questions jointes de P. Prévot et M. Freilich au secrétaire d'État à la Digitalisation sur 'les risques du Log4Shell' (*C.R.I.*, Chambre, 2021-2022, 25 janvier 2022, COM 666, p. 23, Q. nºs 23387C et 24275C)

Questions jointes de G. Defossé, A. Ponthier, Ch. Lacroix, A. Flahaut et P. Buysrogge à la ministre de la Défense sur 'la cyberattaque contre le site de la Défense' (*C.R.I.*, Chambre, 2021-2022, 26 janvier 2022, COM 671, p. 20, Q. nºs 23607C, 23612C, 23634C, 24318C et 24502C)

Débat d'actualité et questions jointes de F. Demon, V. Matz, T. Vandenput, B. Moyaers, H. Rigot et S. Goethals à la ministre de l'Intérieur sur 'la manifestation du 23 janvier' (*C.R.I.*, Chambre, 2021-2022, 26 janvier 2022, COM 676, p. 19, Q. nos 24423C, 24450C, 24457C, 24490C, 24495C, et 24514C)

Questions jointes de K. Metsu, E. Gilissen, M. Freilich et S. Cogolati au ministre de la Justice sur 'les risques de cybersurveillance liés aux équipements Dahua et Hikvision' (*C.R.I.*, Chambre, 2021-2022, 26 janvier 2022, COM 677, p. 1, Q. nos 23995C, 24232C, 24363C et 24454C)

Question de P. Buysrogge au ministre de la Justice sur 'l'extrémisme de gauche en Belgique et à Bruxelles' (*C.R.I.*, Chambre, 2021-2022, 26 janvier 2022, COM 677, p. 24, Q. no 24477C)

Question de J. Pillen au ministre des Affaires étrangères sur 'l'accord de sécurité global entre la Belgique et la Bulgarie ainsi que d'autre pays' (*Q.R.*, Chambre, 2021-2022, 31 janvier 2022, no 76, p. 110, Q. no 575)

Question de S. Cogolati au ministre de la Justice sur les 'risques de censure et cybersurveillance sur les smartphones Huawei, Xiaomi et OnePlus' (*Q.R.*, Chambre, 2021-2022, 31 janvier 2022, no 76, p. 251, Q. no 909)

Question de G. Dallemagne au ministre de la Justice sur 'le rapport de la Sûreté de l'État sur les Frères musulmans' (*Q.R.*, Chambre, 2021-2022, 31 janvier 2022, no 76, p. 268, Q. no 951)

Question de G. Dallemagne au ministre de la Justice sur 'le rapport de la Sûreté de l'État concernant les réfugiés' (*Q.R.*, Chambre, 2021-2022, 31 janvier 2022, no 76, p. 271, Q. no 953)

Question de S. Cogolati au ministre de la Justice sur 'les systèmes de vidéosurveillance de nos bases militaires en Belgique et à l'étranger' (*Q.R.*, Chambre, 2021-2022, 31 janvier 2022, no 76, p. 282, Q. no 382)

Question de M. Freilich au ministre de la Justice sur la 'Défense - cyberattaque' (*Q.R.*, Chambre, 2021-2022, 31 janvier 2022, no 76, p. 285, Q. no 388)

Questions jointes de N. Boukili et F. De Smet au secrétaire d'État à l'Asile et la Migration sur 'le retrait du permis de séjour de M. Toujgani' (*C.R.I.*, Chambre, 2021-2022, 1er février 2022, COM 681, p. 1, Q. nos 24124C et 24129C)

Questions jointes de D. Safai et D. Van Langenhove au secrétaire d'État à l'Asile et la Migration sur 'la bataille procédurale d'Abdallah Ouahbour' (*C.R.I.*, Chambre, 2021-2022, 1er février 2022, COM 681, p. 30, Q. nos 24601C, 24691C et 24649C)

Questions jointes de F. Demon et M.-Ch. Marghem au ministre de la Justice sur 'les poursuites contre les émeutiers après les manifestations contre les mesures sanitaires' (*C.R.I.*, Chambre, 2021-2022, 2 février 2022, COM 683, p. 48, Q. nos 24641C en 24774C)

Echange de vues et questions jointes de Th. Francken, P. Buysrogge, A. Ponthier, M. Vindevoghel, R. Hedebouw et N. Boukili à la ministre de la Défense sur 'la vision stratégique' (*C.R.I.*, Chambre, 2021-2022, 9 février 2022, COM 688, p. 1, Q. nos 24329C, 24330C, 24376C, 24506C, 24680C et 24681C)

Questions jointes de S. Cogolati, K. Metsu et J. Pillen à la ministre de la Défense sur 'les systèmes de vidéosurveillance de nos bases militaires en Belgique et à l'étranger' (*C.R.I.*, Chambre, 2021-2022, 9 février 2022, COM 688, p. 46, Q. nos 24270C, 24589C, 24755C et 25092C)

Question de S. Matheï à la ministre de la Défense sur 'le transport militaire à caractère humanitaire' (*Q.R.*, Chambre, 2021-2022, 11 février 2022, no 77, p. 305, Q. no 399)

