Rapport d'activités 2021
Activiteitenverslag 2021

Comité Permanent R
Vast Comité I

Comité Permanent de Contrôle des
services de renseignement et de sécurité

Vast Comité van Toezicht op
de inlichtingen- en veiligheidsdiensten

ACTIVITEITENVERSLAG 2021
RAPPORT D'ACTIVITÉS 2021

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.

ACTIVITEITENVERSLAG 2021

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de
inlichtingen- en veiligheidsdiensten

Voorliggend *Activiteitenverslag 2021* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 25 mei 2022.

(*getekend.*)
Serge Lipszyc, voorzitter
Pieter-Alexander De Brock, raadsheer
Thibaut Vandamme, raadsheer
Frédéric Givron, griffier

Activiteitenverslag 2021
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
BCP	*Business continuity plan*
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
Cama	*Case Manager*
CCB	Centrum voor Cybersecurity Belgium
CCIRM	*Collection Coordination Information Requirement Management* (ADIV)
CCIV	Coördinatiecomité Inlichtingen en Veiligheid
CI	*Counterintelligence*
CIA-model	Confidentiality, Integrity & Availability-model
CMDB	*Component Management Database*
CMRO	Commissie voor de Modernisering van de Rechterlijke Orde
COC	Controleorgaan voor de politionele informatie
Coma	*Collection Manager*
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*

DRI	Directie van de politionele informatie en de ICT-middelen (Federale politie)
DRMB	Dienst voor Religieuze en Morele Bijstand
DRP	*Disaster recovery plan*
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 gegevensbeschermingsautoriteit
GBW	Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (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*
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 veiligheids-machtigingen, 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 1bis 'Het informatiebeheer' van hoofdstuk IV van de WPA
KB OCAD	Koninklijk besluit van 28 november 2006 tot uitvoering van de Wet van10 juli 2006 betreffende de analyse van de dreiging
KMS	Koninklijke Militaire School
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*
NAVO	Noord-Atlantische Verdragsorganisatie
NSIP	Nationaal Strategisch Inlichtingenplan
NTSU-CTIF	*National Technical & Tactical Support Unit – Central Technical Interception Facility* (geïntegreerde politie)
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open sources intelligence*
Parl. St.	Parlementaire Stukken van Kamer en Senaat
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*
SIGINT	*Signals intelligence*
SOP	*Standard Operating Procedures*
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 veiligheids-adviezen
WEC	Wet van 13 juni 2005 betreffende de elektronische communicatie
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

WOORD VOORAF

Het jaar 2021 herinnerde ons eraan hoe kwetsbaar de planeet is, hoe kwetsbaar samenlevingen zijn, hoezeer de democratie op de proef wordt gesteld en hoe precair de rechten van de burgers zijn.

Het verschijnsel van potentieel gewelddadige extremisten - religieus of ideologisch - wordt verder in de hand gewerkt door aanvallen op bepaalde instellingen. Deze aanvallen hebben de instellingen blijvend verzwakt. De aanslag op het Capitool in Washington is ongetwijfeld het meest opvallende voorbeeld van het afwijzen van democratische instellingen. Zou een dergelijk scenario geen gevolgen kunnen hebben voor onze Belgische instellingen?

Dit soort dreiging is verre van verdwenen. Het wordt integendeel versterkt door de sociale media. Zo werden er veel samenzweringstheorieën over COVID-19 verspreid. Hoewel de basis al eerder was gelegd, bleek de pandemie het perfecte voorwendsel om bevolkingsgroepen verder tegen elkaar op te zetten.

Staatsgrepen en het omverwerpen van de 'machthebbers' verplichten ons vandaag, net als in het verleden, om in te grijpen en zelfs onze landgenoten zo nodig te repatriëren. Deze betrachting om te beschermen vereist een versterking van de inzet van onze inlichtingen- en veiligheidsdiensten in het buitenland.

Het proces dat volgde op de aanslagen in Parijs, net zoals het proces in Antwerpen na de verijdelde aanslag in Villepinte, herinneren er ons ook aan dat de inlichtingendiensten hun partnerschap moeten versterken en de gezamenlijke strijd tegen het terrorisme moeten opvoeren.

In België vormden kwesties in verband met jihadistische bewegingen een vruchtbare voedingsbodem voor de toenemende polarisatie van de samenleving. Ook het onderzoeksverslag over het toezicht op extreemrechts heeft zijn relevantie bewezen. Het onderzoek van het Comité heeft, naar aanleiding van de zoektocht naar een gewapende militair die onze instellingen bedreigde, aangetoond hoe kwetsbaar sommige van onze instellingen zijn ten aanzien van dit verschijnsel, dat niet enkel onze buurlanden treft.

Wat onze inlichtingendiensten betreft, mogen wij niet vergeten dat ons land een kruispunt is voor vele Europese en internationale instellingen, alsook voor vele gemeenschappen en opposanten. Deze bijzondere situatie vereist een permanente investering in het versterken van de bescherming van de vermelde entiteiten en personen en ook in de strijd tegen buitenlandse inmenging.

De veiligheidsdiensten moeten worden aangemoedigd om proactiever op te treden en beter op elkaar in te spelen, om zo te streven naar een geconsolideerde en samenhangende Belgische inlichtingen- en veiligheidsgemeenschap. Ik steun Jaak Raes, administrateur-generaal van de Veiligheid van de Staat, in zijn streven om de 'need to know' te verzoenen met de 'need to share'.

Ik steun eveneens het project voor een geïntegreerd personeelsstatuut voor het personeel van de inlichtingen- en veiligheidsdiensten. Het is zonder twijfel een onontbeerlijke stap in de ontwikkeling van synergieën tussen de diensten. Ik roep op tot het optimaliseren van de middelen en het versterken van de beschikbare deskundigheid in de strijd tegen bedreigingen. Ik ben van mening dat het veiligheidsvraagstuk een meer duidelijke en ambitieuzere strategische visie van de Nationale Veiligheidsraad vereist op het vlak van de veiligheidsuitdagingen die ons door de constante wijziging van onze samenleving worden opgelegd.

Door de impact van COVID-19 werd de dagelijkse organisatie van het Comité grondig ontwricht. De continuïteit van de werkzaamheden kon alleen worden gewaarborgd dankzij het vastberaden en professioneel bewustzijn van ieder van ons. Onze medewerkers verdienen des te meer lof voor het feit dat zij slechts in beperkte mate gebruik hebben kunnen maken van telewerk. Wij beschikken nog steeds niet over het noodzakelijke beveiligde digitale netwerk om onze dagdagelijkse opdrachten naar behoren uit te voeren. De uitdagingen zijn talrijk, en het Comité wil er dan ook op een afdoende manier op reageren.

De noodzakelijke werkzaamheden op het gebied van synergie die door de Kamer zijn aangevat, stellen ons op heden in staat om de grondslagen ervan te zien. Logischerwijs roept dit nog steeds een aantal vragen en ongerustheid op, maar anderzijds geeft het ook aanleiding tot hoopvolle vooruitzichten. De versterking van het Comité als instelling blijft actueel, net zoals de vragen die zijn gerezen naar aanleiding van het openen van dossiers over het gebruik van *spyware*, het opvolgen van een imam en het volgen van veroordeelde terroristen… Ook al is onze instelling niet de enige, toch is het Vast Comité I een essentiële verdediging van onze rechtsstaat.

Dit jaar wuifden we Martine, Josiane, Wouter, Charles, Ludo, Frank, Jean-Philippe en Christophe uit. Ik wil graag deze medewerkers bedanken voor hun betrokkenheid.

Ik hoop dat het lezen van dit verslag bijdraagt tot een betere perceptie van ons werk en ik wens u een 'stimulerende' lezing!

25 mei 2022,
Serge Lipszyc,
Voorzitter van het Vast Comité van toezicht
Inlichtingen- en veiligheidsdiensten

HOOFDSTUK I.
DE TOEZICHTONDERZOEKEN

In 2021 finaliseerde het Vast Comité I tien toezichtonderzoeken, waarvan drie gezamenlijk met het Vast Comité van Toezicht op de politiediensten. Ook de drie informatiedossiers die werden besproken met de parlementaire Begeleidingscommissie, werden opgenomen in voorliggend hoofdstuk (I.4, I.6 en I.7).

Het zijn diverse instanties of personen die het Comité kunnen 'vatten' met een toezichtonderzoek: de Begeleidingscommissie, de voogdijministers, elke (rechts-) persoon die klacht of aangifte wenst te doen… Het Comité kan ook zelf het voortouw nemen: vijf van de tien in 2021 gefinaliseerde onderzoeken werden ambtshalve opgestart. Uitzonderlijk werden vier onderzoeken uitgevoerd op verzoek van de parlementaire Begeleidingscommissie. Slechts één toezichtonderzoek werd uitgevoerd op vraag van de minister van Defensie. Het Comité zette tevens zijn werkzaamheden voort in het kader van zeven in 2021 of eerder opgestarte onderzoeken. Een korte omschrijving van deze nog lopende en/of opgestarte onderzoeken, volgt in I.14. De naar aanleiding van de toezichtonderzoeken geformuleerde aanbevelingen werden gebundeld in Hoofdstuk XI.

In totaal ontving het Comité in 2021 75 klachten of aangiften.[1] Na een kort vooronderzoek en de verificatie van een aantal objectieve gegevens, wees het Comité 23 klachten of aangiften af omdat ze kennelijk niet gegrond waren[2] (art. 34 W.Toezicht) en in 28 gevallen bleek het Comité onbevoegd om de opgeworpen vraag te behandelen. In dat laatste geval werden de klagers doorverwezen naar de bevoegde instanties (bijv. de Brusselse procureur des Konings, het Vast Comité P of nog, de Gegevensbeschermingsautoriteit). 14 van de 24 van de klachten konden worden afgerond in 2021, tien klachten waren begin 2022 nog in behandeling. In 2021 werden 16 van de 24 klachten gehercategoriseerd als DPA-klacht.[3]

---

1 Eerst wordt de ontvankelijkheid bestudeerd en de klacht 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 'V.6. De behandeling van individuele verzoeken'.

I.1. HET OCAD EN DE ONDERSTEUNENDE DIENSTEN (OPVOLGING)

In juni 2020 rondde het Vast Comité I, samen met het Vast Comité P, een toezichtonderzoek af naar de ondersteunende diensten van het Coördinatieorgaan voor de dreigingsanalyse (OCAD).[4] Dit onderzoek had betrekking op vier ondersteunende diensten: de FOD Binnenlandse Zaken (Dienst Vreemdelingenzaken), de FOD Buitenlandse Zaken, de FOD Mobiliteit en Vervoer en de FOD Financiën (Administratie Douane en Accijnzen).[5] Het doel van het onderzoek was om de relaties tussen de vernoemde ondersteunende diensten en het OCAD te onderzoeken wat betreft de samenwerking en informatie-uitwisseling. Hierbij werd aandacht geschonken aan de rechtmatigheid, de doelmatigheid en de coördinatie van deze samenwerking en informatie-uitwisseling.

Teneinde een antwoord te kunnen bieden op de vragen vanuit de parlementaire Begeleidingscommissie naar een stand van zaken van de geïmplementeerde aanbevelingen uit dit onderzoek, werd begin juni 2020 door de Vaste Comités I en P besloten een opvolgingsonderzoek op te starten.[6]

Het initiële onderzoek had de naleving van de verwerkings- en bewaringsregels van geclassificeerde documenten alsook de goede informatiestromen tussen enerzijds de FOD Buitenlandse Zaken en de FOD Binnenlandse Zaken (Dienst Vreemdelingenzaken) en anderzijds het OCAD aangetoond.

In hun toezichtrapport formuleerden de Vaste Comités I en P een aantal specifieke aanbevelingen voor de FOD Financiën (Administratie Douane en Accijnzen) dat een plan had ontwikkeld om tegemoet te komen aan de verwachtingen gesteld aan de ondersteunende diensten. Als antwoord op de algemene conclusies en aanbevelingen van het rapport, had ook de FOD Mobiliteit en Vervoer getracht zijn samenwerking met het OCAD te verbeteren. Het opvolgonderzoek concentreerde zich dan ook op de maatregelen genomen door beide administraties.

---

4 Zie VAST COMITÉ I, *Activiteitenverslag 2020*, 2-11 ('I.1. De ondersteunende diensten van het OCAD').

5 De inlichtingen- en politiediensten vormden reeds eerder het voorwerp van een gemeenschappelijk toezichtonderzoek naar de ondersteunende diensten van het OCAD. Hierover VAST COMITÉ I, *Activiteitenverslag 2010*, 46 ('II.12.6. Mededeling van inlichtingen aan het OCAD door de ondersteunende diensten) en meer uitgebreid *Activiteitenverslag 2011*, 25-32 ('II.4. De informatiestromen tussen het OCAD en zijn ondersteunende diensten').

6 De resultaten van dit onderzoek werden in april 2021 in de Begeleidingscommissie besproken.

I.1.1. DE OPVOLGING VAN DE AANBEVELINGEN DOOR DOUANE EN ACCIJNZEN

In antwoord op de twee specifieke aanbevelingen geformuleerd in het toezichtrapport uit 2020, stelde de Algemene Administratie Douane en Accijnzen een actieplan op. Op het ogenblik van het afsluiten van het onderzoek (begin 2021) waren de meeste van de in het actieplan opgenomen maatregelen deels in uitvoering. Omwille van de gezondheidscrisis, konden een aantal acties nog niet worden gerealiseerd.

Een eerste specifieke aanbeveling bestond erin dat de dienst een interne analyse zou uitvoeren om te bepalen welke soort informatie die de administratie verzamelt, nuttig zou kunnen zijn voor het OCAD. Een eerste maatregel voorzag dan ook in het opstellen van een plan voor het verzamelen van gegevens op basis van indicatoren van extremisme of terrorisme. Er werd tevens een sensibiliseringsproject opgestart om het signaleren en delen van informatie aan te moedigen. Daartoe werden opleidingen voorzien, in het bijzonder over de indicatoren extremisme en terrorisme. De Administratie Douane en Accijnzen besliste tevens om een inventaris op te maken van de verschillende informatiebronnen waarover ze beschikt (informatie verkregen tijdens operationele activiteiten van de Administratie Operaties en de Administratie Opsporing, alsook informatie opgeslagen in andere interne gegevensbanken). In maart 2021 had de Administratie Opsporing van de Douane en Accijnzen nog altijd geen toegang tot de door het OCAD beheerde gemeenschappelijke gegevensbank.

Een tweede aanbeveling betrof het treffen van gepaste maatregelen om de minimumnormen met betrekking tot de bewaring en raadpleging van geclassificeerde documenten na te leven. Naast de aanschaf van nieuwe brandkoffers en de invoering van een volledig register voor geclassificeerde documenten, werd tevens een handboek voor de gebruikers van geclassificeerde informatie voorbereid door de veiligheidsofficier. Verder beperkte de Administratie Opsporing de toegang tot het BINII-lokaal (*Belgian Intelligence Network Information Infrastructure*, een communicatieplatform voor de uitwisseling van geclassificeerde informatie). Het actieplan voorzag tevens in de periodieke verificatie van de veiligheidsmachtigingen alsook in de organisatie van veiligheidsbriefings voor de houders van een veiligheidsmachtiging.

De Vaste Comités P en I stelden vast dat de Administratie Douane en Accijnzen een aantal acties had ondernomen en een aantal maatregelen had uitgewerkt die nodig waren om tegemoet te komen aan de aanbevelingen uit het initiële onderzoeksrapport.

I.1.2. DE OPVOLGING VAN DE AANBEVELINGEN DOOR DE FOD MOBILITEIT EN VERVOER

Niettegenstaande er in het gezamenlijk verslag van de Vaste Comités I en P geen specifieke aanbevelingen werden geformuleerd voor de FOD Mobiliteit en Vervoer, ontwikkelde ook deze steundienst een plan, vergezeld van een timing, om de doeltreffendheid van zijn activiteiten met het OCAD te verbeteren. In dat plan wordt enerzijds aandacht besteed aan sensibilisering via informatiesessies voor de interne diensten met betrekking tot de rol en de functie van het OCAD en van de Crisiscel van de FOD Mobiliteit en Vervoer. Er werden in 2020 diverse vergaderingen georganiseerd door deze crisiscel om de opdracht van de OCAD toe te lichten alsook de doelstellingen van de samenwerking, en dit met het oog op het identificeren van verbeter- en actiepunten. Zowat gelijktijdig en op het moment van het afsluiten van het toezichtonderzoek, was in de schoot van het FOD Mobiliteit en Transport een nieuwe informaticatool in ontwikkeling. Deze tool moet het beheer en de uitwisseling van informatie tussen het OCAD en de FOD vergemakkelijken.

Verder werd de nadruk gelegd op de uitbouw en de invoering van bevoorrechte kanalen voor het beheren en doorgeven van gegevens, zowel intern de FOD Mobiliteit en Vervoer als met externe diensten. In dat kader werd een handboek met procedures over het beheer van geclassificeerde documenten en het BINII-systeem intern gevalideerd.

De effecten van bovenvernoemde maatregelen kunnen pas mettertijd worden geëvalueerd. De crisiscel liet bij afloop van het onderzoek optekenen dat ze nog altijd veel te veel gegevens of evaluaties afkomstig van het OCAD krijgt, maar begrijpt dat het voor het OCAD moeilijk is om de doorgezonden informatie te filteren.

I.1.3. CONCLUSIE

Zowel de FOD Financiën, Douane en Accijnzen als de FOD Mobiliteit en Vervoer hebben actieplannen uitgewerkt om te voldoen aan de algemene besluiten en aanbevelingen uit het eindverslag van het voornoemde onderzoek. Deze verschillende maatregelen zouden het inderdaad mogelijk moeten maken om de veiligheid van de doorgezonden gegevens beter te garanderen, de informatiestroom te vergemakkelijken en binnen deze ondersteunende diensten te komen tot een betere kennis van het OCAD en zijn opdrachten.

I.2. HET OCAD EN DE 'BIJKOMENDE' ONDERSTEUNENDE DIENSTEN

Bij KB van 17 augustus 2018 werd de lijst van ondersteunende diensten van het OCAD uitgebreid met nog vier diensten, te weten het Nationaal Crisiscentrum, de Thesaurie, het Gevangeniswezen en de Dienst Erediensten en Vrijzinnigheid bij de FOD Justitie. Hoewel deze beslissing dateert van augustus 2018, maakten deze diensten nog geen deel uit van het eerste onderzoek[7] omdat het te vroeg was om de informatiestroom en de in dat kader geïmplementeerde processen te kunnen analyseren. Een nieuw met het Vast Comité P gemeenschappelijk toezichtonderzoek drong zich op.[8]

I.2.1. DE INFORMATIESTROOM TUSSEN HET OCAD EN DE VIER 'BIJKOMENDE' ONDERSTEUNENDE DIENSTEN

Het onderzoek had tot doel de relaties tussen de vier (bijkomende) ondersteunende diensten en het OCAD te bestuderen op het vlak van de doorgifte van informatie naar het OCAD en omgekeerd, alsook op het vlak van de wettelijkheid, de doeltreffendheid en de coördinatie.

Een kwantitatieve analyse van de uitwisseling gaf een eerste indruk van de informatiestromen tussen de steundiensten en het OCAD.

7 Zie VAST COMITÉ I, *Activiteitenverslag 2020*, 2-11 ('I.1. De steundiensten van het OCAD').

8 Ook hiervan werden de resultaten ter bespreking voorgelegd aan de parlementaire Begeleidings-commissie in april 2021.

	2019				
	TOTAAL	IN	OUT	RFI IN	RFI OUT
FOD Justitie - Dienst Erediensten en Vrijzinnigheid	**13**	8	5	8	0
FOD Justitie - Directoraat-generaal Penitentiaire Inrichtingen (DG EPI)	**2273**	2223	50	224	2
FOD Financiën - Algemene Administratie van de Thesaurie	**17**	14	3	7	0
FOD Binnenlandse Zaken - Algemene Directie Crisiscentrum (ADCC)	**2940**	1334	1606	7	8

Tabel 1: Cijfergegevens ontvangen van het OCAD. De gegevens "IN" zijn de inkomende gegevens bij het OCAD komende van de ondersteunende dienst en de gegevens "OUT" zijn de uitgaande gegevens van het OCAD naar de ondersteunende dienst.

De tabel[9] geeft de informatiestroom voor het jaar 2019 tussen het OCAD en de vier ondersteunende diensten weer. De diverse evaluaties vanuit het OCAD, maken geen deel uit van deze gegevens, met uitzondering deze verstuurd naar het Crisiscentrum, als eerste bestemmeling van de evaluaties.

I.2.1.1. FOD Binnenlandse Zaken – Algemene Directie Crisiscentrum

Door zijn opdrachten staat het Crisiscentrum (via zijn Directie *Incident & Crisis Management*) voortdurend in contact met het OCAD. Immers, het centrum bepaalt op basis van de dreigingsevaluaties gemaakt door het OCAD de te nemen maatregelen. In dat opzicht vinden er zeer vaak coördinatie- en veiligheidsvergaderingen plaats, en dit al voordat het Crisiscentrum als ondersteunende dienst werd opgenomen.

De informatiestroom van het OCAD naar het Crisiscentrum is de belangrijkste van de vier bijkomende steundiensten en betreft merendeel evaluaties. Het Crisiscentrum daartegen levert bijzonder weinig informatie aan, tenzij over evenementen of de komst van buitenlandse personaliteiten (bijv. door verzoeken om dreigingsevaluaties). De reden voor de aanwijzing tot steundienst is te vinden in

[9] Deze gegevens werden door het OCAD meegedeeld en werden getrokken uit de databank PROTEUS. Het gaat dus enkel om informatiestromen die door het OCAD relevant worden geacht. De cijfers houden geen rekening met verzoeken (of uitwisselingen) die niet ingevoerd zijn in PROTEUS, bijv. RFI's naar het OCAD gestuurd voor ongekende entiteiten.

de oprichting van de *Belgian Passenger Information Unit* (BelPIU) in de schoot van het Crisiscentrum.[10]

Aangezien het Crisiscentrum en het OCAD voortdurend met elkaar in contact staan en hun kantoren dicht bij elkaar liggen, zijn er geen personeelsleden van het Crisiscentrum gedetacheerd bij het OCAD. De informatiestroom met het OCAD wordt als zeer goed omschreven door de Directie ICM. De procedures die werden ingevoerd, onder meer het gebruik van functionele mailboxen, geven voldoende garanties tegen het mogelijks verlies van informatie.

De informatie-uitwisseling verloopt via drie kanalen: per e-mail (voor de niet-geclassificeerde informatie en evaluaties), via BINII voor geclassificeerde documenten en via de gemeenschappelijke gegevensbanken dewelke het Crisiscentrum rechtstreeks kan bevragen (*hit/no hit*). De veiligheidsmaatregelen aangaande geclassificeerde documenten worden gerespecteerd en toegepast door de veiligheidsofficier.

I.2.1.2. FOD Justitie – Directoraat-generaal Penitentiaire Inrichtingen

Het voornaamste contactpunt van het OCAD bij de FOD Justitie Directoraat-generaal Penitentiaire Inrichtingen is de dienst CelEx (Cel Extremisme), belast met de opvolging van als geradicaliseerd gesignaleerde gedetineerden.

Er werden twee medewerkers van de CelEx als expert gedetacheerd bij het OCAD. Ze dragen ook op die manier bij tot de opdrachten van het OCAD, bijvoorbeeld in het kader van de opvolging en evaluatie van *foreign terrorist fighters* in de schoot van de werkgroep Gevangenissen, of nog, in de *Local Task Forces* (LTF). Ze bleken daarentegen onvoldoende geïnformeerd over de veranderingen binnen het Directoraat-generaal Penitentiaire Inrichtingen (DG EPI). Terwijl de CelEx deze detachering niet meteen als een meerwaarde beschouwd maar eerder als een capaciteitsverlies, wordt de expertise over het gevangeniswezen van de twee medewerkers door het OCAD zeker naar waarde geschat.

De informatiestroom met de DG EPI verloopt in grote mate naar het OCAD. DG EPI verstrekt een grote hoeveelheid informatie uit het gevangenisnetwerk aan het OCAD en ontvangt in retour daarvoor evaluaties van gevangenen. Het is ook de dienst die de meeste verzoeken om informatie (RFI) bij het coördinatieorgaan indient.

---

[10] De Passagiersinformatie-eenheid (of *Belgian Passenger Information Unit* – BelPIU) staat in voor het verzamelen, het opslaan en het verwerken van de gegevens van passagiers die een internationaal transportmiddel vanuit, naar of via België gebruiken, en dit zowel binnen als buiten de Europese Unie. De passagiersgegevens worden voortdurend doorgegeven door de vervoerders en worden geanalyseerd aan de hand van vooraf bepaalde criteria en vergeleken met de databanken GGB en ANG. Wanneer er een '*hit*' is in de GGB (overeenstemmende identiteiten), worden de gegevens ingevoerd in de GGB en gestuurd aan onder meer het OCAD. De gegevens kunnen tevens worden gebruikt voor gerichte opzoekingen.

De toegang tot de GGB en de voeding ervan vergemakkelijken deze informatiestroom. Voorts zorgen de ingevoerde communicatie- en verzendingsroutines (per e-mail via de functionele boxen of per drager voor geclassificeerde documenten) voor een vlotte werking.

De CelEx moet echter een grote informatiestroom vanuit het gevangenisnetwerk beheren. Hoewel de dienst zegt geen personeelstekort te hebben, wordt benadrukt dat er IT-instrumenten nodig zijn om alle informatie die de dienst ontvangt, beter te kunnen analyseren en beheren.