Questions jointes de T. Vandenput et K. Metsu à la ministre de l'Intérieur sur 'Hikvision' (*C.R.I.*, Chambre, 2021-2022, 15 février 2022, COM 698, p. 19, Q. nos 24602C et 24642C)

Question et interpellation jointe de K. Metsu à la ministre de l'Intérieur sur 'la note de politique générale 2022 et les recommandations de la CEP Terrorisme' (*C.R.I.*, Chambre, 2021-2022, 15 février 2022, COM 698, p. 23, Q. nos 24562C et 246I)

Question de D. Van Langenhove au secrétaire d'État à l'Asile et la Migration sur 'la présence en Belgique de terroristes du Groupe Islamique Combattant Marocain' (*C.R.I.*, Chambre, 2021-2022, 16 février 2022, COM 702, p. 17, Q. nº 25060C)

Question de M. Dillen au ministre de la Justice sur 'le plan de transformation numérique' (*C.R.I.*, Chambre, 2021-2022, 16 février 2022, COM 703, p. 25, Q. nº 261I)

Question de P. Buysrogge à la ministre de l'Intérieur sur 'la présence d'extrémistes lors de manifestations' (*C.R.I.*, Chambre, 2021-2022, 23 février 2022, COM 709, p. 1, Q. nº 25043C)

Question de S. De Wit au ministre de la Justice sur 'l'annulation de la loi sur la conservation des données' (*C.R.I.*, Chambre, 2021-2022, 23 février 2022, COM 710, p. 20, Q. nº 25422C)

Questions jointes de Ph. Pivin, G. Dallemagne et S. Rohonyi au ministre de la Justice sur 'l'Exécutif des Musulmans de Belgique' (*C.R.I.*, Chambre, 2021-2022, 23 février 2022, COM 710, p. 22, Q. nºs 25441C, 25583C et 25585C)

Question de M. Freilich à la ministre des Affaires étrangères sur 'l'avis du COIB relatif à la cybersécurité lors des Jeux olympiques d'hiver' (*Q.R.*, Chambre, 2021-2022, 25 février 2022, nº 78, p. 119, Q. nº 602)

Question de N. Boukili au ministre de la Justice sur la 'rémunération des membres du Comité R' (*Q.R.*, Chambre, 2021-2022, 25 février 2022, nº 78, p. 243, Q. nº 1004)

Question d'O. Depoortere au ministre de la Justice sur 'l'utilisation du logiciel Pegasus' (*Q.R.*, Chambre, 2021-2022, 25 février 2022, nº 78, p. 251, Q. nº 1013)

Question de M. Freilich au ministre de la Justice sur 'l'espionnage économique chinois' (*Q.R.*, Chambre, 2021-2022, 25 février 2022, nº 78, p. 255, Q. nº 1022)

Question d'A. Ponthier à la ministre de la Défense sur les 'marchés publics approuvés pour la Défense - ACOS IS' (*Q.R.*, Chambre, 2021-2022, 25 février 2022, nº 78, p. 262, Q. nº 408)

Question d'A. Ponthier à la ministre de la Défense sur 'l'engagement belge prévu dans le cadre de la lutte contre l'EI' (*Q.R.*, Chambre, 2021-2022, 25 février 2022, nº 78, p. 264, Q. nº 410)

Échanges de vues et questions jointes de S. Cogolati, S. De Vuyst, E. Gilissen, N. Boukili, F. De Smet, A. Van Bossuyt, G. Dallemagne, A. Ponthier, W. De Vriendt, J. Pillen, E. Van Hoof, Th. Francken, K. Verduyckt, G. Defossé, S, Creyelman, T. Roggeman, S. Moutquin, E. Platteau, H. Rigot et G. Daems au premier ministre, à la ministre des Affaires étrangères, à la ministre de l'Intérieur, à la ministre de la Défense et au secrétaire d'État à l'Asile et la Migration sur 'la crise ukrainienne, le soutien du gouvernement belge et l'accueil des réfugiés ukrainiens' (*C.R.I.*, Chambre, 2021-2022, 2 mars 2022, COM 712, p. 1, Q. nºs 24261C, 24323C, 25171C, 25262C, 25726C, 24664C, 24721C, 24916C, 25259C, 25263C, 25490C, 25596C, 25696C, 25704C, 25706C, 25707C, 25709C, 25694C, 24663C, 25109C, 25598C, 25693C, 25700C, 25703C, 25705C, 25708C, 25722C, 25725C, 25648C, 25651C, 25690C, 25691C, 25692C, 25699C, 25701C, 25702C, 25711C, 25719C, 25721C, 25723C, 25727C et 25724C)

Question de R. D'Amico au ministre de la Fonction publique sur 'Ericsson et les révélations du Consortium international des journalistes d'investigation' (*C.R.I.*, Chambre, 2021-2022, 9 mars 2022, COM 716, p. 22, Q. nº 25843C)

Question d'O. Depoortere à la ministre de l'Intérieur sur 'le niveau de sécurité, l'analyse du risque et la surveillance accrue des cibles belges potentielles' (*C.R.I.*, Chambre, 2021-2022, 9 mars 2022, COM 716, p. 35, Q. nº 25747C)

Question de M.-Ch. Marghem au ministre de la Justice sur 'le départ de volontaires pour l'Ukraine' (*C.R.I.*, Chambre, 2021-2022, 9 mars 2022, COM 717, p. 32, Q. nº 25865C)

Question de W. De Vriendt à la ministre des Affaires étrangères sur les 'attaques de Daech dans le nord-est de la Syrie' (*Q.R.*, Chambre, 2021-2022, 10 mars 2022, nº 79, p. 155, Q. nº 606)

Question de K. Metsu à la ministre de l'Intérieur sur 'le suivi des nouvelles technologies' (*Q.R.*, Chambre, 2021-2022, 10 mars 2022, nº 79, p. 378, Q. nº 1078)

Question de K. Metsu à la ministre de l'Intérieur sur le 'budget 2022 - lutte contre l'extrémisme violent' (*Q.R.*, Chambre, 2021-2022, 10 mars 2022, nº 79, p. 386, Q. nº 1081)

Échange de vues et questions jointes de K. Metsu, R. Van Lommel, M. Freilich, A. Van Bossuyt, D.Van Langenhove, S. Cogolati, W. De Vriendt, B. Segers, F. De Smet, D. Safai et Th. Francken au premier ministre sur 'la stratégie de sécurité nationale' (*C.R.I.*, Chambre, 2021-2022, 16 mars 2022, COM 721, 1, Vr. nrs. 25758C, 25765C, 25786C, 25811C, 25799C, 25991C, 26001C, 26015C, 26026C, 26067C, 26117C, 26134C et 26151C)

Question d'A. Flahaut au premier ministre sur 'la participation armée de citoyens belges sur le sol ukrainien suite à l'agression russe' (*C.R.I.*, Chambre, 2021-2022, 16 mars 2022, COM 729, p. 14, Q. nº 25981C)

Question d'O. Depoortere au ministre de la Justice sur les 'rémunérations à la VSSE' (*Q.R.*, Chambre, 2021-2022, 18 mars2022, nº 80, p. 235, Q. nº 1005)

Question d'E. Burton au ministre de la Justice sur 'l'OCAM - évasion de terroristes belges en Syrie' (*Q.R.*, Chambre, 2021-2022, 18 mars2022, nº 80, p. 250, Q. nº 1049)

Question d'E. Burton au ministre de la Défense sur 'l'Afghanistan - mission secrète d'évacuation de civils' (*Q.R.*, Chambre, 2021-2022, 18 mars2022, nº 80, p. 278, Q. nº 421)

Question d'A. Laaouej à la ministre de l'Intérieur sur 'les menaces proférées contre les mosquées à la veille du ramadan' (*C.R.I.*, Chambre, 2021-2022, 24 mars 2022, PLEN 171, p. 25, Q. nº 2421P)

Question de T. Vandenput à la ministre de l'Intérieur sur 'la mise à jour de la base de données de l'OCAM' (*Q.R.*, Chambre, 2021-2022, 28 mars 2022, nº 81, p. 269, Q. nº 1110)

Question de K. Jadin à la ministre de l'Intérieur sur 'le décès du dirigeant de l'EI' (*Q.R.*, Chambre, 2021-2022, 28 mars 2022, nº 81, p. 276, Q. nº 1115)

Débat d'actualité sur l' Ukraine et questions jointes d'A Van Bossuyt, A. Ponthier, M. De Maegd, W. De Vriendt, S. Cogolati, S. De Vuyst, N. Boukili, F. De Smet, S. Rohonyi et S. Moutquin à la ministre des Affaires étrangères sur 'la démission de Jens Stoltenberg' (*C.R.I.*, Chambre, 2021-2022, 29 mars 2022, COM 743, p. 1, Q. nºs 24926C, 25027C, 25742C, 25751C, 25769C, 25770C, 25806C, 25847C, 25861C, 26006C, 26016C, 26194C, 26196C, 26602C, 26604C, 26610C, 26615C, 26598C, 26613C et 26626C)

Questions jointes de G. Defossé et E. Van Hoof à la ministre de la Défense sur 'le financement des troupes rwandaises au Mozambique' (*C.R.I.*, Chambre, 2021-2022, 29 mars 2022, COM 743, 60, Q. nºs 25039C, 25184C, 25688C et 25899C)

Débat d'actualité et questions jointes de B. Segers, D. Safai, M.-Ch. Marghem, J. Chanson, K. Aouasti, V. Van Peel, Fr. De Smet et G. Daems à la ministre de l'Intérieur sur 'l'Ukraine' (*C.R.I.*, Chambre, 2021-2022, 30 mars 2022, COM 746, p. 1, Q. nºs 26027C, 26133C, 26141C, 26283C, 26622C, 26624C, 26636C, 26667C en 55026712C)

Question d'A. Ponthier à la ministre de la Défense sur 'les projets pour la composante cyber et le recrutement de personnel' (*C.R.I.*, Chambre, 2021-2022, 30 mars 2022, COM 748, p. 21, Q. nº 24791C)