Een officiële permanentie zou ook zeker een belangrijke toegevoegde waarde betekenen voor DG EPI en zijn diverse partners.

I.2.1.3. FOD Financiën – Algemene Administratie van de Thesaurie

De samenwerking tussen het OCAD en de Algemene Administratie van de Thesaurie van de FOD Financiën speelt zich louter af in het kader van de bevriezing van tegoeden van personen gelinkt aan terrorisme.[11] De afdeling Financiële sancties binnen de dienst *Compliance* is daartoe het contactpunt van het OCAD.

De informatiestroom tussen deze ondersteunende dienst en het OCAD is kwantitatief gering, hetgeen kan worden verklaard door de specifieke aard van hun samenwerking. Bovendien komt het zeer zelden voor dat de Algemene Administratie van de Thesaurie informatie verzamelt die als relevant wordt beschouwd voor de OCAD.

Sinds februari 2019 is één personeelslid bij OCAD gedetacheerd. De procedures voor de bevriezing van tegoeden nemen echter slechts 20% van zijn werktijd in beslag. Dit personeelslid is verbonden aan de Dienst Strategische ondersteuning - Communicatie van het OCAD en daar verantwoordelijk voor administratieve taken.

De met de Thesaurie uitgewisselde informatie is niet geclassificeerd. De uitwisselingen gebeuren hoofdzakelijk per e-mail via de functionele en professionele mailboxen. Sinds eind 2020 heeft de Thesaurie ook rechtstreeks toegang tot de GGB en is zij verplicht gegevens te verstrekken. Er werd, wat betreft de toegang tot en de codering in de GGB, door de veiligheidsofficier een interne procedure opgesteld.

I.2.1.4. FOD Justitie – Directoraat-generaal Wetgeving en Fundamentele rechten en Vrijheden – Dienst Erediensten en Vrijzinnigheid

De aanwijzing van de Dienst Erediensten en Vrijzinnigheid als ondersteunende dienst voor het OCAD moet worden gezien in het licht van zijn bevoegdheden

[11] Omzendbrief van 7 september 2015 betreffende de toepassing van de artikelen 3 en 5 van het KB van 28 december 2006 inzake specifieke beperkende maatregelen tegen bepaalde personen en entiteiten.

in het kader van de erkenning van niet-confessionele godsdiensten en levensbeschouwelijke organisaties en het beheer van het statuut van geestelijken en vertegenwoordigers van de Centrale Vrijzinnige Raad (CVR). Het OCAD werkt in het bijzonder samen met de Cel terrorisme en radicalisering. Dit nieuwe statuut maakt het mogelijk de overdracht van informatie te legaliseren, alhoewel de dienst weinig informatie verzamelt die relevant is voor het coördinatieorgaan.

Er werd erg snel een vergadering belegd tussen het OCAD en deze bijkomende ondersteunende dienst om de samenwerkingsmodaliteiten tussen beiden en tussen de functionaris voor gegevensbescherming en de veiligheidsofficier van de FOD Justitie nader te omschrijven met het oog op het opzetten van de ICT-toegangen van de GGB.

De Dienst Erediensten en Vrijzinnigheid heeft inderdaad toegang tot de GGB. Hoewel het wettelijk kader alleen voorziet in toegang tot de Gegevensbank Haatpropagandisten (GGB HP) door middel van rechtstreekse bevraging (*hit/no hit*), heeft de dienst in de praktijk een volledige toegang tot de GGB - hetgeen de dienst nuttig en noodzakelijk acht. Het Comité achtte het aangewezen om deze toegang te regulariseren.[12]

Er is geen personeelslid bij het OCAD gedetacheerd, maar een medewerker van het coördinatieorgaan werd aangewezen als contactpunt.

De (beperkte) uitwisseling van informatie vindt hoofdzakelijk per e-mail plaats. De ondersteunende dienst beschikt niet over een functionele mailbox: de e-mails worden systematisch naar de twee leden van de Cel terrorisme en radicalisering en naar het hoofd van de dienst gestuurd. Geclassificeerde documenten worden doorgegeven via het BINII-systeem, ondertussen operationeel binnen de FOD Justitie, maar in afwachting van de ontwikkeling van interne procedures voor het gebruik ervan.

I.2.2. VASTSTELLINGEN EN CONCLUSIES

Elk van de vier nieuwe ondersteunende diensten heeft een contactpunt aangewezen voor zijn uitwisselingen met het OCAD, dat de met het coördinatieorgaan uitgewisselde informatie centraliseert. Bij het OCAD zijn personeelsleden gedetacheerd voor DG EPI (twee personen) en de Thesaurie (één persoon). Terwijl DG EPI dit als een verlies van capaciteit beschouwt, waardeert het OCAD de deskundigheid waarover deze personeelsleden beschikken.

De uitwisseling van informatie is het belangrijkst met het Crisiscentrum en het DG EPI. Wat de Thesaurie en de Dienst Erediensten en Vrijzinnigheid betreft, blijft de samenwerking met OCAD zeer specifiek en beperkt tot hun bevoegdheden.

---

12 Zie 'Hoofdstuk V. De controle van de gegevensbanken' (V.2.3)'.

Het OCAD is van mening dat de uitwisseling van informatie met de vier bijkomende ondersteunende diensten zeer goed verloopt. Hoewel er in het verleden reeds uitwisselingen plaatsgevonden, legaliseert de aanwijzing als ondersteunende dienst deze samenwerking, in het bijzonder voor wat betreft de GGB. Via zijn dienst dossier- en documentatiebeheer, stelt het OCAD een permanentie ter beschikking en kan rekenen op een functionele mailbox voor alle informatie-uitwisselingen. Ook de vier ondersteunende diensten zijn van mening dat de informatie-uitwisseling met OCAD zeer goed verloopt. Met uitzondering van de Dienst Erediensten en Vrijzinnigheid, beschikken zij allen over een functionele mailbox.

De minimumveiligheidsnormen voor de bewaring van geclassificeerde documenten worden nageleefd. De procedure voor het gebruik van het BINII-systeem moet echter nog worden afgerond voor de FOD Justitie. Alleen de Thesaurie wisselt geen geclassificeerde informatie uit met het OCAD.

I.3. DE UITWISSELING VAN INFORMATIE OVER EEN WERKNEMER TUSSEN INLICHTINGENDIENSTEN EN EEN PRIVATE- OF PUBLIEKE WERKGEVER

In augustus 2019 ontving het Vast Comité I een klacht van een persoon die werkzaam was voor een publieke instelling. Deze persoon beklaagde zich over het feit dat zijn werkgever informatie had opgevraagd over hem bij een inlichtingendienst en op basis daarvan disciplinaire stappen wou ondernemen.

Na ontvangst van de klacht, en met het oog op de behandeling ervan, werd beslist een onderzoek te openen naar de meer algemene vraag in welke gevallen en onder welke voorwaarden een private of publieke instantie een vraag kan richten tot een of beide inlichtingendiensten over een (kandidaat-)werknemer alsook in welke gevallen de betrokken inlichtingendienst hierop een antwoord mag of moet formuleren en aan welke vereisten dit antwoord vervolgens moet voldoen.[13]

[13] Eind december 2019 werd een extern juridisch advies gevraagd over de eerbiediging van de privacy-rechten van werknemers in het kader van eventuele uitwisselingen tussen werkgevers en inlichtingendiensten.

I.3.1. HET ALGEMENE KADER

Of een inlichtingendienst nu op eigen initiatief of op vraag van een werkgever informatie verschaft over een (kandidaat-)werknemer, in beide gevallen betreft het een inmenging in de privacy en in het recht op de bescherming van persoonsgegevens, ook al betreft het een arbeidsrelatie. Dergelijke inmenging is slechts toegelaten indien er een duidelijke wettelijke basis is, indien de inmenging een legitiem doel nastreeft en proportioneel is (art. 8 EVRM, Conventie 108 en 108+ en art. 22 Grondwet).

Er dient in dit kader ook verwezen te worden naar artikel 2 §1, tweede lid, W.I&V dat stelt dat de inlichtingendiensten '*bij het vervullen van hun opdrachten zorgen (…) voor de naleving van, en (bij)dragen (…) tot de bescherming van de individuele rechten en vrijheden alsook tot de democratische ontwikkeling van de maatschappij*'.

Geen enkele bepaling uit de Inlichtingenwet verbiedt dat een private of publieke instantie een vraag zou richten tot een van de Belgische inlichtingendiensten. Indien een werkgever informatie opvraagt bij een inlichtingendienst, vormt dit een inmenging in het privéleven die slechts mogelijk is indien er een duidelijke wettelijke basis voorhanden is. De Inlichtingenwet laat dit toe in de mate waarin de werkgever met rede van oordeel is dat de inlichtingen die hij doorstuurt nuttig kunnen zijn voor de uitvoering van de opdrachten van de betrokken inlichtingendienst (art. 14 W.I&V m.b.t. publieke actoren; art. 16 W.I&V m.b.t. private actoren).

De Belgische wetgever heeft slechts in twee gevallen voorzien dat een werkgever (op eigen verzoek of op initiatief van de inlichtingendienst) rechtstreeks of onrechtstreeks informatie kan bekomen over een (kandidaat-)werknemer: in geval van een veiligheidsscreening of in geval van een dreiging. Ook de loutere vraag of een (kandidaat-)werknemer[14] al dan niet 'gekend' is bij één van de twee Belgische inlichtingendiensten, moet kunnen aangeknoopt worden bij een van deze twee regelingen.

I.3.2. DE WERKGEVER WIL EEN VEILIGHEIDSSCREENING

I.3.2.1. De wettelijke basis voor veiligheidsscreenings

Met veiligheidsscreenings worden situaties bedoeld waarbij een werkgever, los van een voorafgaandelijk element, alle personen wil laten *screenen* die een bepaalde toelating of vergunning behoeven. Een private of publieke werkgever kan van deze

[14] De meest klassieke voorbeelden zijn deze van een veiligheidsmachtiging om toegang te krijgen tot geclassificeerde informatie, het veiligheidsattest om toegang te krijgen tot een bepaald locatie of een bepaald evenement, of nog, het veiligheidsadvies dan kan aangevraagd worden voor tientallen verschillende toelatingen.

mogelijkheid gebruik maken onder de voorwaarden bepaald in de Classificatiewet van 11 december 1998. In principe zal de werkgever alleen het resultaat van de *screening* krijgen.[15]

In bepaalde gevallen (bijv. bij een veiligheidsmachtiging) is de werknemer onderworpen aan een vorm van een 'permanente s*creening*'. Hij moet m.a.w. gedurende de hele looptijd van zijn machtiging voldoen aan de vereisten om die machtiging te bekomen. Indien een werkgever op een gegeven ogenblik twijfelt aan die voorwaarde, kan hij hierover zijn veiligheidsofficier raadplegen. Deze kan op zijn beurt de veiligheidsoverheid en/of de onderzoekende inlichtingendienst vatten. Maar niets belet dat de werkgever rechtstreeks contact opneemt met een inlichtingendienst indien hij van oordeel is dat hij over informatie beschikt die nuttig is voor de uitoefening van hun opdrachten (artt. 14 of 16 W.I&V).

Het is dus van belang te onderlijnen dat de wettelijke regeling duidelijk bepaalt welke persoonsgegevens onder welke vorm (bijv. een onderzoeksverslag) aan welke bestemmeling (meestal een veiligheidsoverheid) kunnen worden overgezonden.

I.3.2.2. Artikel 19, eerste lid, eerste zinsnede W.I&V[16]

Het Comité wijst er op dat artikel 19 van de Inlichtingenwet geen grondslag biedt voor het systematisch doorgeven van informatie aan werkgevers die hierom verzoeken in het kader van de door hen te verlenen toelatingen of vergunningen.

---

15 Het is de veiligheidsofficier - de persoon aangeduid binnen een private of publieke instantie, die instaat voor de naleving van de classificatieregels en de contactpersoon tussen de instantie, de betrokkene en de bevoegde veiligheidsoverheid - die op de hoogte zal zijn van de concrete elementen van het dossier. Maar deze veiligheidsofficier is op zijn beurt onderworpen aan een specifiek en strafrechtelijk gesanctioneerd beroepsgeheim (artt. 23 en 24 Classificatiewet). Hij kan de elementen waarover hij beschikt niet zomaar meedelen aan de werkgever.

16 Het volledige eerste lid van art. 19 W.I&V luidt als volgt: "*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.*"

I.3.3. DE WERKGEVER IS HET VOORWERP VAN EEN (VERMEENDE) DREIGING

I.3.3.1. Artikel 19, eerste lid, laatste zinsnede W.I&V

Artikel 19 W.I&V luidt als volgt: '*De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee (…) aan de instanties en personen die het voorwerp zijn van een dreiging bedoeld in de artikelen 7 en 11*.'[17]

Dit artikel vormt een duidelijke wettelijke basis voor een inlichtingendienst om (persoons)gegevens mee te delen aan publieke of private[18] personen en instanties, en dus desgevallend ook aan een werkgever wiens werknemer een dreiging vormt die wettelijk gezien moet worden opgevolgd door de VSSE of de ADIV.

De bepaling vormt, in samenlezing met artikel 14 of 16 W.I&V, ook de wettelijke grondslag voor een verontruste publieke of private werkgever die een inlichtingendienst bevraagt over zijn werknemer omdat die naar het oordeel van de werkgever een (mogelijke) dreiging vormt in de zin van de Inlichtingenwet.[19] Deze bepalingen vormen ook de wettelijke basis om naar aanleiding van deze vraag desgevallend concrete elementen mee te delen over de werknemer die die (vermeende) dreiging aannemelijk kunnen maken.[20]

I.3.3.2. Een nadere uitwerking van deze regeling in een richtlijn?

Nu de laatste zinsnede van artikel 19, eerste lid W.I&V voldoende duidelijk is als de wettelijke basis voor informatieoverdracht naar publieke en private instanties, is er wél een verplichting om de modaliteiten van deze mogelijkheid nader uit te werken.

---

17 Het Comité voerde al eerder twee toezichtonderzoeken uit waarbij de toepassing van de laatste zinsnede van artikel 19, eerste lid, W.I&V centraal stond: VAST COMITÉ I, *Activiteitenverslag 2015*, 41 e.v. ('II.9. Klacht over het verstrekken van persoonlijke informatie door een inlichtingenagent aan een derde'); VAST COMITÉ I, *Activiteitenverslag 2012*, 14 e.v. ('II.2. De opvolging van buitenlandse inlichtingendiensten ten aanzien van hun diaspora in België').

18 De wet verwijst alleen naar 'instanties en personen'. Er is geen reden om aan te nemen dat deze regeling, anders dan de eerste zinssnede van artikel 19, eerste lid, W.I&V, beperkt zou zijn tot publieke (rechts)personen.

19 Het gegeven dat het wettelijk kader een werkgever van een openbare dienst toelaat om informatie te verstrekken of vragen te stellen over een van zijn personeelsleden, betekent echter niet dat de inlichtingendiensten de gestelde vraag kunnen of moeten beantwoorden. Het feit dat de inlichtingendienst een vraag niet kan (of wil) beantwoorden, betekent niet dat het onwettig of onrechtmatig is om de vraag te stellen.

20 Deze mededeling/vraag kan voor een inlichtingendienst uiteraard de aanleiding vormen om een inlichtingenonderzoek op te starten. Het al dan niet opstarten van een dergelijk onderzoek alsook de diepgang ervan, staat juridisch gezien los van de vraag of en wat een inlichtingendienst aan een werkgever mag meedelen. Uiteraard is het niet legitiem een (per definitie privacyschendend) onderzoek te starten indien er geen enkele aanwijzing is van een potentiële of concrete dreiging tegen fundamentele staatsbelangen.

Ingevolge artikel 20 §3 W.I&V dient de Nationale Veiligheidsraad (NVR) in een richtlijn de voorwaarden te bepalen waaronder inlichtingen kunnen worden meegedeeld aan private of publieke instanties of personen. Voor zover het Comité kon nagaan, werd nog niet voldaan aan deze verplichting wat betreft de situatie van personen en instanties die het voorwerp zijn van een dreiging.[21] Het Comité onderlijnde met klem zijn aanbeveling opdat de NVR een dergelijke allesomvattende richtlijn zou uitvaardigen dewelke een houvast biedt aan de inlichtingendiensten in deze delicate materie, waarbij het al dan niet doorgeven van informatie ernstige gevolgen kan hebben voor het algemene én private belangen.

Het belang van een dergelijke richtlijn is in de ogen van het Comité eens zo belangrijk nu kon worden vastgesteld dat op het niveau van de inlichtingendiensten zelf, hieromtrent geen nadere regeling werd uitgewerkt. Wat betreft de VSSE kan niettemin verwezen worden naar twee richtlijnen. Vooreerst is er de als vertrouwelijk geclassificeerde instructie van 10 oktober 2016 die handelt over de wijze waarop dient gereageerd te worden in geval van een vraag vanuit een publieke overheid om verificatie van een bepaalde persoon. Het Comité kon evenwel vaststellen dat deze richtlijn niet verduidelijkt op basis van welke wettelijke regeling bepaalde antwoorden moeten worden verschaft. De richtlijn lijkt niet van toepassing op de situatie voorzien in de laatste zinsnede van artikel 19, eerste lid, W.I&V. Alleszins regelt zij niet de verhouding met private actoren. Het Comité plaatst overigens vraagtekens bij de wettelijkheid van sommige passages van deze richtlijn, omdat ze schijnbaar ingaan tegen de wettelijke regeling inzake veiligheidsscreenings. Daarnaast stelde de VSSE in 2018 ook een vertrouwelijk geclassificeerde richtlijn op over disruptief optreden of verstoren.[22] Alhoewel het meedelen van informatie aan een persoon of instantie die het voorwerp is van een dreiging, perfect onder die definitie te brengen is, wordt in die richtlijn nergens verwezen naar artikel 19 W.I&V, noch naar enige andere wettelijke bepaling.

I.3.3.3. Limieten gesteld door de Inlichtingenwet

In welke gevallen en binnen welke limieten mag nu toepassing worden gemaakt van de mogelijkheid voor een inlichtingendienst om een (publieke of private) derde op de hoogte te brengen van inlichtingen waarover ze beschikt?

De dreigingen die bedoeld worden in artikel 19 W.I&V zijn wat betreft de VSSE, elke activiteit van spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties, criminele organisaties die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het

21 Het Comité had in het kader van een onderzoek m.b.t. de strijd tegen terrorisme en extremisme reeds aangedrongen op zo'n richtlijn (VAST COMITÉ I, *Activiteitenverslag 2012*, 92).

22 Dit is het dermate hinderen van dreigingen opdat deze niet langer plaatsvinden of dat de schadelijkheid ervan aanzienlijk wordt teruggebracht.

wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land in het gedrang kan brengen (art. 7 W.I&V). Er moet dus niet alleen een bepaalde activiteit zijn van de werknemer (bijv. extremisme), deze moet ook een gevaar inhouden voor een of meerdere fundamentele staatsbelangen. En in de context van artikel 19 W.I&V moet die private of publieke instantie ook het voorwerp zijn van de dreiging. Een werkgever mag dus niet geïnformeerd worden over bijv. de extremistische activiteiten van zijn werknemer, indien die werkgever op geen enkele wijze zelf het voorwerp is van een dreiging.

Het weze ook duidelijk dat er geen toepassing mag gemaakt worden van artikel 19 W.I&V wanneer er op geen enkele wijze fundamentele staatsbelangen op het spel staan zoals bijv. imagoschade voor een privébedrijf (tenzij dit bijv. het verlies van het vertrouwen in bepaalde instellingen betekent), een slechte werksfeer of een financieel verlies (tenzij deze financiële belangen de individuele belangen van de onderneming overstijgen en als fundamenteel voor het land kunnen aanzien worden).

De dreigingen die voor de ADIV een aanleiding kunnen zijn om publieke of private instanties of personen te verwittigen, moeten gevonden worden in artikel 11 W.I&V. Het betreft bijvoorbeeld elke activiteit die een bedreiging betekent voor de onschendbaarheid van het nationaal grondgebied of de bevolking, de militaire defensieplannen, het wetenschappelijk en economisch potentieel met betrekking tot bepaalde bedrijvenactief in defensie-gerelateerde sectoren, de vervulling van de opdrachten van de strijdkrachten, de veiligheid van de Belgische onderdanen in het buitenland, de militaire veiligheid van het personeel dat onder de minister van Defensie ressorteert…

Aangezien de mededeling van gegevens op basis de laatste zinsnede van artikel 19, eerste lid, W.I&V een duidelijke finaliteit heeft (vrijwaren van fundamentele staatsbelangen tegen bepaalde activiteiten waarvan de betrokken instantie of persoon het voorwerp is), moet de mededeling van (persoons)gegevens ook beperkt zijn tot die informatie die bijdraagt tot het opvolgen of – indien nodig - neutraliseren van de dreiging.

De eerste verplichting van een inlichtingendienst die wordt geconfronteerd met een verzoek om informatie is dan ook na te gaan om welk probleem, welk incident, welke dreiging het zou kunnen gaan. In dit verband zou de inlichtingendienst zijn databanken kunnen raadplegen om de aan hem meegedeelde naam of namen te verifiëren.[23] Het lijkt ook voor de hand te liggen dat de inlichtingendienst contact opneemt met de werkgever om het verzoek in de juiste context te plaatsen. Daartoe zal met name moeten worden nagegaan waarom de werkgever wil weten of zijn werknemer bekend is bij de inlichtingendiensten, wat het probleem en de

[23] Dit is ook wat de richtlijn van de VSSE van 10 oktober 2016 voorschrijft bij een vraag van een publieke overheid om een persoon te verifiëren.

dreiging is, of er een veiligheids- of ander incident is geweest, of er sprake is van een noodsituatie…

Indien die gegevens geen uitsluitsel geven in de ene of de andere richting, kan verder onderzoek door de dienst aangewezen zijn. De reikwijdte van dit onderzoek kan niet *in abstracto* worden bepaald. Dit zal afhangen van de aard van de bedreiging en van de informatie die in de loop van het onderzoek naar voren komt. Bij dergelijk onderzoek zal de dienst alleszins rekening moeten houden met de proportionaliteits- en subsidiairiteitsprincipes.

De antwoorden op deze vragen en de resultaten van het bijkomende onderzoek moeten de inlichtingendienst toelaten te beoordelen of ze in deze bevoegd is en desgevallend toepassing kan maken van artikel 19 W.I&V en wat ze, gelet op de dreiging, al dan niet kan meedelen aan de werkgever.

I.3.3.4. Wat mag of moet worden meegedeeld?

In wat volgt, wordt er van uit gegaan dat er effectief sprake is van een dreiging. De vraag stelt zich vervolgens wat op welke wijze kan meegedeeld worden.[24]

I.3.3.4.1. Het proportionaliteits- en subsidiariteitsbeginsel

Gelet op de eisen van de proportionaliteit en de subsidiariteit moet de eerste vraag zijn of de werkgever *überhaupt* in kennis mag gesteld worden. Indien de dreiging zeer vaag en weinig ernstig is, of indien de dienst de evaluatie van de dreiging zelf kan opvolgen of de dreiging kan counteren op een andere wijze (bijv. door de werknemer zelf aan te spreken zodat die zich realiseert dat hij wordt opgevolgd), dan is een mededeling van persoonsgegevens aan een werkgever mogelijk disproportioneel en niet subsidiair.

Indien dit niet volstaat en de dreiging is voldoende ernstig, dan dient de mogelijkheid zich aan om de werkgever in kennis te stellen. Ook hier moet worden afgewogen hoeveel en welke informatie wordt gegeven. De regel hierbij is opnieuw dat er, gegeven de aard en de ernst van de dreiging en nood en de mogelijkheden om deze te counteren, gestreefd wordt naar een de minimale inmenging in het privéleven.

---

[24] Eerst wordt kort de hypothese aangehaald waarbij de inlichtingendienst in hoofde van de werknemer (eventueel na een eerste bevraging of na een grondiger inlichtingenonderzoek) *geen enkele* dreiging in de zin van de Inlichtingenwet vaststelt. Op dat ogenblik maakt de werkgever per definitie niet het voorwerp uit van een dreiging en kan strikt genomen geen toepassing gemaakt worden van artikel 19 W.I&V. Het Comité is echter van oordeel dat in deze gevallen aan de inlichtingendienst de mogelijkheid moet gelaten worden om de werkgever mee te delen dat er geen sprake is van een dreiging in de zin van de Inlichtingenwet (hetgeen uiteraard niet betekent dat er geen andersoortige dreiging kan zijn voor de werkgever). Het Comité oordeelde reeds in die zin in in een eerder onderzoek VAST COMITÉ I, *Activiteitenverslag 2015*, 41 e.v. ('II.9. Klacht over het verstrekken van persoonlijke informatie door een inlichtingenagent aan een derde').

Indien de dreiging echter dermate ernstig is dat deze alleen door een tussenkomst van de werkgever kan gecounterd worden, kan méér en concretere informatie worden meegedeeld die bijvoorbeeld kan dienen om een administratieve of private beslissing (bijv. disciplinaire sanctie, overplaatsing, ontslag…), te onderbouwen. Het weze duidelijk dat het uiteindelijke doel van de inlichtingendienst hier het neutraliseren of verkleinen van een dreiging moet zijn.