Question d'A. Ponthier au ministre de la Justice sur 'les archives de la sûreté coloniale' (*C.R.I.*, Chambre, 2021-2022, 30 mars 2022, COM 751, p. 7, Q. nº 26463C)

Questions jointes de D. Ducarme et S. Rohonyi au ministre de la Justice sur 'les Frères musulmans et la menace éventuelle que ceux-ci constituent en Belgique' (*C.R.I.*, Chambre, 2021-2022, 30 mars 2022, COM 751, p. 14, Q. nºs 26463C, 26663C et 26668C)

Question de S. Loones au ministre de la Justice sur le 'filtrage des investissements, acquisitions et participations étrangers' (*Q.R.*, Chambre, 2021-2022, 5 avril 2022, nº 82, p. 159, Q. nº 1054)

Question de S. Matheï à la ministre de la Défense sur la 'composante de cyberdéfense' (*Q.R.*, Chambre, 2021-2022, 5 avril 2022, nº 82, p. 227, Q. nº 406)

Question de S. Matheï à la ministre de l'Intérieur sur les 'campagnes de désinformation - service de sécurité' (*Q.R.*, Chambre, 2021-2022, 5 avril 2022, nº 82, p. 292, Q. nº 1152)

Question d'O. Depoortere à la ministre de l'Intérieur sur les 'cibles potentielles en Belgique - niveau de sécurité, analyse des risques et surveillance accrue' (*Q.R.*, Chambre, 2021-2022, 21 avril 2022, nº 83, p. 378, Q. nº 1162)

Questions jointes d'O. Depoortere et N. Boukili à la ministre de l'Intérieur sur 'l'utilisation du logiciel Pegasus' (*C.R.I.*, Chambre, 2021-2022, 27 avril 2022, COM 767, p. 28, Q. nos 27060C et 27170C)

Questions jointes de M. De Maegd et G. Dallemagne au ministre de la Justice sur 'la profanation du monument commémoratif du génocide arménien et la lutte contre le radicalisme' (*C.R.I.*, Chambre, 2021-2022, 28 avril 2022, PLEN 176, p. 10, Q. nos 2485P et 2488P)

Question de G. Defossé la ministre de la Défense sur 'l'ingérence étrangère dans l'islam belge' (Q.R., Chambre, 2021-2022, 2 mai 2022, nº 84, p. 295, Q. nº 446)

Question de G. Defossé la ministre de la Défense sur les 'cibles potentielles en Belgique - niveau de sécurité, analyse des risques et surveillance accrue' (Q.R., Chambre, 2021-2022, 11 mai 2022, nº 85, p. 225, Q. nº 1168)

Questions jointes de B. Pas, K. Metsu et E. Platteau au ministre de la Justice sur 'le rapatriement de femmes de l'EI' (*C.R.I.*, Chambre, 2021-2022, 1er mai 2022, PLEN 181, p. 2, Q. nos 2544P, 2551P et 2565P)

Question de S. Creyelman au premier ministre sur 'la cyberactivité contre notre pays depuis l'invasion russe en Ukraine' (*Q.R.*, Chambre, 2021-2022, 25 mai 2022, nº 86, p. 69, Q. nº 193)

Question de S. Creyelman au premier ministre sur 'l'agrément des mosquées' (*Q.R.*, Chambre, 2021-2022, 25 mai 2022, nº 86, p. 238, Q. nº 1139)

Question de T. Van Grieken au ministre de la Justice sur la 'vérification de sécurité pour les militaires' (*Q.R.*, Chambre, 2021-2022, 25 mai 2022, nº 86, p. 294, Q. nº 464)

Débat d'actualité et questions jointes de S. Cogolati, M. Freilich, A. Ponthier, G. Dallemagne et K. Verduyckt à la ministre de la Défense sur 'le matériel Huawei du SGRS et de la Défense' (*C.R.I.*, Chambre, 2021-2022, 1er juin 2022, COM 802, p. 10, Q. nos 26849C, 26870C, 26871C, 27247C et 28265C)

Échange de vues sur le suivi des recommandations de la commission d'enquête 'Attentats terroristes' et questions jointes de K Van Vaerenbergh, N. Boukili, O. Vajda, Ph. Pivin, M. Dillen, N. Boukili, G. Dallemagne, S. Rohonyi, M.-Ch. Leroy, K. Aouasti et K. Metsu au ministre de la Justice sur 'recommandations de la commission d'enquête Attentats terroristes pour la Sûreté de l'État' (*C.R.I.*, Chambre, 2021-2022, 3 juin 2022, COM 806, p. 1, Q. nos 28307C, 28321C, 28329C, 28335C, 28338C, 28340C, 28341C, 28345C, 28346C, 28347C, 28348C, 28349C, 28350C, 28351C, 28352C, 28353C, 28354C, 28355C, 28356C, 28357C, 28358C, 28359C, 28360C, 28361C, 28362C, 28363C, 28364C, 28365C, 28368C, 55028369C, 28370C, 28371C, 28372C, 28374C, 28375C, 28376C, 28377C, 28378C, 28386C, 28387C, 28388C, 28390C, 28393C, 28397C, 28389C, 28391C, 28392C, 28394C, 28398C, 28399C, 28400C, 28402C, 28410C, 28411C, 28412C, 28413C, 28418C, 28421C, 28441C, 28443C, 28448C et 28449C)