Aansluitend bij de vraag naar een proportionele informatieverstrekking, rijst de vraag of een inlichtingendienst in zijn mededeling zelf een oplossing mag suggereren aan de bedreigde publieke of private instantie of – sterker nog – mag deelnemen aan de besluitvorming over het handelen door de bedreigde instantie of persoon. Bedoeld wordt bijvoorbeeld de suggestie om iemand te ontslaan. Het Comité was van oordeel dat dit niet onwettelijk is in de mate waarin de gesuggereerde oplossing zelf wettelijk en proportioneel is.

Tot slot stelde zich de vraag of uit artikel 19 W.I&V een *verplichting* blijkt om te antwoorden op een vraag of om *op eigen initiatief* gegevens te verstrekken. De bepaling stelt dat de inlichtingen- en veiligheidsdiensten hun inlichtingen *'slechts meedelen'* aan instanties en personen die het voorwerp zijn van een dreiging. Alhoewel de bepaling op dit vlak niet erg duidelijk is, was het Comité van oordeel dat een inlichtingendienst verplicht is om gegevens mee te delen indien alleen hierdoor de realisatie van een ernstige dreiging tegen fundamentele staatsbelangen kan voorkomen worden. In de andere gevallen bepaalt zij autonoom wat de beste strategie vormt, gegeven de dreiging. Het Comité beveelde aan dat deze onduidelijkheid wordt opgehelderd ofwel door een wetgevend initiatief ofwel door een regeling ter zake in de verplicht op te stellen richtlijn van de Nationale Veiligheidsraad.

Hierbij aansluitend suggereerde het Comité om te onderzoeken of het nuttig zou zijn om een verplichte melding naar de werkgever in het leven te roepen ten aanzien van iedere (kandidaat-)werknemer die is opgenomen in een Gemeenschappelijke gegevensbank *terrorist fighters* of haatpredikers.

I.3.3.4.2. Andere aandachtspunten: zorgvuldigheid, classificatie en schriftelijke mededeling van informatie

In een inlichtingencontext bestaan er weinig zekerheden, en dit gegeven moet mee de beslissing bepalen om en hoe een werkgever te informeren. Om over een rechtmatige informatievertrekking te kunnen spreken, moet de mededeling voldoende onderbouwd zijn door betrouwbare inlichtingen. Ze dient daarenboven zorgvuldig verwoord te zijn.[25]

[25] Er mag bijvoorbeeld geen ongenuanceerd beeld wordt gegeven van de onderliggende inlichtingen, of een bepaald element mag niet als 'vaststaand' worden voorgesteld indien het om 'een visie over' of 'een aanvoelen van' gaat. De meegedeelde informatie moet in die zin ook 'eerlijk' zijn door een objectief beeld te bieden van de wijze waarop de inlichtingendienst de dreiging en de rol van de betrokkene daarin ziet, zonder 'manipulatief' te zijn in die zin dat ze de besluitvorming van private of publieke werkgever wil sturen.

Daarnaast beschikt niet elke private en publieke instantie over een veiligheidsmachtiging. Dit betekent dat geclassificeerde informatie zal moeten gedeclassificeerd worden. Dit geldt des te meer indien de informatie moet dienen om een beslissing van de werkgever te schragen.

Tot slot bepaalt artikel 19 W.I&V niet op welke wijze een bedreigde instantie in kennis moet worden gesteld. Het Comité is van oordeel dat dit om redenen van rechtszekerheid, behoudens hoogdringendheid, schriftelijk dient te gebeuren. Dit om discussies achteraf te vermijden en een parlementaire of zelfs jurisdictionele controle toe te laten.

I.3.4. CONCLUSIES

Voor de informatieverstrekking door de inlichtingendiensten aan een private of publieke werkgever gelden – terecht – strenge regels, omdat de mededeling grote gevolgen kan hebben voor de betrokken personen. Minimaal betekent dit een inbreuk op de privacy en in het uiterste geval kan het de basis vormen voor ingrijpende maatregelen die de betrokkenen in hun rechtspositie kunnen aantasten.

Indien de VSSE en de ADIV op eigen initiatief of op verzoek informatie verstrekken aan een publieke of private werkgever (en het loutere meedelen of een persoon 'gekend' is of niet valt daar ook onder), moet aan alle wettelijke vereisten voldaan zijn, te weten:

1. er moet een specifieke wettelijke grondslag zijn;
2. de dienst moet zorgvuldig tewerk gaan bij de interne totstandkoming van de te verstrekken gegevens en in de communicatie daarover naar de ontvanger;
3. de mededeling moet beantwoorden aan de eisen van de noodzakelijkheid; en
4. de mededeling moet proportionaliteit zijn.

Wat betreft de wettelijke basis, benadrukte het Comité dat het buiten de twee besproken situaties (m.n. de werkgever wil een veiligheidsscreening of de werkgever is voorwerp van dreiging) niet toegelaten is om informatie te verschaffen over een werknemer aan een publieke of private werkgever. Vanuit het oogpunt van de inlichtingenagent is dergelijke mededeling afhankelijk van de concrete situatie mogelijks zelfs strafbaar.

Het Comité beklemtoonde tevens dat niets een werkgever uit de overheids- of de privésector belet om informatie mee te delen aan of vragen te stellen aan een Belgische inlichtingendienst over een mogelijke bedreiging in de zin van de Wet van 30 november 1998 waarvan een van zijn personeelsleden de 'oorzaak' zou zijn.

Het Comité nodigde spelers uit de publieke en private sector wel uit om te onderzoeken of bepaalde potentiële dreigingen niet preventief kunnen ondervangen worden door voor bepaalde functies, toelatingen of vergunningen een beroep te doen op het systeem van de veiligheidsscreenings uit de Classificatiewet. Het Co-

mité benadrukte wel dat dit systeem oordeelkundig moet gebruikt worden en niet mag leiden tot een ongebreidelde toepassing.

Het Comité was van oordeel dat de VSSE en de ADIV binnen zes maanden na het afsluiten van deze studie een voorstel tot richtlijn ter uitvoering van de laatste zinsnede van artikel 19, eerste lid, moesten opstellen ten behoeve van respectievelijk de minister van Justitie en van Defensie met het verzoek het voorstel ter goedkeuring voor te leggen aan de Nationale Veiligheidsraad.

I.4. ERNSTIGE TEKORTKOMINGEN AANGAANDE DE NATIONALE VEILIGHEID

Begin juli 2020 richtte de voorzitter van het Vast Comité I een geclassificeerd schrijven aan de (toenmalige) minister van Buitenlandse Zaken en Defensie, onder meer bevoegd voor de Nationale Veiligheidsoverheid (NVO) en de Algemene Dienst Inlichting en Veiligheid (ADIV). In zijn hoedanigheid van voorzitter van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen[26] werden immers ernstige tekortkomingen aangaande de nationale veiligheid vastgesteld.

De rechtstreekse aanleiding vormde een dossier aangaande de verlenging in januari 2020 van een veiligheidsadvies; de werkneemster in kwestie had in 2015 al een positief veiligheidsadvies gekregen. Dit gaf haar toegangsrecht tot zones op de luchthaven van Brussel-Nationaal dewelke omwille van veiligheidsredenen slechts beperkt toegankelijk zijn. Uit een geclassificeerd rapport bleek evenwel dat haar partner een van de vermeende co-auteurs was van de aanslagen in Parijs en Brussel. Zij onderhield regelmatig contacten met hem tijdens gevangenisbezoek in een ruimte zonder bewaking.

Ondanks het onmiskenbare veiligheidsrisico, werd het besluit om het advies of de machtiging van betrokkene in te trekken, pas genomen op het moment dat er een verzoek tot verlenging werd ingediend.[27]

Het Vast Comité I interpelleerde de Regering en onderstreepte dat hiermee het dysfunctioneren van de administraties en openbare overheden werd aangetoond, waarbij het 'vakjesdenken' verhindert om de veiligheid van de burger te kunnen garanderen. Het Comité wees de Regering ook op de recurrentie van dit probleem,

---

26 Het Beroepsorgaan is het administratief rechtscollege dat bevoegd is om kennis te nemen van beroepen inzake veiligheidsmachtigingen, -attesten en -adviezen in het kader van de Wet van 11 december 1998. De voorzitter van het Beroepsorgaan is tevens de voorzitter van het Vast Comité I. Hierover: Hoofdstuk X. Het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen.

27 Ook het toezichtonderzoek naar de wijze waarop de inlichtingendiensten veiligheidsscreenings uitvoerden, besteedde bijzondere aandacht aan deze problematiek. Hierover VAST COMITÉ I, *Activiteitenverslag 2019*, 2-14 ('I.1. De uitvoering van veiligheidsscreenings door de inlichtingendiensten').

dat al werd onderstreept tijdens de werkzaamheden van de Parlementaire Onderzoekscommissie naar de 'terroristische aanslagen' van 22 maart 2016.[28]

Tussen juli 2020 en februari 2021 volgde een uitvoerige briefwisseling tussen het Vast Comité I, de (toenmalige) minister van Buitenlandse Zaken en Defensie, de voorzitter van de Nationale Veiligheidsoverheid en de voorzitter van het College van Procureurs-generaal. Er werd onder meer gevraagd een werkgroep op te richten om de vastgestelde dysfuncties te onderzoeken.

Het Vast Comité I diende vast te stellen dat weinig gehoor werd gegeven bij het aankaarten van de problemen aangaande de nationale veiligheid.[29] Gezien het daarmee aan het einde van zijn prerogatieven kwam, werd de situatie voor nuttig gevolg toevertrouwd aan de Kamer van volksvertegenwoordigers. De nuttige opmerkingen vanuit het Vast Comité I zouden zijn meegenomen in de werkzaamheden van verschillende werkgroepen die binnen de Nationale Veiligheidsoverheid werden opgericht. Daarin is er onder meer aandacht voor een structurele hervorming van de NVO.

I.5. DE OPVOLGING VAN SCHADELIJKE SEKTARISCHE ORGANISATIES EN CRIMINELE ORGANISATIES

Op vraag van de Begeleidingscommissie van de Kamer van volksvertegenwoordigers opende het Vast Comité I een toezichtonderzoek naar de wijze waarop de Veiligheid van de Staat (VSSE) twee van haar wettelijke opdrachten uitvoerde, i.e. de opvolging van schadelijke sektarische organisaties[30] en deze van criminele

---

28 BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS, *Onderzoekscommissie terroristische aanslagen 22 maart 2016. Beknopt overzicht van de werkzaamheden en aanbevelingen*, 2018.

29 De thematiek vormde het voorwerp van parlementaire vragen (cf. Vraag van C. Thibaut aan de minister van Buitenlandse Zaken over het 'uitblijven van antwoorden van de NVO aan het Comité I inzake veiligheidsmachtigingen' (*Vr. en Ant*. Kamer 2020-21, 15 juli 2021, QRVA59, 108, Vr. nr. 342)) en persartikelen (bijv. L. BOVÉ, *De Tijd*, 6 mei 2021 ('Kamer slaat alarm over veiligheidsscreenings').

30 In een streven naar objectiviteit wordt onder 'sekte', 'schadelijke sektarische organisatie' of 'schadelijke sektarische groep' verstaan 'elke groepering met een levensbeschouwelijk of godsdienstig doel, of die zich als dusdanig voordoet die als schadelijk wordt beschouwd en zo het voorwerp kan uitmaken van welke belangstelling ook vanwege de Veiligheid van de Staat (VSSE)'.

organisaties. In het verleden boog het Vast Comité I zich al eerder over verschillende aspecten van deze problematiek.[31]

I.5.1. CONTEXTUALISERING

I.5.1.1. De schadelijke sektarische organisaties

Gedurende lange tijd hebben de Belgische autoriteiten blijk gegeven van bijzondere terughoudendheid ten aanzien van bewegingen die werden geacht sektair te zijn. Die houding werd ingegeven door de moeilijkheid om een standpunt in te nemen op een domein dat raakte aan de fundamentele vrijheden van godsdienst, denken, meningsuiting en vereniging.

In de loop van de jaren 1980 brachten meerdere tragische en sterk gemediatiseerde gebeurtenissen dit fenomeen onder de aandacht van zowel de bevolking als van de autoriteiten, wat leidde tot heel wat initiatieven in België in de loop van de jaren 1990. Zo werd in 1996 een parlementaire onderzoekscommissie 'sekten' opgericht.[32] Een Informatie- en adviescentrum inzake de schadelijke sektarische organisaties (IACSSO) en een Administratieve coördinatiecel (ACC) werden bij Wet van 2 juni 1998 opgericht.[33] Een koninklijk besluit[34] kende het secretariaat van de ACC toe aan de Veiligheid van de Staat.

---

31 Wat betreft de schadelijke sektarische organisaties: VAST COMITÉ I, *Activiteitenverslag 1996*, pp. 88-100 ('Hoofdstuk 2. Toezichtsonderzoek inzake de doeltreffendheid van de inlichtingendiensten met betrekking tot de activiteit van sekten in België'); *Activiteitenverslag 2006*, pp. 63-65 ('II.6.2. Schadelijke sektarische organisaties en de bevoegdheid van de Veiligheid van de Staat'); *Activiteitenverslag 2007*, p. 41-42 ('II.10.9. Schadelijke sektarische organisaties'); *Activiteitenverslag 2010*, pp. 13-24 ('II.2. De opvolging van schadelijke sektarische organisaties') en *Activiteitenverslag 2014*, pp. 51-54 ('II.5. Een klacht van de Scientologykerk tegen de Veiligheid van de Staat').
Wat betreft criminele organisaties: VAST COMITÉ I, *Activiteitenverslag 2002*, 19-20 ('Hoofdstuk II.2.6. Toezichtonderzoek over de inlichtingen waarover de Veiligheid van de Staat beschikt inzake een affaire van visumfraude'); *Activiteitenverslag 2004*, 13-18 ('IV.2.2. Onderzoek naar de wijze waarop de Belgische inlichtingendiensten functioneren en samenwerken in het kader van hun nieuwe wettelijke opdracht betreffende de dreigingen van criminele organisaties').

32 *Parl. St.*, Kamer, 1995-1996, nr. 313/008.

33 Wet van 2 juni 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 (*BS* 25 november 1998). Deze wet voorziet in actieve samenwerking tussen het IACSSO, de ACC en de andere openbare diensten die betrokken zijn bij deze strijd, zoals het Federaal Parket, de parketten-generaal, de parketten van aanleg, de politie, de Veiligheid van de Staat en de plaatselijke overheden.

34 Koninklijk besluit tot wijziging van het koninklijk besluit van 8 november 1998 houdende samenstelling, werking en organisatie van de Administratieve Coördinatiecel inzake de strijd tegen schadelijke sektarische organisaties (*BS* 9 december 1998).

I.5.1.2. Criminele organisaties

In 2019 werden in het kader van een studie bij de Federale Gerechtelijke Politie meer dan 600 criminele organisaties, verenigingen van misdadigers of groepen van daders in België geteld.[35]

In haar verslag van 2020[36] meldt de Cel voor Financiële Informatieverwerking (CFI) op haar beurt dat ze in 2020 31.605 meldingen had ontvangen. De cel verklaarde ook dat nog in 2020 1.228 nieuwe dossiers werden overgemaakt aan de gerechtelijke autoriteiten en dat informatie uit 2.765 meldingen werd doorgezonden naar en gebruikt door de parketten en het federaal parket, goed voor een totaalbedrag van 1.885,31 miljoen euro. Het rapport preciseert verder dat "*in 2020 de CFI opvallend veel doormeldingen heeft verricht waarbij er sprake is van georganiseerde misdaad*".[37]

I.5.2. DE MATERIËLE BEVOEGDHEID

De taakstelling van de VSSE binnen de opvolging van schadelijke sekten en criminele organisaties situeert zich binnen haar inlichtingenopdracht. Krachtens artikel 7, 1° W.I&V wordt deze omschreven als '*het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen*'.

De wetgever heeft hierbij geopteerd om een limitatieve lijst op te stellen van veiligheidsdreigingen die behoren tot het bevoegdheidsdomein van de VSSE (m.n. terrorisme, extremisme, spionage, inmenging, proliferatie, schadelijke sektarische organisaties en criminele organisaties).

De *'schadelijke sektarische organisaties'* worden daarbij omschreven als '*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*' (art. 8, 1°, tweede lid, e W.I&V).

Ook *'criminele organisaties'* werden door de wetgever omschreven als een nationale veiligheidsdreiging die onder de interessesfeer van de VSSE dient te vallen. Dit

---

35 Federale Politie, 'Diagnose - Eerste benadering van criminele organisaties', april 2020, p. 4. De FGP benadrukt dat "*de problematiek van terrorisme of de financiering ervan 20 keer wordt vermeld*".

36 https://www.ctif-cfi.be/images/documents/Dutch/Jaarverslagen/2020.pdf, 10.

37 https://www.ctif-cfi.be/images/documents/Dutch/Jaarverslagen/2020.pdf, 22.

begrip wordt in de Inlichtingenwet omschreven als *'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.'* (art. 8, 1°, tweede lid, f W.I&V).

Vandaar dat de VSSE slechts bevoegd is voor de opvolging van criminele organisaties indien de criminele organisaties *'wezenlijk betrekking hebben op de activiteiten bedoeld in artikel 8, 1°, a) tot e) en g)'*- zijnde de activiteiten inzake terrorisme, extremisme, spionage, inmenging, proliferatie en schadelijke sekten – *'of die destabiliserende gevolgen kunnen hebben op het politieke of sociaal-economische vlak'*.

Niet alle schadelijke sektarische en criminele organisaties behoren zodoende tot de wettelijke interessesfeer van de VSSE. Daarnaast schrijft de Inlichtingenwet voor dat deze pas tot de bevoegdheid van de VSSE behoren, wanneer de activiteiten ervan een dreiging kunnen betekenen voor de inwendige of uitwendige veiligheid van de Staat en/of voor het wetenschappelijk of economisch potentieel van het land.

Wat betreft de opvolging van schadelijke sektarische organisaties, verklaarde het Comité in 2015 wat volgt: "*Er dient te worden onderstreept 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.*[38] *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).

I.5.3. DE PROCEDURELE BEVOEGDHEID

De procedurele bevoegdheid binnen de inlichtingenopdracht laat zich, in eerste instantie, bepalen door de in artikel 7, 1° W.I&V opgesomde activiteiten: *'het inwinnen, analyseren en verwerken van inlichtingen'*. Hieruit blijkt dat de VSSE schadelijke sekten en criminele organisaties gaat bestrijden via informatiegaring en inlichtingenanalyse en het vervolgens doorgeven van de bekomen inlichtingen (m.n. de verrijkte informatie) aan andere instanties (bijv. politionele of gerechtelij-

[38] Waaraan de VSSE toevoegt (14 april 2021): "*et le service, au surplus, se trouve privée d'échanges fructueux en la matière avec ses correspondents étrangers*" (en de dienst bovendien verstoken blijft van vruchtbare uitwisselingen op dit gebied met zijn buitenlandse correspondenten (vrije vertaling).

ke overheden). Laatstgenoemden nemen uiteindelijk de nodige tegenmaatregelen ter bescherming van de nationale veiligheid.

Om deze opdrachten uit te voeren, zette de VSSE, op het hoogtepunt van haar activiteiten in deze materies, volgend personeel in:

- Schadelijke sektarische organisaties (1999-2000): zes medewerkers in de 'Sectie Analyse' (waarvan drie niveau A) en negen medewerkers in de 'Operationele sectie';
- Criminele organisaties (jaren 2000): twee medewerkers in de 'Sectie Analyse' en twee medewerkers in de 'Operationele sectie'.

I.5.4. DE BELEIDSPRIORITEITEN

Artikel 7, 1° W.I&V vestigt een wettelijke verplichting tot handelen in hoofde van de VSSE. Dit wil evenwel niet zeggen dat er geen prioriteiten gelegd kunnen worden binnen de werkzaamheden van de VSSE. De dienst heeft immers onvoldoende capaciteit en middelen ter beschikking om alle tot zijn bevoegdheid behorende nationale veiligheidsdreigingen te detecteren, op te volgen en te beheersen (noch zou ze deze ooit kunnen hebben). Het leggen van prioriteiten is daarom een noodzaak, zelfs een plicht.

Een dergelijke lezing wordt bevestigd in diverse wettelijke en reglementaire bepalingen. Vooreerst bepaalt artikel 4 W.I&V dat de VSSE haar opdrachten verricht door tussenkomst van de minister van Justitie, doch *'overeenkomstig de richtlijnen van de Nationale Veiligheidsraad'*.

De opdracht van de Nationale Veiligheidsraad (NVR) is vastgelegd in artikel 3 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'. Deze stelt dat de NVR, *'(a)ls coördinerend beleidsorgaan'*, *'belast (is) met (…) de bepaling van de prioriteiten van de inlichtingen- en veiligheidsdiensten'*.

In juli 2015 heeft diezelfde Nationale Veiligheidsraad beslist dat de VSSE de schadelijke sektarische organisaties en criminele organisaties niet langer actief (onze onderlijning) opvolgt. Aangezien België het hoofd diende te bieden aan een golf van binnen- en buitenlandse aanslagen of pogingen daartoe, beslisten de ministers van Justitie en Defensie om de prioriteit van de opdrachten te herdefiniëren en aanpassingen door te voeren wat betreft de inzet van personeel en materiële middelen van de inlichtingendiensten.

Op 25 augustus 2015 verklaarde toenmalig minister van Justitie wat volgt: "*De Staatsveiligheid reorganiseert vanaf 1 september haar buitendienst met een ongeziene focus op het radicalisme en het terrorisme*." In verband hiermee liet de Veiligheid van de Staat ook nog weten: "*De Nationale Veiligheidsraad heeft het Actieplan 2015 van de Veiligheid van de Staat goedgekeurd. Op basis van dit plan heeft de directie*

van de Veiligheid van de Staat beslissingen genomen met betrekking tot haar organisatie" (vrije vertaling), en ook nog: "*Gevolg van deze nieuwe focus: andere bedreigingen zoals sekten en bedrijfsspionage worden op de achtergrond geplaatst"* (vrije vertaling).[39]

Dit werd in 2020 ook zo bevestigd door de VSSE, waarbij gesteld werd dat "*le suivi actif des organisations sectaires nuisibles a été mis en suspens, sauf au cas où une menace d'ingérence, d'espionnage, de prolifération, d'extrémisme ou de terrorisme y serait liée.*" Eenzelfde vaststelling geldt voor de opvolging van de criminele organisaties.

Tot slot bepaalt artikel 2 van het koninklijk besluit van 5 december 2006 betreffende het algemeen bestuur en de ondersteuningscel van de Veiligheid van de Staat dat de directie-generaal van de VSSE (m.n. de administrateur-generaal en de adjunct-administrateur-generaal) *'verantwoordelijk (zijn) voor de uitwerking en de uitvoering van een vierjaarlijks strategisch plan dat de prioriteiten bepaalt van de Veiligheid van de Staat en de operationele strategieën om deze prioriteiten uit te voeren*'. Artikel 3 schrijft voor dat de VSSE jaarlijks een actieplan dient voor te leggen aan de minister van Justitie en dit ter realisatie van het strategisch plan. Dit actieplan bevat, onder meer, de strategische doelstellingen en de middelen om deze te verwezenlijken. Uit deze plannen moet blijken dat sinds de aanslagen in Verviers (januari 2015), Parijs (november 2015) en Brussel (maart 2016) terrorisme en (islamitisch-, rechts- en links)extremisme, samen met spionage, de drie grote speerpunten vormen in het beleid van de VSSE en als dusdanig als belangrijkste dreigingen worden beschouwd. Zowel schadelijke sektarische organisaties als criminele organisaties komen niet voor in de prioriteitenlijst.

I.5.5. DE TOEGELATEN BELEIDSRUIMTE

Bij het vastleggen van beleidsprioriteiten worden de Nationale Veiligheidsraad en de minister van Justitie juridisch begrensd. Prioriteiten moeten zich vooreerst situeren binnen het door de wetgever vastgelegde bevoegdheidsdomein, zijnde binnen de te beschermen belangen en de bestrijden veiligheidsdreigingen.

Daarnaast zijn noch de Nationale Veiligheidsraad, noch de minister van Justitie, noch de VSSE bevoegd om een veiligheidsdreiging in zijn geheel, voor alle soorten inlichtingenactiviteiten en ten alle tijde, als niet op te volgen te kwalificeren. Een dergelijke maatregel komt neer op een door de uitvoerende macht gedane schorsing van artikel 7, 1° *i.o.* artikel 8, 1° W.I&V. Het leggen van prioriteiten binnen de inlichtingenopdrachten van de VSSE heeft betrekking op het bepalen van

[39] De minister van Justitie zal in 2016 deze beleidskeuze nog bevestigen in antwoord op een parlementaire vraag en verduidelijkt dat e*en ontwerp van KB tot wijziging wordt opgesteld en tot doel heeft de Veiligheid van de Staat te ontlasten van deze taak* (het secretariaat van de ACC, onze toevoeging) *en het toe te vertrouwen aan het secretariaat van het IACSSO.*

de aangelegenheden waarbij actief door de inlichtingendienst een informatiepositie dient opgebouwd te worden. Het betekent geenszins dat, indien de VSSE passief informatie van een derde verkrijgt waarin concrete aanwijzingen (*leads*) besloten liggen van mogelijke problematische activiteiten[40], de VSSE geen plicht zou hebben om deze aanwijzingen nader te beoordelen en desgevallend actief te onderzoeken. De VSSE heeft weliswaar de bevoegdheid om een opportuniteitsoordeel te nemen binnen haar onderzoeken, maar heeft eveneens een onderzoeksplicht t.a.v. de door de wetgever opgesomde veiligheidsdreigingen. Het zorgvuldigheidsbeginsel indachtig zal de beoordeling van *leads*, en de daaropvolgende beslissing om een *lead* al dan niet verder actief te onderzoeken, dienen te gebeuren a.d.h.v. vooraf bepaalde objectieve criteria. Het wettigheidsbeginsel indachtig, mogen dergelijke criteria er niet toe leiden dat in de praktijk een wettelijk bepaalde veiligheidsdreiging nooit verder wordt onderzocht.

I.5.6. DE ORGANISATORISCHE VERTALING VAN DE BELEIDSPRIORITEITEN

Aanvullend moet de vraag gesteld worden op welke wijze deze juridisch begrensde beleidsruimte gevolgen heeft voor de organisatorische vertaling van de beleidsprioriteiten? Anders gesteld: wat kan en wat kan niet binnen de creatie en de opheffing van diensten en secties? En dient er een gereserveerde capaciteit te worden voorzien?

De minister van Justitie (*cf*. art. 5, §3 W.I&V) en, in subsidiaire orde, de directie-generaal van de VSSE (*cf*. art. 2 KB 5 december 2006) zijn binnen de door de wetgever en de Koning bepaalde regels verantwoordelijk voor het bepalen van de organisatiestructuur van de VSSE.[41]

Binnen dit wetgevend en reglementair kader behoort het tot de discretionaire bevoegdheid van de uitvoerende macht om al dan niet een (analyse)dienst of (operationele) sectie voor een bepaalde veiligheidsdreiging in te richten. De in de VSSE gedane opheffing van de analysedienst Sekten en, eerder, van de operationele sectie Sekten, behoort dan ook tot de autonomie van vernoemde beleidsverantwoordelijken.

Wel dient de VSSE zich op een manier te organiseren dat ze kan voldoen aan de wettelijke plicht tot handelen wanneer ze passief informatie verkrijgt van een derde waarin concrete aanwijzingen besloten liggen van mogelijke problematische

---

40 Van bijv. schadelijke sektarische organisaties of criminele organisaties zoals wettelijk omschreven.

41 Op regeringsniveau werd in het Koninklijk besluit van 5 december 2006 (*supra*) bepaald dat de VSSE bestaat uit een directie Operaties, een directie Analyse en een Stafdirectie. Op wetgevend niveau werd bijvoorbeeld in de Classificatiewet bepaald dat de VSSE dient te beschikken over een veiligheidsofficier. In de Gegevensbeschermingswet werd dan weer vastgelegd dat de dienst een functionaris voor gegevensbescherming dient te hebben.

activiteiten van schadelijke sekten of van criminele organisaties. Er kan voorzien worden in een gereserveerde capaciteit (bijv. x aantal analisten én x aantal collecte-agenten) die verantwoordelijk zijn om dergelijk passief verkregen informatie te onderzoeken en om desgevallend bijkomende informatie erbij in te winnen.[42] Dergelijke VSSE-agenten kunnen nog belast zijn met andere door de VSSE-leiding bepaalde taken, doch oefenen een eerstelijnsrol uit wanneer problematische informatie over sekten of criminele organisaties aan de VSSE werd overgemaakt. Indachtig dat sommige activiteiten van schadelijke sektarische organisaties eveneens gekwalificeerd kunnen worden als extremistische en/of inmengingsactiviteiten, kan desgevallend geopteerd worden om dergelijke gereserveerde capaciteit in te richten bij de voor deze dreigingen bevoegde diensten en secties. Gelet op het transversaal karakter van de dreiging 'criminele organisaties' zou dit tot het additioneel takenpakket van andere diensten en secties kunnen behoren.

I.5.7. NOOD AAN VERSTERKING EN EEN BREDER MAATSCHAPPELIJK DEBAT

In de loop van het onderzoek kon het Vast Comité I vaststellen dat de prioritisering van de opdrachten conform was aan het wettelijk en reglementair kader.

Nadat in 2021 werd vastgesteld dat de VSSE slechts een eerder beperkt aantal openstaande dossiers kon opvolgen – en dat er voor deze administratie onmiskenbaar sprake was van een tekort aan personeel en bijgevolg de verplichting tot het maken van keuzes – herinnerde het Comité opnieuw aan de dringende vraag van de VSSE aangaande een verhoging van haar personeels- en financiële middelen en een nauwkeurige bepaling van haar wettelijke opdrachten.

---

42 Waarbij de VSSE laat optekenen (14 april 2021): *"La Sûreté de l'Etat applique déjà la recommandation de constituer une 'capacité réservée', à la fois opérationnelle et d'analyse, mobilisable le cas échéant pour assurer un traitement adéquat aux informations reçues relatives aux organisations sectaires nuisibles et aux organisations criminelles, au cas où elles intéresseraient la sûreté de l'Etat ou le potentiel scientifique ou économique de la Belgique".* (De Veiligheid van de Staat past reeds de aanbeveling toe om een "gereserveerde capaciteit" op te zetten, zowel operationeel als voor analyse, die indien nodig kan worden gemobiliseerd om een passende behandeling te garanderen van ontvangen informatie met betrekking tot schadelijke sektarische organisaties en criminele organisaties, indien deze van belang zouden zijn voor de veiligheid van de Staat of voor het wetenschappelijk of economisch potentieel van België" (vrije vertaling)

Het Comité stelde dan ook dat een breder maatschappelijk (lees parlementair?[43]) debat over het in de Inlichtingenwet van 1998 voorziene takenpakket van de civiele inlichtingendienst en de hieraan gekoppelde prioriteitenstelling, zich opdringt. En bijgevolg, dat de toekenning van voldoende capaciteiten en middelen om het geheel van bedreigingen voor de nationale veiligheid dat behoort tot het takenpakket van de VSSE, het voorwerp dient uit te maken van een grondige discussie.

I.6. AANDACHT VAN DE BELGISCHE INLICHTINGENDIENSTEN VOOR EEN ADIV-MEDEWERKER EN ZIJN RELATIES MET RUSSISCHE BURGERS[44]

In 2014-2015 stelden de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) een gezamenlijk onderzoek in naar een reserve-officier van de (toenmalige) Directie I (Inlichtingen) van de ADIV.

Betrokkene kwam al in 2008 onder de aandacht van de VSSE na een melding van een buitenlandse partner. In 2012 wordt hij opnieuw vermeld en gesitueerd als een 'perifere doelwit' van een Russische oligarch. Twee jaar later wordt de VSSE zich bewust van zijn hoedanigheid van reserve-officier bij de militaire inlichtingendienst. Er wordt een samenwerking met de ADIV opgestart en elementen in het bezit van beide inlichtingendiensten lijken te wijzen op spionage. In februari 2015 trekt de ADIV zijn veiligheidsmachtiging in. De beslissing wordt door het gevatte Beroepsorgaan bevestigd. Het dossier wordt begin juli 2015 door de VSSE afgesloten. Betrokkene bleek op de hoogte te zijn gebracht van het onderzoek naar zijn persoon.

---

43 De VSSE denkt in dezelfde richting (14 april 2021): "*C'est au Parlement, tant dans sa fonction de législation que de controle du pouvoir exécutif, qu'il appartiendra d'apprécier si (considérant les moyens humains et matériels limités dont elle dispose et la gravité parfois extrême des nombreuses menaces liées à l'extrémisme, au terrorisme, à l'ingérence, à l'espionnage et à la prolifération auxquelles elle est confrontée in concreto) il est opportun ou bien d'exiger de la Sûreté de l'Etat qu'elle assure à nouveau le suivi actif des organisations sectaires nuisibles, ou bien de l'en décharger, ou bien de valider la décision du Conseil nationale de sécurité du 13 juillet 2015 approuvant la mise en suspens du suivi actif des organisations sectaires nuisibles.*" (Het is aan het Parlement om, zowel in zijn wetgevende functie als in zijn controle op de uitvoerende macht, te beoordelen of (gelet op de beperkte personele en materiële middelen waarover het beschikt en de soms extreme ernst van de vele dreigingen in verband met extremisme, terrorisme, inmenging, spionage en proliferatie waarmee het *in concreto* wordt geconfronteerd) het al dan niet passend is de Veiligheid van de Staat of te verplichten de actieve opvolging op schadelijke sektarische organisaties te hervatten, ofwel haar van deze taak te ontheffen, ofwel het besluit van de Nationale Veiligheidsraad van 13 juli 2015 tot goedkeuring van de opschorting van de actieve monitoring van schadelijke sektarische organisaties te bekrachtigen (vrije vertaling)).

44 Het kortstondige onderzoek had tot doel de Begeleidingscommissie te informeren n.a.v. het verzoek om inlichtingen aan het adres van het Vast Comité I van 6 juni 2019 van een lid van de parlementaire Begeleidingscommissie.

Het Vast Comité I kon op basis van de door de ADIV en de VSSE verzamelde en aan het Comité meegedeelde informatie niet besluiten of er al dan niet sprake was van spionage in hoofde van betrokkene. Sinds de uitspraak van het Beroepsorgaan heeft betrokkene Defensie verlaten.

I.7. VEILIGHEIDSSCREENINGS VAN MILITAIREN EN BURGERPERSONEEL BIJ DEFENSIE

Jaarlijks onderzoeken de Veiligheid van de Staat en de Algemene Dienst Inlichtingen en Veiligheid meerdere duizenden personen die een of andere vergunning of toelating willen bekomen of die een bepaalde functie willen bekleden. Met deze onderzoeken willen ze nagaan of de betrokkenen voldoende garanties bieden op het vlak van betrouwbaarheid en veiligheid. Eerder opende het Comité een breder toezichtonderzoek naar de wijze waarop de inlichtingendiensten dergelijke veiligheidsscreenings[45] uitvoeren.[46]

In het verlengde van dit onderzoek kon worden vastgesteld dat bepaalde personeelsleden binnen Defensie bij hun kandidaatstelling, aanwerving of in de loop van hun carrière nooit of slechts éénmalig aan een dergelijke veiligheidsscreening worden/werden onderworpen. Daarop bestudeerde het Vast Comité I de screening van militairen en burgerpersoneel bij Defensie (I.7.1), alsook de screening van de studenten van de Koninklijke Militaire School (I.7.2.).

I.7.1. DE SCREENING VAN MILITAIREN EN BURGERS BIJ DEFENSIE

De Wet van 28 februari 2007 tot vaststelling van het statuut van de militairen en kandidaat-militairen van het actief kader van de Krijgsmacht beschrijft, onder meer, de wervingsprocedure.

Kandidaten moeten aan verschillende voorwaarden voldoen: ze moeten de burgerlijke en politieke rechten genieten en blijk geven van de onontbeerlijke morele kwaliteiten (artt. 8 en 9). Ook mogen ze geen negatief veiligheidsadvies hebben gekregen (na een veiligheidsverificatie) of deze veiligheidsverificatie niet

---

45 Onder 'veiligheidsscreenings' wordt begrepen: *"een door of krachtens de wet opgelegde beoordeling door een administratieve overheid op basis van eigen of aangeleverde (persoons)gegevens waarbij uitgemaakt wordt of een private (rechts)persoon een profiel vertoont waaruit een risico blijkt dat hij/zij een niet-geëigend gebruik zal of zou kunnen maken van een bepaalde toelating en daarbij of daardoor bepaalde fundamentele (staats)belangen in het gedrang kan brengen zodat diezelfde of een andere (buitenlandse) overheid geïnformeerd kan beslissen over de toekenning, intrekking of beperking van die toelating"*.

46 VAST COMITÉ I, *Activiteitenverslag 2019*, 2 e.v. ('De uitvoering van veiligheidsscreenings door de inlichtingendiensten').

hebben geweigerd. Dit betekent dat behoudens indien de loopbaan van betrokkene een wijziging van het veiligheidsniveau zou vereisen, de militairen van het departement Defensie slechts één veiligheidsscreening tijdens hun volledige militaire loopbaan ondergaan. Het Comité was de mening toegedaan dat de vraag diende te worden gesteld of een dergelijke veiligheidsverificatie niet periodiek zou moeten worden herhaald tijdens de loopbaan van het militair personeel.[47]

Een andere regeling geldt voor wat betreft de burger(kandidaten) bij Defensie.[48] De overgrote meerderheid van het burgerpersoneel (1100 personen) zijn statutair; deze ambtenaren zijn benoemd en hebben de eed afgelegd. Een tweede groep burgers bestaat uit contractuelen die, net als in de privésector, op basis van een arbeidsovereenkomst worden aangeworven. Daarnaast zijn er ook burgers die niet als Defensiepersoneel worden beschouwd (bijv. onderzoekers aangeworven door het Patrimonium, gedetacheerde docenten van de Gemeenschappen bij de Koninklijke School voor Onderofficieren…). Alle aanwervingen van burgers, met uitzondering van de Rosetta-contracten[49], verlopen verplicht via SELOR.

Enkele uitzonderingen niet te na gesproken[50], wordt het burgerpersoneel van het departement Defensie niet onderworpen aan een veiligheidsverificatie. Het Comité was de mening toegedaan dat dit verschil in behandeling slechts kan worden gerechtvaardigd indien het ongepaste gebruik van de functie die zij uitoefenen, de fundamentele belangen van de Staat niet in gevaar kan brengen.

Het Vast Comité I bracht in dat kader de gevolgen van de evolutie van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen onder de aandacht. Immers, naast een mogelijke of concrete dreiging in een gebouw of plaats, kunnen sommige sites inherent (en permanent) gevoelig zijn voor dreigingen: de tarmac van een luchthaven, een basis van Defensie, enz. Het ongeëigende gebruik van de mogelijkheid om toegang te verkrijgen tot een dergelijke site kan ernstige schade toebrengen aan fundamentele belangen van de Staat. Hetzelfde geldt voor personen die een specifieke functie of opdracht uitoefenen of die een specifieke toelating willen verkrij-

47 Het blijkt immers dat de integriteit van sommige militairen wel degelijk een probleem kan vormen. Dit betekent dat deze leden alleen als zodanig bekend zullen zijn wanneer zij een bedreiging vormen die door de ADIV werd opgespoord.

48 Met inbegrip van de leden van de Dienst voor religieuze en morele bijstand (DRMB).

49 Rosetta-contracten of 'startbaanovereenkomsten' zijn contracten van een jaar die worden aangeboden aan jongeren onder de 26 jaar. Defensie organiseert de aanwervingsgesprekken zelf naargelang van haar behoeften.

50 Bijv. diegenen die worden aangeworven of gedetacheerd bij de ADIV, aangezien houder zijn van een veiligheidsmachtiging een van de essentiële voorwaarden is om er te kunnen worden tewerkgesteld.

gen. Aanvankelijk stond de wet toe dat 'elke administratieve overheid' dergelijke (positieve) adviezen kon vragen.[51]

De Wet van 23 februari 2018 en het KB van 8 mei 2018[52] hebben de procedure voor het veiligheidsadvies hervormd, zowel op het niveau van de reglementaire beslissing van de administratieve overheid als op het niveau van het individuele beslissingsmechanisme.

I.7.2. EEN VEILIGHEIDSSCREENING VOOR DE (BUITENLANDSE) STUDENTEN VAN DE KONINKLIJKE MILITAIRE SCHOOL?

De Koninklijke Militaire School (KMS) is een militaire instelling voor universitair onderwijs belast met de academische, militaire en fysieke basisvorming van toekomstige officieren, en met de voortgezette vorming van officieren tijdens hun loopbaan bij Defensie.[53]

De KMS opent haar deuren voor buitenlande studenten. De Veiligheid van de Staat merkte evenwel opdat [54]: " *[u]niversiteiten doorgaans open staan voor internationale samenwerking, wat alleen maar kan worden toegejuicht. Maar deze openheid is niet zonder risico. Ook andere actoren zijn zich bewust van de kennis die aan onze universiteiten te rapen valt. […] Studenten van militaire onderzoeksinstituten, zoals het Chinese National University of Defense Technology, worden uitgestuurd naar verschillende westerse landen waaronder België, waar ze kennis verwerven die essentieel is voor bepaalde militaire ontwikkelingen. De kennis die ze er opdoen, nemen ze mee naar het leger in hun thuisland. Aan de Belgische universiteiten zijn momenteel enkele tientallen van deze militaire studenten actief.*"

Ook het Vast Comité I was de mening toegedaan dat Defensie een kwetsbaarheid vertoont bij het toelaten van studenten uit het buitenland. Er bestaat namelijk

---

51 De beslissing (van reglementaire aard) om een (individueel) veiligheidsadvies te eisen kon enkel worden genomen "*wanneer de uitoefening van een beroep, een functie, een opdracht of mandaat, of de toegang tot lokalen, gebouwen of terreinen, of het bezit van een vergunning, een licentie of een toelating door een niet-geëigend gebruik schade kon toebrengen aan de verdediging van de onschendbaarheid van het nationaal grondgebied en van de militaire defensieplannen, de vervulling van de opdrachten van de strijdkrachten, de inwendige veiligheid van de Staat, met inbegrip van het domein van de kernenergie, en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen van België, het wetenschappelijk en economisch potentieel van het land, de veiligheid van de Belgische onderdanen in het buitenland of de werking van de besluitvormingsorganen van de Staat*".

52 Wet van 23 februari 2018 houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS*, 1 juni 2018) en Koninklijk besluit van 8 mei 2018 tot wijziging van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS*, 1 juni 2018).

53 De KMS biedt onder meer een basisstafvorming (BStV), een vorming voor Kandidaat Hoofdofficieren (VKHO) en een Hogere Stafopleiding (HStO) aan. Zie www.rma.ac.be

54 https://www.vsse.be/sites/default/files/paragraphs/1-ra2020-nl-version10-single-light.pdf

een aanzienlijk risico van spionage en inmenging voor bepaalde personen, die bovendien toegang krijgen tot informatie van Defensie.

De toelating van buitenlandse studenten vereist volgens het Comité dan ook een voorafgaande en systematische risicoanalyse per geval van de kandidaat-leerling door de ADIV.

I.8. DE OPVOLGING VAN POLITIEKE MANDATARISSEN

I.8.1. INTRODUCTIE

Veelvuldig werd in (parlementaire) debatten[55] de vraag gesteld of en in welke mate de Belgische inlichtingendiensten politieke mandatarissen (mogen) opvolgen en welke regels ze daarbij in acht moeten nemen.[56] Vanaf begin 2018 wordt in deze binnen de VSSE een als 'vertrouwelijk' geclassificeerde dienstnota toegepast. Conform deze nota, die werd geactualiseerd in juni 2020[57], zendt de VSSE twee types van rapporten naar de minister van Justitie en de Premier, met kopie naar het Vast Comité I. Het betreft enerzijds punctuele rapporten over politieke mandatarissen die bijdragen aan de totstandkoming van een dreiging alsook een trimestrieel overzicht van het geheel van documenten waarin melding wordt gemaakt van deze mandatarissen.[58] De minister van Justitie stemde daarbij in met het *'principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991*'.[59]

Gezien nergens wordt vermeld wat het Comité wordt geacht aan te vangen met voormelde informatie, nam het zelf het initiatief een methodologie uit te werken

---

55 Zie recent nog: Vraag van S. Creyelman aan de minister van Justitie over de 'politieke dossiers bij de VSSE' (*Vr. en Ant*. Kamer 2019-20, 16 juli 2020, QRVA 23, 33, Vr. nr. 351).

56 VAST COMITÉ I, *Activiteitenverslag 2019*, 69-70 ('IV.3. Toezicht op de opvolging van politieke mandatarissen').

57 De dienstnota van 13 december 2017 werd in juni 2020 geactualiseerd om de rapportage ten aanzien van de directie inzake disruptieve activiteiten te verbeteren. Ondanks herhaaldelijk verzoek mocht het Comité van de ADIV – die net zoals de VSSE werd aangespoord tot aanname van een uniforme richtlijn met klare en eenduidige regels met betrekking tot de inwinning, verwerking, raadpleging, opslag en archivering aangaande politieke mandatarissen, geen informatie in die zin ontvangen. De ADIV beschikte niet over een specifieke procedure (SOP) om met deze informatie om te gaan noch werd bepaald hoe het Vast Comité I hiervan op de hoogte te brengen

58 De bedoelde politieke mandatarissen zijn de ministers van de diverse regeringen, de Belgische commissaris in de Europese Commissie en de leden van de verschillende Parlementen, inclusief de Belgische leden van het Europees Parlement. Het gaat niet om andere verkozenen of aangeduide mandatarissen (bijv. op gemeentelijk vlak, zoals schepenen, of op provinciaal vlak, bijv. de gouverneurs).

59 *'met het toezichtsbeginsel/beginsel van verificatie/ dat noodzakelijk blijkt conform de organieke wet van 18 juli 1991'* (vrije vertaling) In: Brief van de minister van Justitie gericht aan het Vast Comité I d.d. 26 juli 2018 over 'Le recueil d'informations par un service de renseignement concernant une persone exerçant un mandat politique'.

omtrent de 'problematiek van de opvolging van de politieke mandatarissen door de inlichtingendiensten en de rol van het Vast Comité I'. Deze methodologie werd in 2020 door de parlementaire Begeleidingscommissie goedgekeurd. In navolging van deze methodologie werd in 2020 een (periodiek) toezichtonderzoek opgestart.[60] Het onderzoeksveld hierbij was hoe vaak tijdens de referteperiode (van 1 september 2019[61] tot en met 31 augustus 2020) over een mandataris informatie werd verzameld, verwerkt en gerapporteerd. Tevens werd bestudeerd of de informatieverzameling al dan niet wettig of 'disproportioneel' was en of de eerder door het Comité geformuleerde aanbevelingen werden uitgevoerd.[62]

Daartoe stelde het Vast Comité I een lijst op van de (543) personen die tussen de referentieperiode een uitvoerend politiek mandaat bekleedden op Europees, federaal, gewestelijk en gemeenschapsniveau.[63]

Deze lijst werd respectievelijk eind oktober 2020 overgemaakt aan de VSSE en de ADIV. De VSSE bezorgde het Comité de lijsten van relevante documenten opgesteld door haar buitendiensten en de analysedienst. De ADIV meldde dat de dienst tijdens de referteperiode geen Belgische politieke mandatarissen had gevolgd of onderzocht.

I.8.2. VASTSTELLINGEN AANGAANDE DE UITVOERING VAN DE AANBEVELINGEN VAN HET VAST COMITÉ I

I.8.2.1. De uitwerking van richtlijnen met betrekking tot de inwinning, de verwerking, de raadpleging, de opslag en de archivering van gegevens

In 2008 beval het Vast Comité I de uitwerking aan van klare en eenduidige richtlijnen met betrekking tot de inwinning, de verwerking, de raadpleging (met inbegrip

---

60 Het Comité voerde hieromtrent eerder al toezichtonderzoeken uit. Zie VAST COMITÉ I, *Activiteitenverslag 1998*, 67 e.v. ; *Activiteitenverslag 1999*, 12 e.v., *Activiteitenverslag 2008*, 23 e.v. ; *Activiteitenverslag 2013*, 3 ('I.I.3. Een nieuwe dienstnota van de VSSE over de opvolging van parlementsleden').

61 Start van de huidige federale legislatuur - parlementaire zittingsperiode 55 (2019- 2024).

62 VAST COMITÉ I, *Activiteitenverslag 2013*, 3 ('I.I.3. Een nieuwe dienstnota van de VSSE over de opvolging van parlementsleden').

63 In concreto betreft het: a) de ministers van de Vlaamse regering, de *Fédération Wallonie-Bruxelles*, de Waalse gewestregering, de Duitstalige gemeenschapsregering, de Brusselse regering, de federale regering en de Belgische commissarissen in de Europese commissie; b) de leden van de gemeenschaps- en gewestparlementen (*Fédération Wallonie-Bruxelles*, Waals gewest, Brussels Hoofdstedelijk Gewest, Vlaams parlement en Duitstalige gemeenschap), het federaal parlement (Kamer en Senaat) en van de Belgische leden in het Europees Parlement; en c) met uitzondering van voorzitters van politieke partijen die geen lid zijn van een parlement en geen uitvoerend mandaat bekleden van eerdergenoemde niveaus, leden van de Koninklijke familie, ministers van Staat, lokale mandatarissen (burgemeesters, schepenen, gemeenteraadsleden, leden van intercommunales) voor zover ze geen regionaal/gemeenschaps-/federaal/Europees mandaat bekleden, gouverneurs en ex-mandatarissen zonder actueel mandaat.

van de eventuele interne afscherming), de opslag en de archivering van gegevens van bepaalde categorieën van personen die bijzondere verantwoordelijkheden dragen of droegen. [64]

In juni 2020 legde de VSSE nieuwe interne richtlijnen vast inzake de geactualiseerde procedures en '*de meldingsplicht van de VSSE aan de minister van Justitie zodra bepaalde politieke mandatarissen opduiken in documenten van de VSSE*'.[65] De dienstnota verving drie eerdere dienstnota's over hetzelfde onderwerp.[66] Begin december 2020 verstuurde de VSSE een nota aan onder meer de politieke partijen die vertegenwoordigd zijn in het Federale Parlement met toelichting over de gehanteerde procedure wanneer politieke mandatarissen genoemd worden in het kader van onderzoeken van de VSSE.[67]

Niettegenstaande zijn aanbevelingen uit 2013[68], mocht het Vast Comité I van de ADIV geen informatie ontvangen dat het in een specifieke procedure (SOP)

64 VAST COMITÉ I, *Activiteitenverslag 2013*, 3 ('I.I.3. Een nieuwe dienstnota van de VSSE over de opvolging van parlementsleden')

65 VSSE, Dienstnota van 11 juni 2020.

66 De dienstnota van 4 juli 2013 met als onderwerp '*Wijzigingen voor het opstellen van documenten die in VESTA opgeslagen zijn*', de dienstnota van 25 juli 2013 met als onderwerp '*Dienstnota omtrent het linken van parlementsleden en politieke mandatarissen in documenten van de VSSE*' en de dienstnota van 13 december 2017 met als onderwerp '*de meldingsplicht van de VSSE aan de minister van Justitie zodra bepaalde politieke mandatarissen opduiken in documenten van de VSSE*'.