Question de S. Creyelman à la ministre de la Défense sur 'les investissements supplémentaires dans la Défense' (*Q.R.*, Chambre, 2021-2022, 9 juin 2022, nº 87, p. 239, Q. nº 461)

Question de S. Creyelman à la ministre de la Défense sur les 'mesures de sécurité en matière d'extrémisme au sein de la Défense' (*Q.R.*, Chambre, 2021-2022, 9 juin 2022, nº 87, p. 240, Q. nº 465)

Question d'E. Burton à la ministre de l'Intérieur sur 'les Belges partis en Ukraine pour combattre' (*Q.R.*, Chambre, 2021-2022, 9 juin 2022, nº 87, p. 265, Q. nº 1242)

Questions jointes de M. Freilich au premier ministre sur 'les cyberrisques' (*C.R.I.*, Chambre, 2021-2022, 14 juin 2022, COM 815, p. 6, Q. nos 26784C et 28450C)

Question de T. Vandenput à la ministre de l'Intérieur sur 'les contrôles de sécurité pour les emplois sensibles' (*C.R.I.*, Chambre, 2021-2022, 15 juin 2022, COM 818, p. 15, Q. nº 28264C)

Question d'O. Depoortere à la ministre de l'Intérieur sur 'l'utilisation de routeurs wifi et d'autres produits Huawei au SPF Intérieur' (*C.R.I.*, Chambre, 2021-2022, 15 juin 2022, COM 818, p. 27, Q. nº 28409C)

Question de D. Senesael à la ministre de l'Intérieur sur 'les bandes de motards' (*C.R.I.*, Chambre, 2021-2022, 15 juin 2022, COM 818, p. 32, Q. nº 28579C)

Échange de vues sur le suivi des recommandations de la commission d'enquête 'Attentats terroristes' et questions jointes d'O. Vajda, Ph. Pivin, D. Ducarme et G. Dallemagne à la ministre de l'Intérieur sur 'le suivi des recommandations après les attentats et les recommandations législatives' (*C.R.I.*, Chambre, 2021-2022, 21 juin 2022, COM 824, p. 1, Q. nos 28330C, 28337C, 28643C, 28645C, 28646C, 28647C, 28798C, 28800C, 28802C, 28803C, 28979C, 28980C, 28981C et 28982C)

Question de N. Boukili à la ministre de la Fonction publique sur 'un moratoire éventuel sur le développement du réseau 5G d'Ericsson' (*C.R.I.*, Chambre, 2021-2022, 22 juin 2022, COM 830, p. 1, Q. nº 27264C)

Questions jointes de B. Pas et K. Metsu au premier ministre sur 'le rapatriement des femmes de Daech' (*C.R.I.*, Chambre, 2021-2022, 22 juin 2022, PLEN 190, p. 6, Q. nos 2671P et 2694P)

Question de M. Dillen au ministre de la Justice sur 'les coordinateurs de sécurité pour les prisons' (*C.R.I.*, Chambre, 2021-2022, 29 juin 2022, COM 841, p. 7, Q. nº 29079C)

Question de K. Jadin au ministre de la Justice sur 'le contrôle de l'intégrité du personnel' (*Q.R.*, Chambre, 2021-2022, 27 juin 2022, nº 88, p. 297, Q. nº 1237)

Question d'E. Burton à la ministre de la Défense sur 'les militaires belges partis en Ukraine' (*Q.R.*, Chambre, 2021-2022, 27 juin 2022, nº 88, p. 343, Q. nº 477)

Question de S. Creyelman à la ministre de la Défense sur les 'investissements de la loi de programmation militaire en matière de cyber-commandement' (*Q.R.*, Chambre, 2021-2022, 27 juin 2022, nº 88, p. 359, Q. nº 497)

Question d'O. Depoortere à la ministre de l'Intérieur sur 'la lutte coordonnée en matière de cybersécurité et de cybercriminalité' (*Q.R.*, Chambre, 2021-2022, 27 juin 2022, nº 88, p. 384, Q. nº 1270)

Question de M. Freilich à la ministre de l'Intérieur sur 'les mesures de sécurité pour la communauté juive' (*Q.R.*, Chambre, 2021-2022, 27 juin 2022, nº 88, p. 393, Q. nº 1279)

Question de K. Metsu au secrétaire d'État à l'Asile et la Migration sur 'Fedasil - circulation de l'information' (*Q.R.*, Chambre, 2021-2022, 27 juin 2022, nº 88, p. 480, Q. nº 599)

Question de M. Dillen au ministre de la Justice sur 'l'accès du SGRS à la banque de données SIDIS suite' (*C.R.I.*, Chambre, 2021-2022, 29 juin 2022, COM 841, p. 5, Q. nº 29078C)