67 Procedure politieke mandatarissen inzake: '*Vermelding van een politiek mandataris in de databank van de VSSE*', '*Indien de politiek mandataris het slachtoffer is van een dreiging*', '*De veronderstelde of bewezen betrokkenheid van een politiek mandataris bij de totstandkoming van een dreiging*' (Nota VSSE).

68 VAST COMITE I, *Activiteitenverslag* 2013, 112 ('IX.1.2. Een richtlijn over inlichtingenwerk t.a.v. personen met bijzondere verantwoordelijkheden en politieke partijen' en 'IX.1.3. Eénduidige richtlijnen omtrent het melden van de opvolging van politici').

voorzag om met deze informatie om te gaan, noch werd een procedure bepaald om het Vast Comité I op de hoogte te brengen.[69]

I.8.2.2. Bijzondere aandacht voor de positie van de vermelde politieke mandatarissen

Het Vast Comité I beval aan dat de inlichtingendiensten in hun rapportage de nodige aandacht moesten besteden aan de hoedanigheid van een in een verslag vermeld persoon ten aanzien van de dreiging (slachtoffer, actor, passant…). Politieke mandatarissen kunnen te allen tijde (in de uitvoering van hun mandaat/in de marge van een dreiging) voorkomen in de informatie die de inlichtingendiensten verzamelen. Ze kunnen genoemd worden door menselijke bronnen, opduiken in berichten van partnerdiensten, voorkomen in lijsten die ontstaan door toepassing van technische middelen (bijv. telefonielijsten). In dergelijke gevallen loopt de politicus eerder toevallig door het beeld van de inlichtingendiensten.

De dienstnota van de VSSE bevat de bepaling dat politieke mandatarissen die voorkomen in documenten van de VSSE enkel 'gelinkt' mogen worden indien ze rechtstreeks in verband te brengen zijn met een dreiging als slachtoffer of als dader zoals bedoeld in de Inlichtingenwet.

Uit nazicht van de bedoelde documenten bleek evenwel dat de hoedanigheid van de vermelde politieke mandatarissen onvoldoende duidelijk stond aangegeven.

---

[69] Op 30 november 2017 meldde de ADIV het Vast Comité I dat sinds de aanbevelingen van 2013 de Organieke Wet van 1998 enkele malen geamendeerd of gewijzigd werd, stellende dat geen politieke of wetgevende autoriteit te kennen gegeven hadden dat er dergelijke regels dienden te worden opgesteld met betrekking tot het opvolgen van politieke verantwoordelijken. De opvolging van politieke verantwoordelijken door de ADIV had volgens deze laatste nog geen schade toegebracht aan de vrijheid van vereniging of meningsuiting en indien dit wel het geval zou zijn, zou dit gebaseerd zijn op de Organieke Wet die in overeenstemming is met de Universele Verklaring van de Rechten van de Mens en met de uitspraken van het Europees Hof voor de Mensenrechten, in die zin dat voorzien wordt dat in bepaalde speciale, welomschreven situaties kan worden ingegaan tegen één of ander fundamenteel recht. Ondanks deze vaststelling was de ADIV van mening dat alle initiatieven die de democratische controle op de inlichtingendiensten konden versterken dienden te worden aangemoedigd en dat ook de ADIV zelf in deze versterking een cruciale rol kon spelen. Vanuit deze optiek nam de ADIV het initiatief om contact op te nemen met de VSSE om zich te beraden over de genoemde aanbeveling(en). Aanvullend meldde de ADIV het Vast Comité I op 6 december 2017 dat het het voornemen had om in de loop van 2018 gelijkaardige procedures als die van de VSSE uit te werken om de democratische controleorganen te informeren, met dien verstande dat het uitwerken van dergelijke procedures ook gekoppeld moest worden aan het uitwerken van interne procedures betreffende het opslaan en archiveren van informatie over de betreffende politieke mandatarissen en organisaties. Het uitwerken van deze procedures diende deel uit te maken van een ruimer project dat voorziet in het opstellen van een aantal interne richtlijnen voor het functioneren van (kader)personeel van de ADIV. De audit van het Vast Comité I naar het functioneren van de Directie CI en van de ADIV, in februari en maart 2018, en de publicatie van de resultaten van deze audit op 15 mei 2018, doorkruisten de plannen van de ADIV om de genoemde procedures uit te werken. De ADIV oordeelde evenwel dat het verstandig zou zijn de conclusies af te wachten van het Business Process Re-engineering (BPR), het interne hervormingsproces van de ADIV dat er kwam als gevolg van de audit van het Vast Comité I. Op 6 januari 2020 ging de ADIV van start met zijn nieuwe structuur.

I.8.2.3. De uitwerking van artikel 19 W.I&V[70]

Bovenvernoemde dienstnota bepaalt dat een overzicht van alle documenten waarin politieke mandatarissen opduiken om de drie maanden door de VSSE aan het Vast Comité I wordt overgemaakt. Het overzicht bevat referenties van documenten die ruwe informatie bevatten en analysedocumenten. Het overzicht geeft ook aan welke nota's (zie verder) aan de minister van Justitie en de Premier werden overgemaakt.[71]

Ook wat de ADIV betreft, beveelde het Vast Comité I aan om haar driemaandelijks een overzicht te bezorgen van alle documenten waarin politieke mandatarissen worden vermeld.

I.8.3. DE COLLECTE, DE ANALYSE EN DE VERSPREIDING VAN INLICHTINGEN OVER POLITIEKE MANDATARISSEN TUSSEN 2019 EN 2020

I.8.3.1. Collecte en analyse

Tijdens de referentieperiode, werden van de 543 politieke mandatarissen:
- 267 of 49,17% niet opgenomen in de VSSE-databank;
- 124 of 22,84% opgenomen in de VSSE-databank, maar zonder link met een dreiging;
- 152 of 28% opgenomen in de VSSE-databank met vermelding in door de VSSE opgestelde (828) analysedocumenten over een dreiging.

Van de 828 documenten, zijn 53% (439) onderzoeksrapporten, 25% (206) documenten afkomstig van een externe (inter)nationale partner, 6% (53) nota's aan de Belgische autoriteiten en 16% (130) voornamelijk synthesefiches waarbij een interne analyse gemaakt wordt van een dossier en notulen van een vergadering.

---

70 "Art. 19 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.*
Met eerbiediging van de persoonlijke levenssfeer van de personen en voor zover de voorlichting van het publiek of het algemeen belang dit vereist, mogen de administrateur-generaal van de Veiligheid van de Staat en de chef van de Algemene Dienst Inlichting en Veiligheid, of de persoon die elk van hen aanwijst, inlichtingen aan de pers mededelen.".

71 De minister van Justitie en de Premier worden niet geïnformeerd over het louter accidenteel opduiken van politieke mandatarissen in documenten van de VSSE.

I.8.3.2. De verspreiding van inlichtingen

De VSSE bezorgt elke trimester aan de Premier en de minister van Justitie, met kopie aan het Vast Comité I, een overzicht van alle documenten in dewelke politieke mandatarissen voorkomen.

Daarnaast worden, zodra er op basis van beschikbare informatie een 'vermoeden' van betrokkenheid van een politieke mandataris bestaat bij de totstandkoming van een dreiging, de minister van Justitie en de Premier, met kennisgeving aan het Vast Comité I, geïnformeerd (meldingsfiches). Deze fiches kunnen worden vervolledigd met gedetailleerde geanalyseerde en geverifieerde informatie dat de notificatie aan de overheden rechtvaardigt. Tijdens de referentieperiode werden vijf van dergelijke meldingsfiches opgesteld voor evenveel mandatarissen.

Verder deelt de VSSE ook informatie mee over politieke mandatarissen wiens naam verschijnt in sommige documenten, zonder dat deze evenwel betrekking hebben op een concrete dreiging. Deze informatie, die wordt gedeeld via de zogenaamde '*notes aux autorités*, vermeldt de VSSE (minstens) de beschrijving van de wijze waarop de politieke mandataris bijdraagt tot de totstandkoming van de dreiging, een inschatting van de mogelijke gevolgen die deze betrokkenheid kan doen ontstaan of heeft doen ontstaan (voor zover daar zicht op is) en hoe het dossier verder zal worden opgevolgd door de VSSE.

Tijdens de referentieperiode maakten 17 op 543 politieke mandatarissen (3,13%) het voorwerp uit van 53 *notes aux autorités* (21 i.v.m. extremisme, 25 i.v.m. spionage en inmenging, en 7 andere, zoals bijv. criminele organisaties en corruptie).

I.8.4. RESPECT VOOR DE GRONDRECHTEN VAN POLITIEKE MANDATARISSEN

Het Vast Comité I vond geen aanwijzingen dat de VSSE politieke mandatarissen viseerde om redenen buiten de wettelijk opgesomde belangen en bedreigingen om, noch dat zij anders worden behandeld dan andere beroepsgroepen.

Uit het onderzoek van de *notes aux autorités* bleek niet dat bij de informatievergaring, -analyse en -verspreiding de grondrechten van de politieke mandatarissen niet werden gerespecteerd.

Steunend op de criteria opgenomen in de door de Begeleidingscommissie goedgekeurde methodologie, bleek uit het onderzoek dat politieke mandatarissen niet op disproportionele wijze voorkomen in de documenten van de VSSE.

I.9. HET OPSPOREN EN OPVOLGEN VAN DE RADICALISERING VAN EEN MILITAIR: DE ZAAK-JÜRGEN CONINGS

Midden mei 2021 verliet Jürgen Conings, door het Coördinatieorgaan voor de dreigingsanalyse (OCAD) gelabeld als 'potentieel gewelddadig extremist (PGE)[72]' in het bezit van wapens de kazerne van Leopoldsburg. Op het ogenblik van zijn verdwijning was betrokkene als korporaal-chef tewerkgesteld bij Defensie. Al snel wordt duidelijk dat betrokkene al bekend was bij de politie-, inlichtingen- en veiligheidsdiensten (*infra*). De zaak beroert de publieke opinie en roept, terecht, heel wat (parlementaire) vragen op.[73]

Op verzoek van de minister van Defensie opende het Vast Comité I het *'toezichtonderzoek naar het opsporen en 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'*.

De minister van Defensie had daarbij drie opdrachten voor ogen: (a) de betrouwbaarheid na te gaan van informatie over personen die verdacht worden van radicalisering binnen Defensie en (b) een samenwerking bewerkstelligen met de inspecteur-generaal van Defensie belast met een audit die meer in het bijzonder betrekking had op de aspecten van het personeelsbeheer, en c) een reeks aanbevelingen te formuleren om de goede werking van de ADIV, maar ook van Defensie in haar geheel, te garanderen.

Wat betreft de rol van het OCAD in deze, werd samen met het Vast Comité P een '*gezamenlijk toezichtonderzoek naar de rol van het OCAD in de opvolging van Jürgen Conings, met name voor wat betreft het ingestelde vooronderzoek, de dreigingsevaluatie niveau 3 en de gevolgen daarvan, en de informatie-uitwisseling over betrokkene*' opgestart.[74] De onderzoeksrapporten werden begin juli 2021 besproken met de parlementaire Begeleidingscommissie.

---

72 De 'PGE' vormen één van de categorieën van de gemeenschappelijke gegevensbank Terrorist Fighters waarvan het OCAD operationeel beheerder is. De als PGE ingeschreven entiteiten moeten voldoen aan een aantal criteria zoals gedefinieerd in het 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 1bis 'Het informatiebeheer' van hoofdstuk IV van de wet op het politieambt, *BS* 27 januari 2020. Hierover : *VAST COMITÉ I, Activiteitenverslag 2020*, 128 ('VI.1.1. De toevoeging van potentieel gewelddadige extremisten in de GGB TF').

73 Zie bijv. Actualiteitsdebat over de voortvluchtige militair (Commissie voor Landsverdediging), *Hand.* Kamer 2020-21, 26 mei 2021, CRIV55COM490 en de debatten naar aanleiding van het verlag van de Inspecteur-generaal: *Hand.* Kamer 2020-2021, 16 juni 2021, CRIV55COM519.

74 Zie 'I.10. De rol van het OCAD in de opvolging van de militair Jürgen Conings'.

I.9.1. EEN BEELD VAN DE PROFESSIONELE LOOPBAAN VAN JÜRGEN CONINGS

Het professionele parcours van Jürgen Conings is een kluwen van affectaties en mutaties, buitenlandse missies[75], opleidingen allerhande[76] en bijklussen in de private bewakingssector. De carrière van de militair, aangevangen in 1992, wordt gekenmerkt door verschillende affectaties tot aan zijn mutatie in juni 2020, op zijn vraag, naar de *Cel Pre-Deployment Training for Individual Augmentees* (PDT-IA[77]) een eenheid in Leopoldsburg die instaat om militairen voor te bereiden op buitenlandse missies. Hij was er logistiek medewerker en in die hoedanigheid onder meer verantwoordelijk voor het uithalen van wapens en munitie voor schietoefeningen.

In 2015 komt hij voor het eerst in het vizier van de Veiligheid van de Staat. Betrokkene kreeg in de schoot van Defensie steeds goede evaluaties, ondanks een sanctie (een arrest van vier dagen) voor racistische uitlatingen op Facebook in november 2019.[78] Het rapport van het Inspectoraat-generaal van Defensie maakt ook melding van psychosociale factoren.[79]

In maart 2020 solliciteert hij bij de Federale Politie voor de functie van veiligheidsagent, maar wordt afgekeurd op basis van zijn persoonlijkheidstest. Parallel met zijn affectaties bij Defensie, loopt zijn parcours in de private veiligheidssector als bewakingsagent.

Op 31 augustus 2020 wordt zijn veiligheidsmachtiging niet verlengd. Dezelfde dag wordt hij door het OCAD in 'vooronderzoek potentieel gewelddadig extremist' (PGE) geplaatst. Op 17 februari 2021 krijgt hij het full statuut 'PGE niveau 3' (art. 6, §1, 1°/2 KB TF). Op 3 maart 2021 wordt zijn sociale promotie geannuleerd. Op 17 mei 2021 kan hij ongestoord de kazerne in Leopoldsburg verlaten in het bezit van wapens en de volgende dag wordt zijn verdwijning gesignaleerd. Sinds 21 mei 2021 werd een onderzoeksrechter gevorderd voor 'moordpoging in een terroristische context' en 'verboden wapenbezit in een terroristische context'. De procedure voor ambtsontheffing werd opgestart. Op 20 juni 2021, vijf weken na zijn verdwijning, wordt hij levenloos aangetroffen.

Jürgen Conings maakte deel uit van een dertigtal[80] militairen die wegens hun extreemrechts gedachtengoed werden opgevolgd door de militaire inlichtingen-

---

75 Onder meer in ex-Joegoeslavië (BELBAT), in Afghanistan (Resolute Support Mission) en in Jordanië (Operation Desert Falcon).

76 Onder meer opleidingen voor rollend materiaal, technische opleidingen (*technic worker*, magazijnbeheer, radio herstelling…) en diverse wapenopleidingen.

77 Deze cel van de Landcomponent is verantwoordelijk voor de voorbereiding van militairen uit heel Defensie die als individu zullen deelnemen aan operaties. Hierbij kan worden gedacht aan militairen die ingezet worden in bepaalde opdrachten, los van een groot detachement gelinkt aan hun eigen eenheid of zelfs component.

78 Het motief luidt: *"Betrokkene heeft op sociale media een mening geuit die niet strookt met de waarden van Defensie en schade toebrengt aan het imago van Defensie"*.

79 Inspectoraat-generaal, Eindrapport E2103, Intern onderzoek PDT-IA, Beperkte verspreiding.

80 Ter vergelijking, de politiediensten volgen bijna 2500 personen op in het rechts-extremistische milieu.

dienst.[81] Bij zijn verdwijning kreeg hij de steun van ex-militair Tomas Boutens, voortrekker van de neonazigroepering Bloed, Bodem, Eer & Trouw.[82] Op een van zijn Facebookprofielen verwees hij naar de 'Siegrune', een runenteken dat in nazi-Duitsland werd gehanteerd. Meer nog dan de sporadische contacten met Boutens, bleek hij opgemerkt in de kringen van het Vlaams Legioen[83], waar hij gevechtstraining zou hebben gegeven. Jürgen Conings dook ook op op de Facebookgroep *Knights of Flanders*, een vereniging van extreemrechtse signatuur.

I.9.2. HET JURIDISCH EN BELEIDSMATIG KADER

Alvorens de informatiepositie van de inlichtingendiensten aangaande Jürgen Conings te evalueren, was het van belang de bevoegdheden van de VSSE en de ADIV te duiden in het kader van het detecteren, opvolgen en bestrijden van het terrorisme, extremisme en radicalisme.

I.9.2.1. De inlichtingenopdracht van de VSSE en de ADIV

De taakstelling van de VSSE binnen de strijd tegen het terrorisme, extremisme en radicalisme situeert zich in hoofdorde binnen haar inlichtingenopdracht (art. 7, 1° W.I&V). De wetgever heeft hierbij geopteerd om een limitatieve lijst op te stellen van veiligheidsdreigingen die behoren tot het bevoegdheidsdomein van de VSSE. Art. 8, 1°, tweede lid, b en c W.I&V definiëren de dreigingen die het voorwerp van het toezichtonderzoek uitmaakten, te weten terrorisme en extremisme.

Ook de werkzaamheden van de ADIV binnen de aanpak van het terrorisme, extremisme en radicalisme situeren zich in hoofdorde binnen zijn inlichtingenopdracht zoals gedefinieerd in artikel 11, §1, 1° W.I&V. Net zoals bij de VSSE dient de ADIV bepaalde fundamentele belangen van het land te vrijwaren door middel van de detectie, opvolging en bestrijding van bepaalde bedreigingen tegen deze belangen. Er bestaan ook verschillen met de bevoegdheidsomschrijving van de VSSE. Het belangrijkste verschil bestaat in de vereiste aanwezigheid van een militair as-

---

81 Extreemrechtse invloeden in militaire rangen is geen uniek Belgisch fenomeen en evenmin nieuw. In de Duitse elite-eenheid *Kommando Spezialkräft* (KSK) zijn sinds 2017 vijftig militairen verdacht van rechts-extremistische activiteiten. Recent was er in Frankrijk ongerustheid over een staatsgreep door ex-generaal uit (extreem-)rechtse kringen en ook in Nederland verlieten de afgelopen vijf jaar meerdere militairen de Krijgsmacht na extreemrechtse uitingen of gedragingen. Eind jaren '90 van vorige eeuw waarschuwde de toenmalige minister van Defensie al dat een para-bataljon nabij Antwerpen niet mocht worden aangetast door fascistische en racistische tendensen.

82 Boutens werd samen met zestien andere personen (zowat twee derden van de toenmalig gearresteerden bleken beroepsmilitair) veroordeeld tot vijf jaar gevangenisstraf wegens het plannen van terreuracties en het verspreiden van geweldsverheerlijkende ideologie. Boutens was één van de eersten die op Facebook zijn steun aan de voortvluchtige betuigde.

83 Een rechts-extremistische groupuscule die 'strijdt voor het Vlaamse volk en voor Vlaanderen'.

pect, ofwel in het te beschermen belang (bijv. de militaire defensieplannen, de vervulling van de militaire opdrachten), ofwel in de wijze waarop de te beschermen belangen aangetast kunnen worden, zijnde met middelen van militaire aard (bijv. militaire wapens, defensiepersoneel).

De door beide diensten verkregen inlichtingen, of met andere woorden de gecollecteerde en geanalyseerde informatie, worden vervolgens tijdig en doelgericht doorgegeven aan andere instanties.[84] Deze (in hoofdzaak politieke, administratieve, gerechtelijke, politionele, diplomatieke en militaire) instanties nemen uiteindelijk de nodige tegenmaatregelen ter bescherming van de nationale veiligheid.

De ruime wettelijke inlichtingenopdracht noodzaakt de inlichtingendiensten en hun beleidsverantwoordelijken om prioriteiten te leggen binnen de werkzaamheden. De VSSE en de ADIV hebben immers onvoldoende capaciteit en middelen ter beschikking om alle tot hun bevoegdheid behorende nationale veiligheidsdreigingen te detecteren, op te volgen en te beheersen (noch zou ze deze ooit kunnen hebben). De opdracht tot prioritisering is weggelegd voor de Nationale Veiligheidsraad (NVR).[85]

De NVR is eveneens belast met het bepalen van de nadere regels opdat de verschillende veiligheidsactoren zouden komen tot een effectieve samenwerking. Het Nationaal Strategisch Inlichtingenplan (NSIP), gezamenlijk opgesteld door de VSSE en de ADIV en in 2018 gevalideerd door de Nationale Veiligheidsraad *'beoogt'*, onder meer, *'de samenwerking tussen de twee inlichtingendiensten te optimaliseren om te komen tot een zo doeltreffend mogelijke uitvoering van een inlichtingenbeleid ten bate van de bevoegde instanties en van de bevolking.'*[86] In het (geclassificeerde) onderdeel 'Taakverdeling', worden de respectievelijke opdrachten van de VSSE en de ADIV bepaald wat betreft de aanpak van het terrorisme, extremisme en radicalisme.

---

84 Krachtens artikel 19 W.I&V zijn de bestemmelingen van de inlichtingen *'de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, (..) de politiediensten en (…) alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook (…) de instanties en personen die het voorwerp zijn van een dreiging bedoeld in de artikelen 7 en 11.'* De bestemmelingen van de informatie van de inlichtingendiensten zijn bijgevolg bepaalde politieke, bestuurlijke, gerechtelijke, politionele, diplomatieke en militaire overheidsinstanties. Daarnaast kunnen ook bedreigde personen of bedreigde instanties (bijv. een werkgever) in kennis gesteld worden van nuttige informatie.

85 Zoals voorzien in art. 10 W.I&V en art.2 van het koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité voor inlichtingen en veiligheid en het Coördinatiecomité voor inlichtingen en veiligheid, *BS* 29 december 2020.

86 Nationaal Strategisch Inlichtingenplan, p. 4.

I.9.2.2. Het uitvoeren van veiligheidsscreenings door de twee inlichtingendiensten

Naast inlichtingenopdrachten hebben de VSSE en de ADIV ook veiligheidsopdrachten. In eerste orde moet hierbij het uitvoeren van veiligheidsscreenings vermeld worden.

Beide diensten voeren veiligheidsonderzoeken uit, te weten onderzoeken ten dienste van een veiligheidsoverheid (vnl. de Nationale Veiligheidsoverheid – NVO) waarin wordt nagegaan of een persoon aan de voorwaarden inzake geheimhouding, loyauteit en integriteit voldoet die aanwezig dienen te zijn voor het verkrijgen of behouden van een veiligheidsmachtiging.[87] Verder zijn beide inlichtingendiensten belast met het uitvoeren van veiligheidsverificaties met het oog op het toekennen van een veiligheidsattest of -advies.

Binnen de Krijgsmacht vervult de ADIV eveneens de functie uit van veiligheidsoverheid. Dit wil zeggen dat ze, naast het uitvoeren van de veiligheidsonderzoeken en -verificaties, eveneens belast is met de afgifte van veiligheidsmachtigingen en veiligheidsadviezen. Het Comité stelde echter vast dat er binnen de Krijgsmacht geen algemene instructie bestaat waarbij op exhaustieve wijze de functies binnen Defensie worden opgesomd die houder moeten zijn van een veiligheidsmachtiging.

Krachtens de Wet van 28 februari 2007 tot vaststelling van het statuut van de militairen en kandidaat-militairen van het actief kader van de krijgsmacht wordt wel een positief veiligheidsadvies vereist voor elke kandidaat-militair (*cf.* art. 9, 9°). De wet legt evenwel geen periodieke veiligheidsscreening voor militairen op.

I.9.2.3. De verantwoordelijkheid van de ADIV inzake militaire veiligheid[88]

Naast de inlichtingenopdracht en het uitvoeren van veiligheidsonderzoeken en -verificaties, is de ADIV eveneens belast met *'het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting,*

---

87 De veiligheidsonderzoeken vinden plaats overeenkomstig de (gedateerde en weinig aangepaste) richtlijnen van 16 februari 2000 van het Ministerieel Comité voor inlichting en veiligheid (heden: de Nationale Veiligheidsraad). Het Comité bracht nogmaals de urgentie onder de aandacht om de richtlijnen van het Ministerieel Comité voor inlichting en veiligheid handelend over allerhande veiligheidsvoorschriften te actualiseren (omvang veiligheidsonderzoeken; classificatieregels; bewaring geclassificeerde stukken; infosec; taken veiligheidsofficieren). Betrokken richtlijnen dateren allen van 2001 en behoeven aanpassing.

88 Het Comité brengt in herinnering dat het reeds in 1999 en 2003 – telkenmale n.a.v. een omvangrijke wapen- en/of munitiediefstal op een militaire site – verslag uitbracht van een t.g.v. deze incidenten geopend toezichtonderzoek. Deze handelden over *'de doeltreffendheid van (ADIV) en de samenwerking van de twee inlichtingendiensten in verband met de wapendiefstal te Houthulst in 1997'* (VAST COMITÉ I, *Activiteitenverslag 1999*, pag. 83 ev.) en over *'de veiligheid en de bewaking van de militaire wapenopslagplaatsen (Thuin)'* (VAST COMITÉ I, *Activiteitenverslag 2003*, pag. 206 ev.).

plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen' (art. 11, §1, 2° W.I&V). Het begrip militaire veiligheid omvat zodoende, naast de veiligheid van inlichtingen, ook *'de veiligheid van de personen, van het materieel en van de installaties'*.[89]

Daartoe werden door de ADIV verschillende richtlijnen opgesteld en verspreid, zoals bijvoorbeeld deze over de opslag van wapens en munities (de Reglementen IF5 en IF5 bis).[90] De bevoegdheden van de ADIV bestaan erin het militair commando te adviseren inzake de aangewezen beschermingsmaatregelen, het verifiëren van de uitvoering ervan, het bij deze gelegenheden vaststellen van eventuele lacunes, het overmaken van de geconstateerde tekortkomingen aan het vermelde militair commando en het doen van de nodige aanbevelingen om eraan te verhelpen.

I.9.3. ONDERZOEKSVASTSTELLINGEN

De zaak-Conings is illustratief voor de vaststellingen die het Vast Comité I de afgelopen jaren doorheen zijn toezichtsonderzoeken deed.[91] Het lijkt alsof deze zaak een knooppunt vormt van alle eerdere constateringen, in het bijzonder wat betreft de militaire inlichtingendienst ADIV. Ook de aansluitend geformuleerde aanbevelingen bleven hun actualiteitswaarde houden. Dat gold tevens voor de aanbevelingen van de Parlementaire onderzoekscommissie 'terroristische aanslagen'.[92]

I.9.3.1. De informatiepositie van de VSSE

Jürgen Conings kwam voor het eerst onder de aandacht van de Veiligheid van de Staat in september 2015 in het kader van een Facebookgroep die fondsen inzamelde voor Dwekh Nawsha, een christelijke paramilitaire organisatie die de Assyrische gemeenschap in Irak verdedigde tegen de Islamitische Staat.[93] Hij trok een tweede maal de aandacht van de VSSE in oktober 2018.

---

89 Wetsontwerp houdende regeling van de inlichtingen- en veiligheidsdienst, *Parl. St.* Kamer 1995-1996, nr. 49-638/001, 11-12.

90 De ADIV heeft de laatste jaren meerdere malen aan het Vast Comité I te kennen gegeven dat het Reglement IF5(-bis) geactualiseerd zal worden. De meest recente versie van het Reglement overgemaakt aan het Comité is deze van het jaar 2016. Het Comité heeft geen kennis van een meer actuele globale versie.

91 Zie bijv. VAST COMITÉ I, *Activiteitenverslag 2020*, 38-53 ('De opvolging van extreemrechts door de Belgische inlichtingendiensten'); *Activiteitenrapport 2019*, 2-13 ('De uitvoering van veiligheidscreenings door de inlichtingendiensten'); *Activiteitenrapport 2016*, 70-73 ('Individuele evaluaties door het OCAD'); *Activiteitenrapport 2011*, 7-14 ('Een audit bij de militaire inlichtingendienst') en 25-33 ('De informatiestromen tussen het OCAD en de steundiensten').

92 *Parl. St.* Kamer, 2016-17, 54DOC1752/008 (15 juni 2017).

93 Volgens open bronnen zouden *foreign fighters* uit onder andere de Verenigde Staten, Frankrijk, het Verenigd Koninkrijk en Australië zich hebben aangesloten bij Dwekh Nawsha.

In beide documenten van 2015 en 2018 wordt vermeld dat betrokkene een militair is. Het Vast Comité I stelde vast dat de informatie uit 2015 door de VSSE niet werd gedeeld met de ADIV, aangezien ze op dat moment als onvoldoende relevant werd beschouwd door de VSSE. De informatie uit 2018 werd gedeeld met de ADIV tijdens een vergadering met de Werkgroep Extreemrechts, waar in algemene bewoordingen de naam van de organisatie en de voornaamste figuren werden gedeeld. Deze informatie werd in 2020 ook gedeeld met het OCAD.

Tussen juli 2020 en mei 2021 stelde de VSSE een aantal informatieverslagen op waarin de deelname van Conings aan activiteiten van de extreemrechtse groeperingen *Knights of Flanders* en Vlaams Legioen wordt gemeld. Ook stelde de VSSE vast dat Conings contacten onderhield met Tomas Boutens, de in 2014 voor feiten van terrorisme veroordeelde ex-militair en leider van de neonazigroepering Bloed, Bodem, Eer en Trouw (BBET).

Eind juni 2020 richtte de VSSE een nota aan onder andere het OCAD, het Federaal Parket en de ADIV waarin de VSSE gewag maakt van een extremistisch Facebookprofiel van Conings en de door hem geuite bedreigingen aan het adres van viroloog Marc Van Ranst. Begin augustus 2020 stelt de VSSE een aantal specifieke vragen aan de ADIV. Voor zover het Vast Comité I kon nagaan, werd door de ADIV nooit formeel geantwoord op deze vragen van de VSSE.

I.9.3.2. De informatiepositie van de ADIV

Vanaf juli 2020, kort nadat Conings via politionele informatie in verband werd gebracht met mogelijke bedreigingen aan het adres van Marc Van Ranst, wordt intern de ADIV gemeld dat betrokkene extra aandacht dient te krijgen. Deze informatie werd op dat moment niet door de ADIV meegedeeld aan het OCAD, hoewel er met betrekking tot Conings reeds een vooronderzoek liep in het kader van zijn mogelijke opname als PGE in de GGB TF.

In februari 2021 keurt de ADIV een inlichtingenoperatie goed, t.t.z. de inzet van bijzondere inlichtingenmethoden, met Conings als één van de doelen. Het onderzoek van het Comité kon evenwel aantonen dat tot 17 mei 2021 geen enkele bijzondere inlichtingenmethoden effectief werd ingezet. De ADIV verklaarde dit als zijnde een gevolg van de te grote werklast en de afwezigheid van voldoende medewerkers belast met het beheer van de BIM's.[94]

Er werd geen beroep gedaan op de tussenkomst van de VSSE in deze, omdat het een militair betrof.

[94] Bij afwezigheid of verhindering van medewerkers, wordt niet automatisch in hun vervanging voorzien. Op die wijze kon het gebeuren dat de operatie met o.m. Conings tot voorwerp, een vertraging opliep gezien de afwezigheid door ziekte van de *case manager* die de operatie moest leiden alsook de afwezigheid van de vertegenwoordiger van de ADIV op de cruciale LTF van 24 februari 2021 waarop de vermelding gebeurde dat Conings werd ingeschreven als PGE in de GGB TF en de toekenning van dreigingsniveau 3 (*infra*).

Uit de gesprekken die door het Vast Comité I werden gevoerd met de medewerkers van de ADIV is gebleken dat deze medewerkers niet of nauwelijks vertrouwd zijn met het gebruik en de finaliteit van de GGB TF.[95] Voor hen verandert de opname van een entiteit niets aan de opvolging van deze entiteit op het vlak van inlichtingenwerk.

Niettegenstaande een vijftigtal medewerkers van de ADIV een rechtstreekse toegang hebben tot de GGB TF, werden er voor de periode tussen november 2020 en april 2021, amper een dertigtal loggings door slechts enkele medewerkers vastgesteld.[96] Wat specifiek Jürgen Conings betreft, werd zijn inlichtingenfiche geraadpleegd op 15 januari en 19 februari 2021 (op 17 februari krijgt hij PGE niveau 3). De inlichtingenoperatie die de ADIV wilde opstarten met betrekking tot betrokkene in dezelfde periode, had geen verband met het gegeven dat betrokkene door het OCAD werd geëvalueerd als PGE en er voor hem een dreigingsniveau 3 werd vastgesteld.

Er kon worden geconcludeerd dat er binnen de ADIV geen rekening wordt gehouden met het bestaan van het Plan R en de GGB TF. Er bleek dat noch het feit dat betrokkene het voorwerp uitmaakte van een vooronderzoek PGE, noch dat hij als PGE werd opgenomen in de GGB TF, noch dat het OCAD aan hem een dreigingsniveau 3 toekende, een impact had op de opvolging van betrokkene door de militaire inlichtingendienst.

De ADIV voldeed niet aan zijn verplichtingen aangaande de werking van de *Lokale Task Forces* (LTF).[97] Na de opname in vooronderzoek van betrokkene in de GGB werd geen bijkomende informatie aangeleverd door de ADIV (gegeven het militaire statuut van betrokkene), en werd door de dienst geen aanzet gegeven tot een debat over eventueel te nemen maatregelen. Op de bijeenkomst van de betrokken LTF van 24 februari 2021 waarop de opname van Conings in de GGB FTF en het dreigingsniveau 3 werd meegedeeld, was bovendien geen vertegenwoordiger van de ADIV aanwezig.

---

95 Zij bleken niet op de hoogte van wat de betekenis en de gevolgen zijn van een opname van een entiteit in één van de categorieën van de GGB TF en van een bepaald dreigingsniveau dat aan een dergelijke entiteit is toegekend.

96 Uit de gesprekken bleek dat niemand van de analyse- of collectedienst noch de hiërarchie op de hoogte was dat Jürgen Conings was opgenomen in de GGB TF, en dus ook niet van het feit dat betrokkene sinds eind februari 2021 als PGE niveau 3 stond geficheerd.

97 Bijkomend probleem is dat de bijeenkomsten van de betrokken LTF in de beginperiode van de COVID 19-pandemie voor enige tijd werden opgeschort (maart en april 2020) en daarna plaatsvonden in een 'hybride' vorm, waarbij sommige diensten fysiek deelnamen aan de vergaderingen, terwijl andere diensten enkel deelnamen via videoconferentie. Omwille van de onbeveiligde communicatie via videoconferentie, kon geen geclassificeerde informatie tussen de deelnemers worden uitgewisseld.

I.9.3.3. Gebrekkige communicatie

Naast sommige dysfuncties in de communicatie met de VSSE[98] en het OCAD[99], zette de zaak-Jürgen Conings de blijvende communicatieproblemen in de schoot van de ADIV zelf in het voetlicht. Reeds in eerdere toezichtonderzoeken alsook door de parlementaire onderzoekscommissie terroristische aanslagen, werd vastgesteld dat de dienst het hoofd moet bieden aan grote uitdagingen inzake interne communicatie, informatiedoorstroming en -beheer en werden hierover aanbevelingen geformuleerd.

De in januari 2020 uitgetekende nieuwe structuur om tegemoet te komen aan de aanbevelingen, kon deze problemen uit het verleden (vooralsnog) niet verhelpen. Uit het onderzoek bleek dat vooral medewerkers van de ADIV op de 'hiërarchisch lagere echelons' de huidige structuur van de dienst als complex en onduidelijk percipiëren. Er bleek onduidelijkheid over de bevoegdheden en de communicatielijnen.

Daarnaast kon het Comité vaststellen dat er zich binnen het analyseplatform PF6, belast met de opvolging van extreemrechts, een aantal problemen hebben voorgedaan tussen juli 2020, het moment waarop Jürgen Conings onder de aandacht kwam omwille van bedreigingen tegen viroloog Marc Van Ranst, en februari 2021, het moment waarop betrokkene wordt opgenomen in de GGB TF.

Ook over de precieze werking van de *Defence Intelligence & Security Command and Control* (DISCC) bestaat er veel onduidelijkheid. De DISCC bestaat onder meer uit een Steering Committee, verantwoordelijk voor de operationele aansturing van het inlichtingenwerk en dat onder bevel staat van het hoofd van de ADIV. Een belangrijk onderdeel van de DISCC is het *Collection Coordination Intelligence Requirements Management* (CCIRM), dat een cruciale rol heeft in de coördinatie en behandeling van alle inkomende (*Requests for Information* (RFI), HUMINT-rapporten) en uitgaande (*Requests for Collect* (RFC), nota's aan autoriteiten) informatie.

Meerdere medewerkers spraken hun twijfel uit over de kennis van de werking van de dienst en de ervaring met inlichtingenwerk van de medewerkers die deel uitmaken van de DISCC (maar meer in het bijzonder van het CCIRM). Door deze gebrekkige kennis en ervaring zou informatie vaak te traag en verkeerd worden georiënteerd. De twijfels die bij bepaalde medewerkers bestaan over de goede wer-

---

98 In 2018 communiceerde de VSSE de informatie aangaande Jürgen Conings op een vergadering van de Werkgroep extreemrechts (Plan R). De ADIV antwoordde niet formeel op een nota van 8 januari 2021, waarin de VSSE haar bezorgdheid uitte ten aanzien van Jürgen Conings. De ADIV zou de vraag opgeworpen hebben tijdens een bilaterale vergadering die plaatsvond op 15 januari 2021.

99 Zie hierover het gemeenschappelijk toezichtonderzoek van de Vaste Comités I en P (I.10.). De medewerkers van de ADIV onderlijnden dat het niveau 3 van de dreiging niet aan de ADIV werd overgemaakt in een afzonderlijke evaluatie. Het OCAD liet dan weer opmerken dat de dreigingsevaluaties van personen opgenomen in de GGB TF enkel kunnen geconsulteerd worden via dat kanaal.

king van de DISCC, zorgt ervoor dat informatie buiten de DISCC om circuleert, waardoor parallelle informatiestromen ontstaan.

In voorliggend dossier verklaarden de medewerkers van het analyseplatform PF6 dat zij de belangrijke nota van de VSSE van begin januari 2021, waarin deze dienst zijn bezorgdheid uitspreekt over Jürgen Conings en een aantal vragen stelt aan de ADIV, nooit ontving, en dus ook niet werd beantwoord. Deze bewuste nota werd volgens PF6 door de DISCC niet ingevoerd in het *Request for Information Management*-systeem, dat normalerwijze gebruikt wordt voor inkomende vragen van externe diensten.

In de schoot van de DISCC zijn de leden van het Steering Committee, die verondersteld worden operationele beslissingen te nemen, onvoldoende op de hoogte van de inhoud van de dossiers. Er werd ook vastgesteld dat de beslissingen van het Steering Committee zelden officieel worden neergeschreven, waardoor verwarring ontstaat.

Een derde essentieel onderdeel van de DISCC zijn de zogenaamde *Case Managers* (CaMa) en *Collection Managers* (CoMa) belast met de vertaling van de informatiebehoeften van de analyseplatforms naar de inzet van collectemiddelen, wanneer er gebruik dient te worden gemaakt van bijzondere inlichtingenmethoden (BIM). Door het feit dat de CaMa en CoMa organisatorisch deel uitmaken van de DISCC, vallen zij buiten de structuren (Directies) waar de analyseplatformen en collectediensten zijn ondergebracht. Deze Directies kennen dan weer hun eigen structuur en hiërarchie, wat leidt tot discussies over bevoegdheden en prioriteiten. Zo is bijvoorbeeld het hoofd van de sectie C6/Investigations (dewelke deel uitmaakt van de Directie Collecte) in de huidige structuur niet bevoegd om te beslissen waarvoor zijn medewerkers inhoudelijk worden ingezet.

Het onderzoek toonde eveneens aan dat de provinciale detachementen[100], belast met de deelname aan de maandelijkse vergaderingen van de *Local Task Force* (LTF) en het onderhouden van contacten met de korpscommandanten (CO's) en de veiligheidsofficieren van de eenheden, te weinig worden gevaloriseerd. Het Comité stelde vast dat deze 'nabijheid' te weinig wordt benut door de centrale diensten uit Evere. Meer bepaald worden de provinciale detachementen te weinig aangestuurd. [101]

Verder is ook is gebleken dat er weinig overleg is tussen de provinciale detachementen en het hoofdkwartier, waardoor de medewerkers in de provinciale detachementen zich enigszins aan hun lot overgelaten voelen, en zelf hun prioriteiten stellen. Zo kon het gebeuren dat Jürgen Conings op 18 februari 2021 als

---

100 De provinciale detachementen zijn als het ware een antenne van de ADIV in elke provincie en staan dus veel dichter bij de militaire eenheden dan de centrale diensten in Evere. In deze positie zijn ze dan ook in staat om bepaalde ontwikkelingen snel te detecteren of om van dichtbij bepaalde zaken/gebeurtenissen op te volgen. Maar ook zijn zij vaak de best geplaatsten om op de vragen van de centrale diensten te antwoorden omdat ze ter plaatse de contacten hebben en de omgeving kennen.

101 Ook hierop werd in het verleden door het Vast Comité I reeds herhaaldelijk op gewezen.

potentieel gewelddadig extremist (PGE) werd opgenomen in de GGB TF met dreigingsniveau 3, en dat hierover geen overleg plaatsvond tussen het bevoegde analyseplatform en de medewerker van het provinciaal detachement Limburg, die namens de ADIV aan de betrokken LTF deelnam.

Het is het detachement Limburg dat in november 2019 voor het eerst melding maakt van Jürgen Conings, meer bepaald zijn betrokkenheid bij de extreemrechtse groepering *Belgian Commandery of Knights Templar*. Vervolgens is er, tot einde juni 2020, het moment waarop andermaal het provinciaal detachement de centrale diensten inlicht dat zij door de Federale Politie en het Parket werd gecontacteerd omdat betrokkene zich via Facebook informeert naar het adres van Marc Van Ranst, geen andere communicatie geweest tussen de centrale diensten in Evere en het provinciaal detachement. Het detachement werd niet gevraagd om bijkomende informatie te verzamelen.

I.9.3.4. De 'watchlist extreemrechts'

De minister van Defensie verzocht het Comité de betrouwbaarheid van de door de ADIV opgestelde *'watchlist'* te beoordelen. In de loop van zijn onderzoek heeft het Vast Comité I vastgesteld dat de *'watchlist'* in feite een intern proces binnen de ADIV was. Om tegemoet te komen aan voorgaande aanbevelingen van het Comité[102] werd een in april 2021 een nieuwe *'watchlist'* opgesteld, te weten een verzameling van individuele fiches met betrekking tot personen die door de ADIV werden opgevolgd in het kader van de extreemrechtse dreiging.

Doel van dit proces is om op basis van een periodieke herbeoordeling het niveau van individuele dreigingen uitgaande van extreemrechts te bepalen, alsook de *follow-up* die daaraan moet worden gegeven (extra informatieverzameling, uitwisseling van informatie met andere diensten, vaststelling van curatieve maatregelen, schrapping van de betrokkene van de *'watchlist'* wanneer blijkt dat hij of zij niet langer een bedreiging vormt…).

De *'watchlist'* is aldus geen volledig afgewerkte verzameling van gegevens over de personen die binnen de reikwijdte van de dreiging in verband met rechts-extremisme vallen en die behoren tot de bevoegdheid van de ADIV. De lijst moet gecombineerd worden met andere informatie. Als een intern proces is het niet de bedoeling dat deze als zodanig wordt meegedeeld aan derden. Aangezien het begrip 'betrouwbaarheid' waaraan de minister van Defensie vroeg de *'watchlist'* te toetsen als zodanig niet verankerd zit in de regeling van de werkzaamheden van de ADIV, heeft het Vast Comité I besloten de in de *'watchlist'* opgenomen (persoons) gegevens te toetsen aan de wettelijke kwaliteitsnorm van de verwerkte (persoons) gegevens, zoals bepaald in het art. 75, derde en vierde lid, en art. 83, eerste lid, van de Wet op de gegevensbescherming. Het is inderdaad zo dat, des te meer de

102 Zie VAST COMITÉ I, *Activiteitenverslag 2020*, 169-171 ('Diverse aanbevelingen naar aanleiding van het toezichtonderzoek naar de opvolging van extreemrechts').

verwerkte gegevens adequaat, ter zake dienend, niet buitensporig, volledig en bijgewerkt zijn overeenkomstig het doel van de *'watchlist'*, hoe meer deze *'watchlist'* als 'betrouwbaar' kan worden beschouwd.

In dit normatieve kader was het Vast Comité I - gelet op het doel van de *'watchlist'*, namelijk een intern werkproces in ontwikkeling voor het signaleren en monitoren van de dreiging van extreemrechts dat onder de bevoegdheid van de ADIV valt - van oordeel dat de overeenstemming van de *'watchlist'* met artt 75. lid 3 en 4, en 83, lid 1, van de Wet op de gegevensbescherming geen aanleiding gaf tot bijzondere opmerkingen. Het Vast Comité I achtte het desalniettemin noodzakelijk een reeks aanbevelingen aan de ADIV te formuleren, met het oog op de voortzetting, voltooiing en documentering van het werkproces inzake de *'watchlist'*.

I.9.3.5. De opeenvolgende veiligheidsmachtigingen van Jürgen Conings

Jürgen Conings was sinds 21 augustus 2006 in het bezit van een veiligheidsmachtiging niveau GEHEIM.[103] Zijn machtiging werd herhaaldelijk vernieuwd, en dit ondanks diverse politieberichten over betrokkene (aangaande bedreigingen en opzettelijke slagen en verwondingen).

In de loop van de procedure tot aanvraag van vernieuwing door zijn veiligheidsofficier in 2019, maakt de VSSE melding van een 'hit' naar aanleiding van twee feiten van gerechtelijke aard, waarvan er één betrekking had op het bezit van een illegaal wapen. Na contact met de ADIV vond een mondeling gesprek plaats dat aanleiding gaf tot het opstellen van een interne e-mail, waarin werd vermeld dat Jürgen Conings bekend was als lid van een Facebook-groep die de Assyrische belangen in Irak verdedigt. De feiten van 2015 worden vermeld, maar niet de feiten van 2018... Op basis van deze informatie lanceert de ADIV een eerste SOCMINT-analyse. Deze bracht mogelijke banden met extreemrechtse bewegingen aan het licht. Naar aanleiding van een gesprek met betrokkene, concluderen de onderzoekers dat de ontdekte feiten in verband met extreemrechts niet van dien aard zijn dat zij zijn veiligheidsmachtiging aantasten, maar bevelen een waarschuwing aan.

Op 24 juni 2020 krijgt Conings een verlenging van zijn machtiging. Twee dagen later werden bedreigingen geuit aan het adres van Marc Van Ranst; een analist van de ADIV identificeerde Jürgen Conings op de bewakingsvideo's en een administratief verslag (RAR) van de politie vervolledigde het beeld. Een tweede SOCMINT-analyse werd uitgevoerd en bracht nieuwe en meer verontrustende banden

[103] Art. 4 W.C&VM onderscheidt drie classificatieniveaus, te weten VERTROUWELIJK, GEHEIM en ZEER GEHEIM.

met extreemrechts aan het licht. Op basis van deze elementen, heeft de ADIV geweigerd de veiligheidsmachtiging op 31 augustus 2020 te verlengen.[104]

I.9.3.6. De opdracht van de veiligheidsofficier

Op 2 juni 2020 werd Jürgen Conings overgeplaatst naar zijn nieuwe eenheid (PDT-IA) in een functie waarvoor niet langer een veiligheidsmachtiging vereist was. De veiligheidsofficier die verantwoordelijk was voor zijn nieuwe eenheid heeft het verzoek om verlenging niet beëindigd. In bepaalde gevallen en in het kader van de inzet is een dergelijke toestemming inderdaad noodzakelijk.

Begin september 2020 werd hij door de ADIV op de hoogte gebracht van de niet-verlenging. Gezien de COVID-omstandigheden werd betrokkene telefonisch van deze weigering in kennis gesteld. De mondelinge kennisgeving werd schriftelijk bevestigd op 12 november 2020, d.w.z. twee en een halve maand na de weigering.

Het IF5-reglement bij ADIV beschrijft de verantwoordelijkheden van de veiligheidsofficier, onder meer belast met het opstellen van permanente beveiligingsorders en met het toezicht op de uitvoering ervan. Er wordt echter geen melding gemaakt van samenwerking of interactie met het ADIV-personeel.

Het geval van de veiligheidsofficier van Jürgen Conings is bijzonder. Als verantwoordelijke voor een groot aantal kleine onafhankelijke entiteiten, is hij gedelokaliseerd van de eenheden. Deze delokalisatie laat hem zeker geen effectieve controle over de veiligheidsrichtlijnen toe.

Het Vast Comité I stelde vast dat de ADIV niet met de veiligheidsofficier had gecommuniceerd in verband met de weigering van een machtiging aan Jürgen Conings. Het Comité heeft ook vastgesteld dat de veiligheidsofficier niet in staat was controle uit te oefenen op alle gebouwen die onder zijn verantwoordelijkheid vielen.

I.9.3.7. Het wapendepot en de rol van de ADIV

Op 18 mei 2021 merkte een collega van Jürgen Conings op dat wapens en munitie ontbraken uit het wapen- en munitiedepot van de PDT-IA cel. Hij meldde het incident onmiddellijk aan zijn hiërarchie en stelde een intern onderzoek in op het niveau van de Directie Veiligheid (Dir S) van de ADIV. De interne richtlijnen van de ADIV (meer in het bijzonder het Reglement IF5*bis*), sluiten immers uit dat eenzelfde persoon zowel wapen- als munitiebeheerder is. Het IF5-reglement kent ook een speciale status toe aan deze depots. Zo bijvoorbeeld moeten de beheerders van munitiedepots en wapendepots over een veiligheidsmachtiging beschikken.

---

104 Gelet op de termijnen was Jürgen Conings vanaf 17 juli 2020 niet langer gerechtigd dit te doen. Ter herinnering: deze afwezigheid of weigering had geen gevolgen voor zijn nieuwe functie bij Defensie.

Het onderzoek bracht aan het licht dat de regels niet werden gerespecteerd binnen de PDT-IA-cel.

De veelvuldige aanpassingen van de regels, gekoppeld aan de COVID-situatie, stelde Jürgen Conings in staat te beschikken over het arsenaal waarmee hij op de vlucht was geslagen.