Question de P. De Roover au ministre de la Justice sur 'la politique du gouvernement vis-à-vis des terroristes en détention' (*C.R.I.*, Chambre, 2021-2022, 30 juin 2022, PLEN 191, p. 7, Q. nº 2704P)

Questions jointes de K. Metsu, S. Goethals et P. Buysrogge au premier ministre sur 'des précisions sur la stratégie de sécurité nationale' (*C.R.I.*, Chambre, 2021-2022, 5 juillet 2022, COM 844, p. 7, Q. nos 27325C, 27326C, 27327C, 27328C, 27775C, 27950C et 28091C)

Question de P. Buysrogge à la ministre de la Défense sur 'les vérifications de sécurité par le SGRS' (*C.R.I.*, Chambre, 2021-2022, 13 juillet 2022, COM 859, p. 1, Q. nº 28866C)

Question de T. Roggeman au secrétaire d'État à la Digitalisation sur 'le nouveau bâtiment de la Sûreté de l'État' (*Q.R.*, Chambre, 2021-2022, 14 juillet 2022, nº 89, p. 86, Q. nº 338)
Question de M. Dillen au ministre de la Justice sur 'l'augmentations du budget de la VSSE l'État' (*Q.R.*, Chambre, 2021-2022, 14 juillet 2022, nº 89, p. 307, Q. nº 1244)
Question d'E. Platteau à la ministre de l'Intérieur sur 'la banque de données commune reprenant les Terrorist Fighters et les propagandistes de haine' (*Q.R.*, Chambre, 2021-2022, 14 juillet 2022, nº 89, p. 425, Q. nº 1324)
Question de M. Freilich au ministre de la Justice sur 'les fournisseurs à haut risque' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 260, Q. nº 1233)
Question de M. Dillen au ministre de la Justice sur 'l'élimination des déficits et renforcement des services de renseignement et de sécurité' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 265, Q. nº 1247)
Question de M. Dillen au ministre de la Justice sur 'VSSE - amélioration du recrutement et attention portée à la politique du personnel' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 271, Q. nº 1255)
Question de C. Taquin au ministre de la Justice sur 'le suivi et la surveillance des organisations sectaires' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 279, Q. nº 1277)
Question de M. Freilich au ministre de la Justice sur 'TikTok' (Q.R., Chambre, 2021-2022, 11 août 2022, no 90, p. 280, Q. nº 1282)
Question de B. Pas au ministre de la Justice sue 'le rapatriement de combattantes de l'EI belges de Syrie' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 282, Q. nº 1288)
Question d'A. Van Bossuyt au ministre de la Justice sur 'l'espionnage par la Chine' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 284, Q. nº 1291)
Question de G. Dallemagne à la ministre de la Défense sur 'Défense - cyberattaque' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 304, Q. nº 505)
Question de S. Cogolati à la ministre de l'Intérieur sur 'l'AFCN - reconnaissance d'une habilitation de sécurité étrangère' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 351, Q. nº 1339)
Question de K. Metsu à la ministre de l'Intérieur sur 'le plan Canal à Bruxelles et la mise en place des CSIL' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 377, Q. nº 1357)
Question de V. Scourneau à la ministre de l'Intérieur sur la 'sécurité des fonctions sensibles - screening' (*Q.R.*, Chambre, 2021-2022, 11 août 2022, nº 90, p. 392, Q. nº 1369)
Question de K. Aouasti au ministre de la Justice sur 'les bandes de motards' (*Q.R.*, Chambre, 2021-2022, 9 septembre 2022, nº 91, p. 275, Q. nº 1280)
Question de M. Dillen au ministre de la Justice sur le 'projet de protocole d'accord entre la VSSE et la DG EPI' (*Q.R.*, Chambre, 2021-2022, 9 septembre 2022, nº 91, p. 284, Q. nº 1296)
Question d'E. Burton à la ministre de la Défense sur 'le laboratoire clandestin à Klein-Brogel' (*Q.R.*, Chambre, 2021-2022, 9 septembre 2022, nº 91, p. 320, Q. nº 529)
Questions jointes de K. Metsu et B. Pas à la ministre de l'Intérieur sur 'le coût du rapatriement de terroristes de l'EI pour le département de l'Intérieur' (*C.R.I.*, Chambre, 2021-2022, 21 septembre 2022, COM 881, p. 23, Q. nºs 55029655C en 55030088C)
Questions jointes de N. Boukili, A. Laaouej et J. Chanson à la ministre de l'Intérieur sur 'le festival Frontnacht et l'avis de l'OCAM' (*C.R.I.*, Chambre, 2021-2022, 21 septembre 2022, COM 881, p. 44, Q. nºs 55029719C, 55029724C et 55029748C)
Question de K. Aouasti à la ministre de l'Intérieur sur 'le niveau de menace' (*C.R.I.*, Chambre, 2021-2022, 21 septembre 2022, COM 881, p. 64, Q. nº 29926C)
Questions jointes de D. Senesael à la ministre de l'Intérieur sur 'le rapport d'activités 2021 de l'OCAM' (*C.R.I.*, Chambre, 2021-2022, 21 septembre 2022, COM 881, p. 54, Q. nºs 29731C et 29868C)