I.9.4. CONCLUSIES

De zaak-Conings is exemplarisch voor de vaststellingen van de mankementen die het Vast Comité I de afgelopen tien jaar deed bij de inlichtingen- en veiligheidsdiensten in het algemeen en bij de militaire inlichtingendienst in het bijzonder.

Er kan niet worden ontkend dat met de zaak-Conings de militaire inlichtingendienst in het oog van de storm kwam te staan. Het is onmiskenbaar dat er op alle niveaus binnen de ADIV, maar ook in de gehele hiërarchische lijn bij Defensie, (ernstige) fouten werden gemaakt: een structureel personeelsgebrek in de verschillende diensten en op alle niveaus, het grote personeelsverloop, het verlies van kennis en ervaring, een beperkte supervisie in de eenheid van Conings, een manifest gebrek aan informatiedoorstroming (*bottom up* en *top down*), een nieuwe en complexe werkingsstructuur bij de ADIV, te weinig aansturing, personeelsproblemen, geen eenduidig beleid met betrekking tot extremisme, gebrekkige informatie-uitwisseling binnen Defensie en tussen de diverse veiligheidsactoren…. Maar mogelijks kunnen ook bij andere actoren (politie, parketten, onderzoeksrechters…) eveneens fouten worden vastgesteld. Die studie hiervan viel evenwel buiten het bevoegdheidsdomein van het Vast Comité I.

Er kon worden vastgesteld dat de feiten *in casu* wel tijdig door de inlichtingen- en veiligheidsdiensten werden gedetecteerd, maar onvoldoende actief opgevolgd. Dat er een ruime marge voor verbetering is, is duidelijk.

Voor het Vast Comité I staat het buiten kijf dat de ADIV noodzakelijk is in de algemene veiligheidsarchitectuur, zowel in België als in het buitenland. Niettemin moet de werking ervan grondig worden gewijzigd, evenals de structuur. Idealiter zouden de taken van de ADIV moeten worden teruggebracht en zou het verwachte *change management* moeten worden verwezenlijkt in het kader van een professionalisering ten dienste van de veiligheid van de burger.

I.10. DE ROL VAN HET OCAD IN DE OPVOLGING VAN DE MILITAIR JÜRGEN CONINGS

Ter vervollediging van het toezichtonderzoek naar het opsporen en opvolgen van Jürgen Conings door de twee inlichtingendiensten[105], onderzocht het Vast Comité I, samen met het Vast Comité P, "*de rol van het OCAD in de opvolging van Jürgen Conings, met name voor wat betreft het ingestelde vooronderzoek, de dreigingsevaluatie niveau 3 en de gevolgen daarvan, en de informatie-uitwisseling over betrokkene.*" De Vaste Comités P en I bestudeerden de informatiepositie van het coördinatieorgaan, het proces van de dreigingsevaluatie van betrokkene en de informatie-uitwisseling tussen de verschillende partners.[106]

I.10.1. ANALYSE VAN HET WETTELIJK KADER

De Wet betreffende de analyse van de dreiging van 10 juli 2006 (W.OCAD) kent aan het OCAD de opdracht toe om op punctuele basis een gemeenschappelijke evaluatie uit te voeren die moet toelaten te oordelen of dreigingen inzake terrorisme en extremisme zich voordoen en welke maatregelen in voorkomend geval noodzakelijk zijn.

Om de dreiging te evalueren, baseert het OCAD zich op de inlichtingen afkomstig van de ondersteunende diensten (bijvoorbeeld de Veiligheid van de Staat (VSSE), de Algemene Dienst Inlichting en Veiligheid (ADIV) of nog, de Federale Politie). Volgens de W.OCAD zijn de ondersteunende diensten (op straffe van een penale sanctie) verplicht, behoudens het bestaan van een embargoprocedure, ambtshalve of op vraag van de directeur van het OCAD, alle inlichtingen waarover zij in het kader van hun wettelijke opdrachten beschikken en die relevant zijn voor het vervullen van de opdrachten het OCAD, mee te delen binnen de termijnen zoals voorzien in het koninklijk besluit van 28 november 2006 tot uitvoering van de Wet betreffende de analyse van de dreiging. De informatieflux tussen het OCAD en zijn ondersteunende diensten verschilt naargelang het al dan niet geclassificeerde documenten betreft. Het OCAD en de ondersteunende diensten kunnen de geclassificeerde documenten uitwisselen via een geëncrypteerd informaticasysteem (BINII). De geclassificeerde informatie wordt daarna door het OCAD geregistreerd in hun databank PROTEUS. Een functionele mailbox van het OCAD wordt gebruikt voor alle niet-geclassificeerde informatie-uitwisseling.

In artikel 11§6 van het uitvoeringsbesluit op de W.OCAD wordt bepaald dat iedere evaluatie het niveau van de dreiging zal bepalen door zich te steunen op een beschrijving van de ernst en de waarschijnlijkheid van het gevaar of van de drei-

105 Zie 'I.9. Het opsporen en opvolgen van de radicalisering van een militair: de zaak-Jürgen Conings'.

106 De referteperiode liep tot 17 mei 2021, de dag van de verdwijning van Jürgen Conings.

ging.[107] Volgens artikel 10 van de W.OCAD worden de punctuele dreigingsevaluaties gericht tegen personen, groeperingen of gebeurtenissen, die op initiatief van het OCAD worden uitgevoerd, meegedeeld aan de leden van de Nationale Veiligheidsraad, de ondersteunende diensten, de Algemene Directie Crisiscentrum, het Federaal Parket en het lid van het College van procureurs-generaal dat specifiek belast is met terrorisme en extremisme, de Nationale Veiligheidsoverheid evenals aan ieder lid van de regering waarvan de directeur van het OCAD het noodzakelijk oordeelt het te informeren.

De dreigingsevaluatie aangaande een persoon wordt dan weer geregeld overeenkomstig het koninklijk besluit betreffende de gemeenschappelijke gegevensbank Terrorist Fighters van 21 juli 2016 (KB GGB) en de Omzendbrief van 22 mei 2018 van de minister van Veiligheid en Binnenlandse Zaken en de minister van Justitie betreffende de informatie-uitwisseling rond en de opvolging van *terrorist fighters* en haatpropagandisten (beperkte verspreiding) (MO GGB). De Vaste Comités I en P legden zich in dit onderzoek eerder toe op de oprichting en voeding van de gemeenschappelijke gegevensbank *Terrorist Fighters* (GGB TF).

I.10.2. HET OCAD EN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN

Na de aanslagen in 2016, werd met Wet van 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme een wijziging aangebracht in de Wet van 5 augustus 1992 op het Politieambt (WPA) om een wettelijk basis te voorzien voor de oprichting van een gemeenschappelijke gegevensbank met het oog op de preventie en de strijd tegen het terrorisme en het extremisme dat tot terrorisme kan leiden.

Met het KB GGB werd de gemeenschappelijke gegevensbank *foreign terrorist fighters* in het leven geroepen. Met een wijzigingsbesluit van 23 april 2018 werd deze databank omgedoopt tot de gemeenschappelijke gegevensbank *terrorist fighters* (GGB TF) omwille van de toevoeging van een nieuwe categorie *homegrown terrorist fighters* naast de reeds bestaande categorie van *foreign terrorist fighters*. Daarnaast werd met een nieuw koninklijk besluit van dezelfde datum een

---

[107] De verschillende dreigingsniveaus zijn:
- het " Niveau 1 of LAAG " indien blijkt dat de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse niet bedreigd is;
- het " Niveau 2 of GEMIDDELD " indien blijkt dat de dreiging tegen de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse weinig waarschijnlijk is;
- het " Niveau 3 of ERNSTIG " indien blijkt dat de dreiging tegen de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse mogelijk en waarschijnlijk is;
- het " Niveau 4 of ZEER ERNSTIG " indien blijkt dat de dreiging tegen de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse ernstig en zeer nabij is.

onderscheiden gemeenschappelijke gegevensbank voor haatpropagandisten (GGB HP) opgericht.[108]

Ten slotte werden, met het koninklijk esluit van 20 december 2019 twee nieuwe categorieën toegevoegd aan de gemeenschappelijke gegevensbank *terrorist fighters*, m.n. de potentieel gewelddadige extremisten en de terrorismeveroordeelden.[109] In toepassing van het KB FTF en de wijzigingsbesluiten van 2018 en 2019, beoogt de gemeenschappelijke gegevensbank *terrorist fighters* de opvolging van de *foreign terrorist fighters* (FTF), de *homegrown terrorist fighters* (HTF), de potentieel gewelddadige extremisten (PGE) en de terrorismeveroordeelden (TV).

In de lijn van het achterliggende idee om aan informatie-uitwisseling te doen, voorziet de wet in een verplichting tot het voeden van de GGB voor de diensten die een directe toegang hebben tot de gegevensbanken. De gegevens over een in de GGB-geregistreerde entiteit moeten immers voortdurend worden bijgewerkt. Vandaar dat de GGB een dynamische databank wordt genoemd. Enkel de basisdiensten (OCAD, VSSE, ADIV en de geïntegreerde politie) kunnen een nieuwe entiteit en, na validatie van het OCAD, iemand in vooronderzoek plaatsen en dit voor een periode van maximaal zes maanden. Voor elke geregistreerde entiteit waken de diensten die rechtstreeks toegang hebben tot de GGB erover de persoonsgegevens en informatie toe te voegen waarover ze beschikken. De dienst die een persoonsgegeven of een informatie geregistreerd heeft, is de enige die dit persoonsgegeven of deze informatie kan wijzigen, verbeteren of uitwissen.

Als verantwoordelijke voor het operationeel beheer van de GGB, is het OCAD belast de beoordeling van de gegevens van de inlichtingenfiche (*infra*) en het valideren van een entiteit in de GGB op basis van de beschikbare informatie.

---

108 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 1bis "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 en het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt, *BS* 30 mei 2018.

109 Koninklijk besluit van 20 december 2019 tot wijziging van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters, *BS* 27 januari 2020.

I.10.2.1. De inschrijvingsprocedure

De inschrijvingsprocedure voor de categorie potentieel gewelddadige extremisten (PGE)[110], toegevoegd door het KB van 20 december 2019, en waarin Jürgen Conings was opgenomen, werd uitgewerkt in de omzendbrief van de minister van Veiligheid en Binnenlandse Zaken en de minister van Justitie aangaande de uitwisseling van informatie en de opvolging van TF en HP (MO GGB).[111] Terwijl de omzendbrief de informatie-uitwisseling beschrijft aangaande de categorieën FTF, HTF en HP, wordt deze naar analogie toegepast op de potentieel gewelddadige extremisten.

De fase van 'vooronderzoek' (de zgn. 'verrijkingsfase') heeft tot doel de inzameling van gegevens en informatie, *à charge et à décharge*, die nodig zijn om een entiteit als PGE al dan niet te valideren. De MO GGB moedigt de diensten aan om, in de schoot van de LTF's en in het kader van hun respectievelijke wettelijke opdrachten, samen de strategie van informatiegaring te bepalen met het oog op het verrijken van de inlichtingen ('wie doet wat'). Na afloop van deze periode, dewelke maximaal zes maanden kan duren) zal het OCAD, op basis van de beschikbare informatie/inlichtingen, evalueren of de wettelijke criteria al dan niet vervuld zijn. Indien deze niet vervuld zijn, worden de gegevens van de persoon in vooronderzoek automatisch geschrapt.

Conform aan wat werd bepaald in de MO GGB, bestaat de GGB uit inlichtingenfiches dewelke niet-geclassificeerde persoonsgegevens en informatie bevatten afkomstig van alle diensten die de GGB voeden. Deze fiches moeten het mogelijk maken niet alleen de mogelijk potentiële dreiging te beoordelen die deze entiteiten vertonen, maar voornamelijk er een opvolging van te verzekeren met het oog op

---

110 De categorie potentieel gewelddadige extremisten, behelst de natuurlijke personen die een aanknopingspunt met België hebben en die voldoen aan volgende cumulatieve criteria:
a) ze hebben extremistische opvattingen die het gebruik van geweld of dwang als actiemethode in België legitimeren;
b) er zijn betrouwbare aanwijzingen dat ze de intentie hebben om geweld te gebruiken, en dit in verband met de opvattingen vermeld in a);
c) ze voldoen aan minstens een van de volgende criteria die het risico op geweldpleging verhogen: 1) ze hebben systematisch sociale contacten binnen extremistische milieus; 2) ze hebben een psychische problematiek, vastgesteld door een daartoe gekwalificeerde deskundige; 3) ze pleegden daden of stelden antecedenten die beschouwd kunnen worden als ofwel a) een misdaad of wanbedrijf die de fysieke of psychische integriteit van derden aantast of bedreigt; ofwel b) onderrichtingen of een opleiding voor de vervaardiging of het gebruik van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, dan wel voor andere specifieke methoden en technieken nuttig voor het plegen van terroristische misdrijven bedoeld in artikel 137 van het Strafwetboek, ofwel c) bewuste handelingen die als materiële steun voor een terroristische/extremistische organisatie of netwerk gelden; ofwel d) feiten die door hun aard wijzen op een verontrustend veiligheidsbewustzijn in hoofde van betrokkene.

111 De algemene doelstelling van de omzendbrief is *"vanuit een veiligheidsobjectief de informatiehuishouding, het nemen van maatregelen en de gecoördineerde samenwerking tussen de diensten regelen en dit met het oog om de openbare veiligheid tegen de potentiële dreiging maximaal te beschermen door het verstoren van bedreigende activiteiten uitgaande van de Terrorist Fighters (FTF/HTF) en Haatpropagandisten (HP)."*

het anticiperen en het verhinderen van mogelijke terroristische acties. Eenmaal het statuut in de gegevensbank werd gevalideerd, maakt het OCAD een individuele dreigingsevaluatie op, daarbij rekening houdend met alle pertinente informatie waarover het beschikt. Deze evaluatie, die wordt opgenomen in de individuele inlichtingenfiche, zal richtinggevend zijn voor de door te partners te nemen maatregelen.

Om de criteria voor het toekennen van een statuut en de dreigingsanalyse te evalueren, doet het OCAD beroep op zijn eigen risico-evaluatietool RooT37. Op basis van een vaste set, door wetenschappelijk onderzoek onderbouwde, risico-indicatoren wordt een richtinggevende score verkregen. Deze score wordt gecontroleerd door een evaluator van het OCAD, en vervolgens door het 'kwaliteitsteam' binnen het OCAD alvorens een entiteit te kunnen valideren in de GGB.

I.10.2.2. De informatie-uitwisseling met de partners

In het kader van het Plan R(adicalisme)[112] wordt de uitwisseling van informatie georganiseerd in de schoot van de *Lokale Task Forces* (LTF), de beleidsmatige en operationele overlegplatformen van onder meer politie- en inlichtingendiensten binnen de geografische afgebakende zone van het gerechtelijk arrondissement[113], en de lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme (LIVC-R), een gemeentelijk overlegplatform dat moet instaan voor de realisatie van coherente preventieve, repressieve en nazorg-acties. Deze lokale integrale veiligheidscellen zijn, zoals de LTF's, overlegplatformen waar informatie-uitwisseling tussen de sociale- en preventiediensten, de LTF en bestuurlijke autoriteiten moet plaatsvinden inzake radicalisme, extremisme en terrorisme.

Zoals voorgeschreven in de MO GGB, is er voor de LTF een belangrijke rol weggelegd inzake het bepalen van het geheel van veiligheidsmaatregelen. Deze LTF-vergaderingen spelen een cruciale rol bij het prioritiseren en het bepalen van het geheel van veiligheids- en begeleidingsmaatregelen, en dit alles in een geest van onderling overleg.

112 In september 2021 verworden tot 'Strategie Terrorisme en Extremisme' (Strategie TER).

113 Zij verzekeren de opvolging van radicaliserende individuen en groeperingen op lokaal niveau en stellen maatregelen voor om de impact van deze individuen en groepen te reduceren door o.m. informatie, inlichtingen en analyses uit te wisselen en te bespreken.

I.10.3. DE ROL VAN HET OCAD IN DE OPVOLGING VAN JURGEN CONINGS: DE OPNAME IN DE GEMEENSCHAPPELIJKE GEGEVENSBANK

In augustus 2020 opende het OCAD een vooronderzoek PGE over Jürgen Conings. Deze beslissing was gebaseerd op de analyse van sinds juni 2020 door de politie- en inlichtingendiensten doorgestuurde informatie. Het OCAD ging tevens over tot een analyse van zijn activiteiten op de sociale media. De gegevens die werden opgeslagen in de gegevensbank van OCAD, PROTEUS, betroffen voornamelijk door de betrokkene geuitte dreigingen en zijn contacten in het extreemrechtse milieu. Op basis van de beschikbare informatie, waren de Vaste Comités P en I van oordeel dat de opname van betrokkene in vooronderzoek gerechtvaardigd was.

Vanaf de opening van een vooronderzoek bestaat de verplichting voor de basisdiensten om alle relevante informatie naar de GGB te zenden om deze te verrijken. De opvolging dient vanaf dan te gebeuren binnen bevoegde LTF. De analyse van de processen-verbaal van de vergaderingen van deze LTF en van de Werkgroep Extreemrechts (Plan R) bevestigde de agendering van de opvolging van Jürgen Conings vanaf september 2020.

Naar het einde van het vooronderzoek en met behulp van zijn instrument Root37, werd door het OCAD een evaluatie gemaakt van de elementen waarover ze beschikten in het kader van de valideringscriteria zoals omschreven in het KB GGB. Zijn statuut als PGE werd bevestigd en het dreigingsniveau van Jürgen Conings werd ingeschaald op niveau 3 (ernstig). Deze beoordeling werd bevestigd door de evaluator van het OCAD alsook door het kwaliteitsteam halfweg februari 2021.

I.10.4. INFORMATIEUITWISSELING

Het OCAD bracht de verschillende partners van de bevoegde LTF tijdens een vergadering eind februari 2021 op de hoogte van de opname van Jürgen Conings in de gegevensbank alsook van de dreigingsevaluatie. Op deze vergadering was ADIV niet vertegenwoordigd. Het verslag van de vergadering maakt gewag van uitwisseling van informatie over betrokkene.

De opame van Jürgen Conings in de gegevensbank werd onder meer gemeld aan de Federale Politie (voor opname in de ANG), aan BELPIU alsook aan de betrokken LIVC-R (en dus de burgemeester). Het OCAD stuurde evenwel geen bijkomend signaal naar de basisdiensten en de partners aangaande de evaluatie niveau 3 van betrokkene, ervan uitgaande dat de opname in de gegevensbank volstond.

Na zijn opname in de gegevensbank, wordt de opvolging van Jürgen Conings geagendeerd op alle navolgende LTF-vergaderingen en in de Werkgroep Extreem-

rechts, hoewel er niet steeds nieuwe informatie beschikbaar was (*infra*). De enige bijkomende informatie die aan het OCAD werd toegestuurd vóór 17 mei 2021, liet niet toe een wijziging door te voeren aangaande het dreigingsniveau.

Een gevolg van de opname als PGE/niveau 3 in de GGB is dat alle diensten die enkel een toegang *Hit/No Hit* hebben bij consultatie er ook op gewezen worden dat een persoon gekend is. In het geval van Jürgen Conings voerde bijv. de Algemene Directie veiligheid en preventie (ADVP) van de FOD Binnenlandse Zaken een consultatie uit met positief resultaat ("Hit") in het kader van een identificatiekaart als bewakingsagent.

Conform de MO GGB, wordt bij de registratie in de GGB ook een categorie toegekend aan de persoon (A, B of C) die betrekking heeft op de wijze waarop de LTF de persoon verder zal opvolgen. Voor Jürgen Conings werd "B" toegekend, m.n. "dreiging niet extreem groot". De beide Comités wezen op de incoherentie tussen het dreigingsniveau 3 (ernstig) zoals bepaald door het OCAD enerzijds en categorie van opvolging in de LTF anderzijds. Het OCAD preciseerde dat de opvolgingsmaatregelen voor de categorieën A, B en C gelijklopend zijn, maar attendeerde, meer algemeen, op de moeilijke toepassing van de maatregelen zoals voorzien in de MO GGB.[114]

Wat de andere maatregelen betreft zoals de 'aanklampende opvolging' stelt het OCAD vast dat dit ook met de FTF niet altijd even evident is om te realiseren, gelet op het feit dat dit niet afdwingbaar is en dat de MO GGB op het vlak van maatregelen tegen zijn limieten aanloopt. Als er geen inlichtingenonderzoek of strafrechtelijk terrorismeonderzoek kan geopend worden, dan is er niet veel mogelijk. In het geval van Jürgen Conings was er een gerechtelijk onderzoek lopende voor de bedreigingen tegen Marc Van Ranst. Het OCAD stelde dat buiten wat er medegedeeld werd op de LTF, ze geen andere informatie kreeg over het lopende gerechtelijke onderzoek.

Een verder gevolg van het statuut PGE/niveau 3 is dat hij op elke LTF zou besproken worden om te zien welke informatie er naar boven komt en om eventueel te zien of er maatregelen kunnen genomen worden om de dreiging te verminderen. Volgens het OCAD is het evident dat het initiatief bij de ADIV lag, Niettemin werd aan alle diensten een informatie-inspanning gevraagd. Op de LTF-vergaderingen van maart en april 2021 stond betrokkene wel geagendeerd, maar werd hij door geen enkele dienst besproken en werd er dus ook geen informatie gedeeld.

De nota seiningen die werd uitgewerkt door DJSOC/Terro, voorziet voor elke PGE in de ANG in een seining 'discrete controle'. Volgens het OCAD heeft deze maatregel geen resultaat gegeven wat informatie-inwinning betreft, want anders was deze informatie zeker minstens besproken geweest op een LTF.

---

114 Voor het OCAD wil het toekennen van deze categorie B niet zeggen dat er een bijkomende evaluatie gebeurt. De categorie B dient immers ook van dichtbij opgevolgd te worden.

I.10.5. CONCLUSIES

Zich beperkend tot de rol van het OCAD in de opvolging van Jürgen Conings, konden de Vaste Comités I en P de uitwisseling van informatie met het OCAD door de basisdiensten in de fase van het vooronderzoek vanaf augustus 2020 bevestigen. Op basis van deze in PROTEUS geregistreerde informatie en met behulp van het Root37-inistrument, kon het statuut van Jürgen Conings als potentieel gewelddadige extremist worden bevestigd en het dreigingsniveau ingeschaald op niveau 3.

Het is het OCAD dat het initiatief nam om Jürgen Conings eerst in vooronderzoek PGE te zetten en hem vervolgens ook de status PGE/niveau 3 toe te kennen. De Vaste Comités I en P vonden de beslissing tot vooronderzoek gerechtvaardigd.

De dreigingsevaluatie van Jürgen Conings werd verspreid door het OCAD volgens de modaliteiten voorzien in de W.OCAD. Niettegenstaande hij door het OCAD werd ingeschaald op niveau 3 (ernstig), werd hij slechts opgenomen in de categorie B (dreiging niet extreem groot). Beide parameters zijn inderdaad onafhankelijk van mekaar.

I.11. DE OPVOLGING VAN EEN REGERINGSCOMMISSARIS DOOR DE VSSE

Bij koninklijk besluit van 17 mei 2021 werd Ihsane Haouach benoemd als regeringscommissaris bij het Instituut voor de gelijkheid van vrouwen en mannen (IGVM). In die hoedanigheid vertegenwoordigde ze de regering in de raad van bestuur van het IGVM. Ze lag evenwel van bij haar aanstelling onder vuur: eerst omwille van haar hoofddoek, vervolgens omwille van een uitspraak over de scheiding tussen kerk en staat. Op 9 juli 2021 diende Ihsane Haouach haar ontslag in. Dezelfde dag werd in de media gesuggereerd dat een nota van de Veiligheid van de Staat (VSSE) hiervan mogelijks aan de basis zou liggen.[115]

I.11.1. EEN NOTA VAN DE VEILIGHEID VAN DE STAAT

In de loop van 2020 werd door de Analysedienst counterextremisme (CE) van de VSSE een synthesenota opgesteld over de Moslimbroederschap in België.[116] Op het ogenblik van de controverse in de pers omtrent de benoeming van

---

115 B. DEMONTY, *Le Soir*, 9 juli 2021 ('Ihsane Haouach démissionne, le gouvernement en possession d'informations sur de potentiels liens avec les Frères musulmans'). Het rapport in kwestie van de VSSE ('Beperkte verspreiding'/ 'Vertrouwelijk') verscheen ook integraal in de pers (bijv. M. VERBERGT, *De Standaard*, 14 juli 2021 ('Dit zegt de Staatsveiligheid letterlijk over Ihsane Haouach')).

116 Hierover 'I.12. Een vernieuwde aandacht voor de Moslimbroederschap' (*infra*).

Ihsane Haouach als regeringscommissaris, herinnert men zich binnen de VSSE dat haar naam voorkwam in deze synthesenota. Betrokkene vormde geen target van de dienst. Evenwel volgt de VSSE acties ten overstaan van verschillende vormen van extremisme op die als dusdanig passen binnen zijn wettelijke opdrachten (art. 8 W.I&V, 'extremisme').