Question de M. Dillen au ministre de la Justice sur les 'détenus radicalisés - suivi à la fin de la peine - récidive' (*Q.R.*, Chambre, 2021-2022, 28 septembre 2022, nº 92, p. 233, Q. nº 1254)
Question de S Cogolati à la ministre des Affaires étrangères sur les 'vérifications de sécurité dans les installations nucléaires' (*Q.R.*, Chambre, 2022-2023, 28 septembre 2022, nº 92, p. 311, Q. nº 22

Questions jointes de M. Prévot, K. Gabriëls, Ph. Pivin, N. Boukili et K. Aouasti au premier ministre sur 'la politique de sécurité du gouvernement face aux menaces des narcotrafiquants et des terroristes' (*C.R.I.*, Chambre, 2021-2022, 29 septembre 2022, PLEN 203, p. 1, Q. nºs 55002833P, 55002834P, 55002840P, 55002838P et 55002839P)
Question de M. Dillen au ministre de la Justice sur 'l'échange d'informations avec la VSSE' (*Q.R.*, Chambre, 2021-2022, 30 septembre 2022, nº 93, p. 56, Q. nº 1295)
Question de C. Taquin à la ministre de l'Intérieur sur les 'mouvements sectaires - nombre de plaintes' (*Q.R.*, Chambre, 2021-2022, 30 septembre 2022, nº 93, p. 154, Q. nº 1405)
Question de S. Cogolati à la ministre de l'Intérieur sur 'les centrales nucléaires belges face à la menace terroriste' (*Q.R.*, Chambre, 2021-2022, 30 septembre 2022, nº 93, p. 213, Q. nº 1445)
Question d'A. Flahaut à la ministre des Affaires étrangères sur 'l'ANS' (*Q.R.*, Chambre, 2021-2022, 30 septembre 2022, nº 93, p. 231, Q. nº 12)
Questions jointes de G. Dallemagne et O. Vajda à la ministre de l'Intérieur sur 'la direction de l'OCAM' (*C.R.I.*, Chambre, 2021-2022, 21 septembre 2022, COM 894, p. 44, Q. nºs 55030712C, 55030744C et 55030882C)
Questions jointes de Ph. Pivin, S. Rohonyi et O. Vajda au ministre de la Justice sur 'le jugement du tribunal de première instance concernant les dirigeants de l'EMB' (*C.R.I.*, Chambre, 2021-2022, 5 octobre 2022, COM 895, p. 48, Q. nºs 55029965C, 55030162C et 55030674C)
Question de S. Creyelman à la ministre de la Défense sur 'le recrutement de profils adéquats pour la composante Cyber' (*Q.R.*, Chambre, 2022-2023, 9 octobre 2022, nº 94, p. 383, Q. nº 534)
Débat d'actualité sur des cyberattaques et questions jointes de M. Freilich, B. Moyaers, B. Pas, D. Senesael et G. Dallemagne au premier ministre sur 'l'attribution des cyberattaques à des groupes chinois de pirates informatiques' (*C.R.I.*, Chambre, 2022-2023, 18 octobre 2022, COM 899, p. 1, Q. nºs 55029671C, 55029676C, 55029765C, 55029827C, 55030228C, 55030235C et 55030714C)
Question d'Y. Ingels à la ministre de l'Intérieur sur 'les tableaux budgétaires en lien avec l'état de l'Union 2022 et l'ANS' (*C.R.I.*, Chambre, 2021-2022, 19 octobre 2022, COM 907, p. 47, Q. nº 55031319C)
Question de M. Dillen au ministre de la Justice sur la 'radicalisation des détenus en prison' (*Q.R.*, Chambre, 2022-2023, 19 octobre 2022, nº 95, p. 133, Q. nº 1297)
Question de P. Buysrogge au ministre de la Justice sur 'l'infrastructure de la VSSE' (*Q.R.*, Chambre, 2022-2023, 19 octobre 2022, nº 95, p. 152, Q. nº 1358)
Question de K. Metsu au ministre de la Justice sur les 'aspects judiciaires de la lutte antiterrorisme' (*Q.R.*, Chambre, 2022-2023, 19 octobre 2022, nº 95, p. 157, Q. n° 1364)
Question de D. Safai au ministre de la Justice sur 'l'expulsion du prédicateur de haine marocain Abdallah Ouahbour' (*Q.R.*, Chambre, 2022-2023, 19 octobre 2022, nº 95, p. 161, Q. nº 1387
Question de S. Cogolati au ministre de la Justice sur 'l'espionnage académique et industriel chinois' (*Q.R.*, Chambre, 2022-2023, 19 octobre 2022, nº 95, p. 178, Q. nº 1401)
Question d'A. Laaouej au ministre de la Justice sur 'le Frontnacht' (*Q.R.*, Chambre, 2022-2023, 19 octobre 2022, nº 95, p. 199, Q. nº 1413)

Échange de vues sur l'escalade de la violence liée à la drogue et questions jointes d'O. Depoortere, S. Van Hecke, V. Matz, M. Dillen, J. Chanson, S. De Wit, N. Boukili, F. Demon, A. Laaouej, E. Thiébaut, S. Rohonyi, Y. Ingels, S. Van Hecke et E. Platteau à la ministre de l'Intérieur sur 'la crise sécuritaire à Anvers (diverses attaques à Borgerhout, Hoboken et à la gare centrale)' (*C.R.I.*, Chambre, 2021-2022, 24 octobre 2022, COM 913, p. 1, Q. nos 55029729C, 55029739C, 55029740C, 55000317I, 55000318I, 55029776C, 55029784C, 55029785C, 55029819C, 55029820C, 55029967C, 55029968C, 55029976C, 55029984C, 55029994C, 55030001C, 55030013C, 55030014C, 55030015C, 55030016C, 55030018C, 55030019C, 55030020C, 55030021C, 55030022C, 55030025C, 55030026C, 55030031C, 55030032C, 55030033C, 55030036C, 55030037C, 55030039C, 55030040C, 55030044C et 55030146C)

Question de S. Van Hecke au ministre de la Justice sur 'l'extension du personnel de la VSSE - conséquences du suivi des organisations sectaires' (*Q.R.*, Chambre, 2022-2023, 7 novembre 2022, no 96, p. 257, Q. no 1425)

Question de Ph. Pivin à la ministre de l'Intérieur sur 'l'index Institute for Jewish Research et European Union Agency for Fondamentel Rights - études' (*Q.R.*, Chambre, 2022-2023, 7 novembre 2022, no 96, p. 314, Q. no 1500)

Questions jointes d'A. Ponthier et P. Buysrogge à la ministre de la Défense sur 'le recrutement d'anciens pilotes occidentaux de la Défense par la Chine' (*C.R.I.*, Chambre, 2022-2023, 9 novembre 2022, COM 926, p. 6, Q. nos 55031334C et 55031757C)

Questions jointes de S. Cogolati en M.-Ch. Marghem au ministre de la Justice sur 'la présence de postes de police chinois à l'étranger' (*C.R.I.*, Chambre, 2022-2023, 9 novembre 2022, COM 927, p. 9, Q. nos 55031668C et 55031524C)

Question de M.-Ch. Marghem au ministre de la Justice sur 'le mariage du terroriste Salah Abdeslam et la surveillance pénitentiaire' (*C.R.I.*, Chambre, 2022-2023, 9 novembre 2022, COM 927, p. 12, Q. no 55031669C)

Échange de vues sur l'attaque au couteau perpétrée sur des policiers de la zone de police Bruxel-les Nord et questions et interpellation jointes de M. De Maegd, M. Dillen, E. Platteau, O. Depoortere, N. Boukili, K. Metsu, E. Thiébaut, H. Rigot, K. Aouasti, K. Geens, G. Vanden Burre, Ö. Özen et L. Zanchetta à la ministre de l'Intérieur sur 'l'attaque de deux policiers à Bruxelles' (*C.R.I.*, Chambre, 2022-2023, 14 novembre 2022, COM 929, p. 1, Q. nos 55031862C, 55000338I, 55031867C, 55031868C, 55031871C, 55031872C, 55031873C, 55031878C, 55031879C, 55031880C, 55031881C, 55031888C, 55031893C et 55031894C)

Question de C. Taquin au ministre de la Justice sur 'les enquêtes contre les mouvements sectaires' (*Q.R.*, Chambre, 2022-2023, 17 novembre 2022, no 97, p. 148, Q. no 1344)

Question de S. Cogolati au ministre de la Justice sur 'les risques sécuritaires et d'ingérence du contrôle des ports belges par la Chine' (*C.R.I.*, Chambre, 2022-2023, 30 novembre 2022, COM 935, p. 4, Q. nos 55031913C)

Question de S. Cogolati à la ministre de l'Intérieur sur 'la présence de postes de police chinois à l'étranger' (*C.R.I.*, Chambre, 2022-2023, 14 décembre 2022, COM 947, p. 8, Q. no 55031525C)

Questions jointes de M. Freilich et O. Depoortere à la ministre de l'Intérieur sur 'l'apologie du Hamas' (*C.R.I.*, Chambre, 2022-2023, 14 décembre 2022, COM 947, p. 11, Q. nos 55031814C et 55031917C)

Question de N. Boukili au ministre de la Justice sur 'l'espionnage avec Pegasus en Belgique' (*C.R.I.*, Chambre, 2022-2023, 14 décembre 2022, COM 948, p. 44, Q. no 55032489C)

Question de S. Rohonyi au ministre des Classes moyennes sur 'le Qatargate et la lutte contre la corruption' (*C.R.I.*, Chambre, 2022-2023, 15 décembre 2022, PLEN 220, p. 26, Q. no 55003065P)

Question de H. Bogaert à la ministre de la Défense sur 'la suspension d'un sous-officier' (*Q.R.*, Chambre, 2022-2023, 16 décembre 2022, nº 99, p. 249, Q. nº 559)

Question de K. Metsu à la ministre de l'Intérieur sur le 'terrorisme et CSIL-R' (*Q.R.*, Chambre, 2022-2023, 16 décembre 2022, nº 99, p. 301, Q. nº 1608)