De VSSE achtte het opportuun de minister van Justitie en de Premier hierover schriftelijk te informeren. Daartoe werd een geclassificeerde nota opgesteld. Ihsane Haouach bleek *'gekend* (is) *omwille van haar nauwe contacten met de Moslimbroeders. Deze contacten tussen de Moslimbroeders en Ihsane Haouach kunnen worden gekaderd binnen een bredere strategie van de Moslimbroeders, waarbij deze proberen te wegen op het publieke debat en de beleidsvorming […]'*. Er werd tevens vermeld dat betrokkene *'voor zover ons bekend zelf geen lid is van de Moslimbroeders en zelf nooit de aandacht heeft getrokken omwille van concrete extremistische stellingnames' […] Het is dan ook niet uit te sluiten dat Ihsane Haouach er zichzelf niet (ten volle) van bewust is dat ze nauwe contacten onderhoudt met de Moslimbroeders. We stellen dan ook voor om de bevoegde Staatssecretaris of haar Beleidscel, net als eventueel mevrouw Haouach zelf, een sensibiliserende briefing aan te bieden'*. [117]

I.11.2. ONDERZOEKSVASTSTELLINGEN

I.11.2.1. Een vernieuwde aandacht voor de Moslimbroederschap (en Ihsane Haouach)?

Niettegenstaande de strijd tegen het terrorisme hoog op de prioriteitenlijst bleef staan, richtte de VSSE haar aandacht de afgelopen jaren opnieuw op andere dossiers. In het kader van de dreigingen 'extremisme' en 'inmenging' werd in 2020 beslist een synthesenota op te stellen over de Moslimbroederschap in België, één van de prioriteiten van de VSSE in haar Actieplan. De naam van Ihsane Haouach kwam in het kader van deze nota voor als een persoon die, al dan niet bewust, in contact stond met deze beweging. De betrokkene was echter geen doelwit van de VSSE.

Via (de beroering in) de pers vernam de VSSE de benoeming van Ishane Haouach als regeringscommissaris. De dienst nam zelf het initiatief om een nota op te stellen, omdat hij van mening was dat de minister van Justitie in kennis moest worden gesteld van het feit dat de betrokkene bekend was in het kader van de opvolging van de wettelijke bevoegdheden in verband met extremisme. Aangezien niet kon worden uitgesloten dat ze niet (volledig) op de hoogte was van haar nauwe banden met de Moslimbroederschap, werd voorgesteld dat de minister een sensibiliserende briefing organiseerde voor de bevoegde staatssecretaris of haar beleidscel, net als voor Ihsane Haouach zelf in een later stadium.

---

117 Citaat uit de in de pers (M. VERBERGT, *l.c.*) gepubliceerde vertrouwelijke nota van de VSSE.

I.11.2.2. Het zorgvuldigheidsbeginsel

In een inlichtingencontext is er weinig zekerheid, en daar moet rekening mee worden gehouden bij de beslissing of en hoe informatie moet worden verstrekt (in dit geval aan de minister van Justitie). Het Comité had eerder verklaard dat "*wil de openbaarmaking van informatie als rechtmatig worden beschouwd, zij voldoende moet worden gestaafd door betrouwbare informatie. Het moet ook met zorg worden geformuleerd. Er kan bijvoorbeeld geen ongenuanceerd beeld worden gegeven van de onderliggende informatie, of een bepaald item kan worden gepresenteerd als een "beeld van" of een "indruk van". In die zin moet de verstrekte informatie ook "accuraat" zijn door een objectief beeld te geven van het beeld dat de inlichtingendienst heeft van de dreiging en de rol van de betrokkene, zonder "manipulatief" te zijn [...]*".[118] Het Comité was van oordeel dat de nota in overeenstemming was met het voormelde voorzorgsprincipe en dat de VSSE in haar mededeling aan de regering voldoende had uitgelegd waarom de banden van de regeringscommissaris met de Moslimbroederschap een bedreiging zouden kunnen vormen.

Hoewel een schriftelijke nota werd voorbereid, werd besloten deze niet meteen te verzenden. De VSSE was zich ervan bewust dat de nota politiek gevoelig en onvolledig was, en dat hij niet mocht uitlekken. Er werd besloten de minister van Justitie mondeling in te lichten, maar het onderhoud vond niet plaats. In artikel 19 W.I&V is niet bepaald hoe de informatie door de VSSE moet worden verstrekt. In het verleden was het Comité van mening dat de mededeling om redenen van rechtszekerheid (behalve in uiterst dringende gevallen) schriftelijk diende te geschieden, om latere discussies te voorkomen en parlementaire (of zelfs juridische) controle mogelijk te maken. De bevoegde staatssecretaris werd niet rechtstreeks ingelicht. De VSSE ging ervan uit dat de Premier of minister van Justitie dat zou doen.

I.11.2.3. Geen verdere onderzoeksbevindingen?

De VSSE was zich bewust van de politieke gevoeligheid van de benoemingskwestie, niet het minst na de plenaire zitting begin juni 2021 in het Parlement. Er werd echter besloten te wachten met de verzending van de nota op de bevestiging van de erin vervatte elementen. De nota werd uiteindelijk meer dan een maand ingehouden, omdat de VSSE niet wou geïnstrumentaliseerd worden. Niettemin leek het erop dat er geen wijzigingen werden aangebracht in de nota die uiteindelijk in juli aan de Premier, de Vice-eersteministers en de minister van Binnenlandse Zaken werd toegezonden. Met andere woorden, er waren geen verdere onderzoeksbevindingen.

---

118 VAST COMITÉ I, Toezichtonderzoek naar de manier waarop de Belgische inlichtingendiensten communiceren met een private of publieke werkgever over een werknemer, 2020.

Op basis van de resultaten van het onderzoek kon het Comité zich niet uitspreken over een oorzakelijk verband tussen de nota en het ontslag van regeringscommissaris Ishane Haouach.

I.11.2.4. Het lekken van een geclassificeerde nota

De nota over Ihsane Haouach werd geclassificeerd als "Vertrouwelijk Wet 11.12.1998". Hij werd evenwel volledig in de pers gepubliceerd, nauwelijks een dag nadat de nota werd toegezonden aan de Premier, de Vice-eersteministers en de minister van Binnenlandse Zaken. Aangezien het strafbaar is om een geclassificeerd document aan een derde te overhandigen, diende de VSSE, terecht aldus het Comité, een klacht tegen onbekenden bij het Brusselse parket.

Het Vast Comité I herinnerde eraan dat het de verantwoordelijkheid is van de veiligheidsofficieren in de verschillende ministeriële kabinetten om toe te zien op het correcte gebruik van geclassificeerde documenten. Ook ontvangers van geclassificeerde nota's dienen uiterst voorzichtig te zijn met deze informatie. In de eerste plaats moeten zij zich ervan bewust zijn dat de overdracht aan een onbevoegde derde een strafbaar feit is. Ten tweede kan het schade toebrengen aan de personen op wie de nota betrekking heeft. Ten derde is het schadelijk voor de inlichtingen- en veiligheidsdiensten zelf en ondermijnt het terechte vertrouwen van het publiek in deze diensten.

I.11.2.5. Een 'verstoringsactie'?

In de nota aan de minister van Justitie wordt voorgesteld een 'bewustmakingsbriefing' te organiseren voor Ihsane Haouach. Het onderliggende doel was tweeledig. Het was niet uitgesloten dat betrokkene zelf niet (volledig) op de hoogte was van haar nauwe banden met de Moslimbroederschap, in welk geval bewustmaking noodzakelijk/nuttig was. Indien zij echter op de hoogte was, kon het doel van een dergelijke briefing zijn een ontwrichtend (in dit geval 'afschrikkend') effect te bewerkstelligen. In dit verband verklaarde de VSSE dat zij voornemens was in de toekomst een disruptieve aanpak te realiseren door procedures en samenwerkingsovereenkomsten te ontwikkelen. De vraag die rees was of het initiatief om te verstoren van een inlichtingen- en veiligheidsdienst moet/kan komen. Deze kwestie, evenals de naleving van de dienstnota 'disruptie' (er was uiteindelijk geen verstoring), was niet het voorwerp van onderzoek.

I.11.2.6. De noodzaak van een screening voor functies met een openbaar karakter?

Nam de VSSE het (spontane) initiatief om de regering in te lichten toen zij kennis nam van de benoeming van Ihsane Haouach tot regeringscommissaris, of moest zij dat doen? Geldt dit ook voor andere openbare functies?[119] En kan iedereen worden gecontroleerd of is een uittreksel uit het strafregister (vroeger de verklaring van goed gedrag) voldoende? De VSSE controleert niet systematisch elke benoeming van een regeringscommissaris of een ander openbaar ambt. Het is juist dat in de loop van de door de dienst verrichte onderzoeken van tijd tot tijd een persoon opduikt die een openbaar ambt bekleedt. In dergelijke gevallen moet worden overwogen of over deze persoon een nota moet worden geschreven. De VSSE wordt in dit verband niet verzocht systematisch advies uit te brengen. Dit is een besluit dat, indien nodig, op politiek niveau moet worden genomen.[120]

Het risico van instrumentalisering moet altijd in gedachten worden gehouden wanneer een politiek gevoelig onderwerp wordt behandeld. De structuur van de nota's moet hieraan worden aangepast (hieraan wordt nog gewerkt): de analisten moeten uitleggen wat het doel van een nota is, wat de leemten zijn, wat moet worden verduidelijkt, aan wie de nota moet worden verstrekt, enz.

I.12. EEN VERNIEUWDE AANDACHT VOOR DE MOSLIMBROEDERSCHAP

Op 19 juli 2021 verzocht de Begeleidingscommissie het Vast Comité I een toezichtonderzoek te openen met als doel enerzijds te bepalen of de Moslimbroederschap wordt opgevolgd door de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) en, anderzijds, of deze beweging volgens de inlichtingendiensten een bedreiging vormt in België.[121] Het onderzoek volgde op het toezichtonderzoek naar de wijze waarop de VSSE de toenmalige regeringscommissaris, Ihsane Haouach, had opgevolgd (zie I.11).

---

119 Zie in die zin de problemen in verband met de benoeming/verwijdering van Salah ECHALLOUI uit de Grote Moskee van Brussel en de moslimexecutieve (negatief advies van de VSSE).

120 *Cf.* de geclassificeerde nota (VERTROUWELIJK Wet 11.12.1998) van de VSSE van 25 augustus 2021 gericht aan de Voorzitter van het Vast Comité I.

121 Het Vast Comité I voerde eerder al twee toezichtonderzoeken ter zake: In 2001 naar de manier waarop de inlichtingendiensten informatie over terrorisme en de radicale islam verzamelden en analyseerden, alsook naar de manier waarop zij de burgerlijke en gerechtelijke autoriteiten informeerden over dit fenomeen. Dit onderzoek had met name betrekking op de aanwezigheid van de Moslimbroeders in België en op de opvolging daarvan door de VSSE (VAST COMITÉ I, *Activiteitenverslag 2001*, 89-143). In 2007 voerde het Comité een onderzoek om na te gaan of de geformuleerde aanbevelingen (opvolging van de radicale islam) door de inlichtingendiensten, waren opgevolgd (VAST COMITÉ I, *Activiteitenverslag 2007*, 7-29).

I.12.1. DE MOSLIMBROEDERS: CONTEXTUALISERING

I.12.1.1. Ontstaan en internationalisering van de beweging

De wortels van de Moslimbroederschap (afgekort 'de Moslimbroeders') liggen in Egypte, waar de beweging in 1928 werd opgericht door Hassan Al-Banna. Bij haar ontstaan heeft de organisatie twee doelstellingen: Egypte bevrijden van de Britse overheersing en de waarden van de islam opnieuw invoeren in de Egyptische samenleving. In 1948 wordt de beweging in Egypte verboden na een reeks confrontaties tussen een deel van de beweging en de overheid. Zeer snel na haar ontstaan internationaliseert de beweging als gevolg van de ballingschap van meerdere politieke leiders. In België zijn de Moslimbroeders aanwezig sinds de jaren 1960 waar ze zich geleidelijk aan engageerden in sociale, religieuze en jeugdactiviteiten.

I.12.1.2. De omvang van het fenomeen in België?

Om de omvang van een fenomeen te kunnen bepalen, is het noodzakelijk dit duidelijk te definiëren. Het Vast Comité I kon vaststellen dat de term 'Moslimbroeders' zich moeilijk laat definiëren en dat er geen precieze definitie bestaat die algemeen wordt aanvaard door de Belgische inlichtingendiensten en de partners van de strafrechtelijke keten in de ruime betekenis. Het gaat om een entiteit met vage omtrekken, met antennes die grote autonomie genieten in vele landen en die de vorm aannemen van verschillende organisaties die op discrete of zelfs geheime wijze handelen binnen diverse domeinen van de samenleving, met doelstellingen op lange termijn die onverenigbaar zijn met de democratische orde. Aangezien het erg moeilijk is om deze beweging duidelijk te omschrijven, is de studie ervan – en meer bepaald de analyse van haar aanwezigheid en beïnvloedingsmacht in België – bijzonder ingewikkeld. Het is ook zeer moeilijk om te bepalen of een persoon al dan niet deel uitmaakt van deze groepering, aangezien deze laatste als zodanig niet over duidelijke structuren beschikt en geen lidkaarten verdeelt.[122]

[122] Het Comité had al op deze moeilijkheid gewezen in zijn activiteitenverslag 2001 (cf. VAST COMITÉ I, *Activiteitenverslag 2001*, p.113.)

De VSSE maakte echter de volgende raming van de aanwezigheid van deze beweging in België: "*De 'internationale moslimbroeders' in ons land worden vertegenwoordigd door de Ligue des Musulmans de Belgique (LMB), die naar schatting een 50-tal leden telt en enkele honderden aanhangers of sympathisanten. Bij ons bevindt zich ook het hoofdkwartier van een Europese koepelvereniging, de Council of European Muslims (CEM; voordien FIOE) die de belangen verdedigt van de moslimbroeders ten aanzien van de Europese instellingen.*"[123]

Op basis van deze cijfers kwalificeerde de minister van Justitie de aanwezigheid van de beweging in België als 'vrij bescheiden'.[124] Niettemin stelden de minister en de VSSE dat de Moslimbroeders "*invloedrijker zijn en belangrijker lijken dan men zou verwachten op basis van hun beperkte ledenaantal*", als gevolg van hun intense sociale en politieke activisme, hun benadering en het profiel van hun leden.[125]

I.12.1.3. Een beweging die in het buitenland als een bedreiging wordt beschouwd?

De verschillende landen nemen sterk uiteenlopende posities in met betrekking tot deze beweging. In sommige landen behoren politieke partijen die beweren deel uit te maken van de Moslimbroederschap tot de regering of de oppositie in het parlement (bijv. Turkije, Marokko, Algerije, Libië). In andere landen wordt de beweging beschouwd als een criminele organisatie.[126] Met de goedkeuring van de nieuwe Antiterrorismewet van 8 juli 2021 is Oostenrijk het eerste Europese land dat de Moslimbroeders verbiedt als organisatie omwille van hun 'religieus geïnspireerde

123 VSSE, *Jaarrapport 2020,* p. 13.

124 Antwoord van de vice-eersteminister en minister van Justitie en Noordzee d.d. 10 mei 2021 op schriftelijke vraag nr. 7 – 1140 van senator Tom ONGENA van 5 maart 2021.

125 *Ibid*.; VSSE, *Jaarrapport 2020*, p. 13.

126 In Egypte, Rusland, Saoedi-Arabië, de Verenigde Arabische Emiraten en ook in Bahrein wordt ze officieel beschouwd als een terroristische organisatie.

criminaliteit'. Hoewel de beweging in andere Europese landen niet verboden is, wordt er recent de nodige aandacht aan besteed in onze buurlanden.[127]

I.12.2. ONDERZOEKSVASTSTELLINGEN

I.12.2.1. Maakt de beweging voorwerp van opvolging uit door de inlichtingendiensten?

Beide inlichtingendiensten volgen de Moslimbroeders op, zij het vanuit zeer verschillende invalshoeken en met de inzet van zeer verschillende middelen.

De VSSE volgt de beweging prioritair op in het kader van haar bevoegdheid inzake de opvolging van extremisme (art. 7, 1° en art. 8, 1°, c W.I&V) en conform de 'Strategische doelstellingen 2021-2024'[128] en de akkoorden afgesloten met de

---

127 In Nederland werd er in 2019-2020, op initiatief van het parlement, een onderzoek gevoerd naar de invloed die bepaalde buitenlandse staten uitoefenen in het kielzog van de Moslimbroeders, inzonderheid in een poging hun democratie een andere richting uit te sturen. Tweede Kamer der Staten-Generaal, (*On)zichtbare invloed, Verslag parlementaire ondervragingscommissie naar ongewenste beïnvloeding uit onvrije landen*, Den Haag, 25 juni 2020, beschikbaar online: https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z12034&did=2020D25817 De resultaten van deze studie bevestigen dat er sprake is van uitoefening – in diverse vormen – van invloed door meerdere bewegingen, waaronder die van de Moslimbroeders, in het land. Het onderzoek verwijst naar meerdere studies die de Nederlandse inlichtingendienst, i.e. de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), in verband met de Moslimbroeders heeft gevoerd. De AIVD kwam in 2011 tot het besluit dat er van de Moslimbroeders geen directe dreiging uitging voor de democratie of de nationale veiligheid, maar dat de activiteiten van de beweging op lange termijn een risico konden vormen, aangezien de Moslimbroeders antidemocratisch zijn en gekant tegen het integratieproces.
De aanwezigheid van de beweging in Frankrijk en de bedreiging die ze er vertegenwoordigt, werden eveneens bestudeerd in het kader van een onderzoekscommissie van de Franse Senaat die in november 2019 een onderzoek voerde naar '*de antwoorden vanwege de autoriteiten op de ontwikkeling van de radicale islam en de middelen om die te bestrijden*' (vrij vertaald) Verslag nr. 595 (2019-2020), 7 juli 2020, nr. 595, beschikbaar online: https://www.senat.fr/rap/r19-595-1/r19-595-1_mono.html#toc62 In het verslag, dat in juli 2020 werd gepubliceerd, staat dat de Broederschap in Frankrijk ca. 50.000 leden telt.
In Duitsland blijkt uit de antwoorden van de federale regering op meerdere parlementaire vragen dat organisaties die banden onderhouden met de Moslimbroeders in het oog worden gehouden door de nationale veiligheidsdienst, i.e. de *Bundesambt für Verfassungsschutz* (BfV), en door alle bureaus van de deelstaten (*Ländesamts für Verfassungsschutz)*. Er werd vastgesteld dat het aantal leden en sympathisanten van de Moslimbroederschap in het land is gestegen, van 1.040 in 2018 tot 1.350, in: Bundesamt für Verfassungsschutz, *Verfassungsschutzbericht 2019*, www.verfassungsschutz.de/SharedDocs/publikationen/DE/2020/verfassungsschutzbericht-2019.pdf?_blob=publicationFile&v=10, pp. 180-181.

128 Er wordt vermeld dat de strijd tegen terrorisme een prioriteit blijft, maar dat de VSSE beoogt om de aandacht ook meer te vestigen op andere dossiers. Hiertoe zal de VSSE de beschikbare personeelsleden en middelen herverdelen, rekening houdend met de actuele dreiging.

ADIV.[129] De VSSE verzamelt informatie over de Moslimbroeders, de organisaties en de personen die ermee zijn verbonden, inzonderheid door middel van gewone inlichtingenmethoden (meer bepaald menselijke bronnen), maar ook met behulp van bijzondere inlichtingenmethoden. Hieruit worden inlichtingen geëxtraheerd die vervolgens worden verspreid naar de overheden en partners ter informatie en sensibilisatie. De problematiek wordt op de voet gevolgd en de capaciteiten werden herverdeeld voor de uitoefening van deze opdracht.[130]

De ADIV op zijn beurt bestudeert de beweging enkel in het kader van de invloed die deze zou kunnen uitoefenen binnen Defensie en dit conform zijn bevoegdheden (art. 11 W.I&V) en de strategische plannen. De dienst doet aan actieve monitoring door informatie te ontvangen die derden produceren, maar verzamelt zelf geen informatie – op proactieve wijze – over de beweging in haar geheel. Na afloop van het onderzoek was het moeilijk zich uit te spreken over de kwaliteit van de informatiepositie van de ADIV. Het is duidelijk dat de voor de verzameling en analyse ingezette middelen minder omvangrijk zijn dan die van de VSSE aangezien dat – in tegenstelling tot de VSSE die het fenomeen in zijn geheel opvolgt – de ADIV de beweging alleen bestudeert in het kader van de invloed die zij zou kunnen uitoefenen binnen Defensie. Het Comité stelde echter vast dat het niveau van prioriteit dat de ADIV toekent aan de opvolging van het fenomeen niet overeenstemt met de middelen die deze dienst inzet om gegevens te verzamelen en te analyseren. Ten slotte stelt het Comité op basis van de verkregen informatie vast dat de ADIV geen inlichtingen met betrekking tot de Moslimbroeders op eigen initiatief heeft meegedeeld aan de overheden of partners tijdens de afgelopen drie jaren.

I.12.2.2. Wordt de beweging geïdentificeerd als een bedreiging voor België?

De VSSE en de ADIV komen tot gelijkaardige conclusies. Er wordt geen bedreiging tegen een specifieke instelling geïdentificeerd die rechtstreeks verbonden is met de Moslimbroeders. Niettemin omschrijft de VSSE de Moslimbroeders als een extremistische beweging[131]en beschouwt ze de beweging van de Moslimbroeders als een hoge en prioritaire dreiging die aanleiding zou kunnen geven tot antidemocratische gedragingen, tot polarisering of nog, tot schending van fundamentele rechten. De VSSE verduidelijkt: "*Ogenschijnlijk respecteren de Moslimbroeders*

---

129 De akkoorden tussen de VSSE en de ADIV leggen vast dat binnen de domeinen van terrorisme, radicalisme en extremisme, de VSSE over een algemene bevoegdheid beschikt in België, en de ADIV over een bevoegdheid beperkt tot de aspecten van terrorisme en extremisme die betrekking hebben tot de militaire belangen of Belgische militairen.

130 In het dossier werd kort voor 2020 opnieuw geïnvesteerd nadat capaciteiten, tot dusver ingezet op dossiers 'terrorisme en extremisme', werden vrijgegeven.

131 Onder extremisme wordt verstaan "*racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat*" (art. 8, 1°, c W.I&V).

de democratische en wettelijke regels. Op korte termijn streven ze ook doelstellingen na die legitiem lijken. Maar hun intern discours en hun visie en doelstellingen op langere termijn staan haaks op de goede werking van de grondwettelijke orde en democratie."[132] "*Het geijkte middel daartoe is proselitisme ('dawa'), onder meer via prediking en (religieus) onderwijs. De Moslimbroeders beschouwen zichzelf daarbij als een elitaire voorhoede die de verschillende moslimgemeenschappen moet verenigen en leiden. Ze streven ernaar om maatschappelijk invloedrijke posities in te nemen, om zo de westerse samenleving van binnenuit te kunnen veranderen. Bovendien trachten ze op verschillende manieren het overheidsbeleid te beïnvloeden.*"[133]

De ADIV is van oordeel dat: "*Les Frères musulmans promeuvent par certains aspects une vision extrémiste de la religion. Ils représentent un danger en ce qu'ils militent activement, et souvent de façon non transparente, en faveur d'une vision identitaire de l'Islam et renforcent ainsi les clivages au sein de la société et des institutions.*"[134] De ADIV stelt ook nog dat de dienst bijzonder oplettend is voor het risico van infiltratie van de Moslimbroeders binnen Defensie.[135] Het was voor het Comité onbekend of het risico op entrisme hoog ingeschat werd door de ADIV.

I.12.2.3. Samenwerking

I.12.2.3.1. Samenwerking tussen de inlichtingendiensten

In de loop van het onderzoek kon worden vastgesteld dat beide Belgische inlichtingendiensten zowel bilateraal als multilateraal inlichtingen over het Moslimbroederschap uitwisselden met buitenlandse inlichtingendiensten.

Op nationaal niveau, diende te worden vastgesteld dat de samenwerking vooral een éénrichtingsverkeer betrof, te weten het delen van informatie door de VSSE met de ADIV.

I.12.2.3.2. Samenwerking met het OCAD

Gelet op de kwalificatie en het dreigingsniveau zoals toegekend door de VSSE, wenste het Comité na te gaan – zonder zich te verliezen in de details – of ook het OCAD de Moslimbroederschap bestudeert.[136]. Hierover bevraagd, antwoordde

---

132 *Ibid.*, p. 13.

133 *Ibid.*, p. 12.

134 "*De Moslimbroeders promoten door bepaalde aspecten een extremistische visie van religie. Ze vormen een gevaar daar ze actief militeren, en vaak op ondoorzichtige wijze, voor een identitaire visie van de islam en versterken aldus de breuklijnen die bestaan binnen de samenleving en de instellingen*" (vrij vertaald). *Ibid*.

135 Nota van de ADIV van 26 augustus 2021 aan de voorzitter van het Vast Comité I.

136 Het OCAD is immers bevoegd voor de evaluatie van de dreiging inzake extremisme wanneer deze dreiging de inwendige en uitwendige veiligheid van de Staat, de Belgische belangen en de veiligheid van de Belgische onderdanen in het buitenland of elk ander fundamenteel belang van het land zou kunnen aantasten (art. 3 W.OCAD).

het OCAD dat het nooit een nota of een studie had geschreven met betrekking tot de Moslimbroeders. Het OCAD identificeert bovendien geen rechtstreekse dreiging die deze beweging voor België vormt en heeft het dus niet over een dreiging op korte of middellange termijn of bevestigt evenmin het hoge niveau van de dreiging, in tegenstelling tot de analyse van beide inlichtingendiensten.

Geïnterpelleerd door het ontbreken van een gezamenlijke visie tussen enerzijds de VSSE en de ADIV en anderzijds het OCAD wat betreft de dreiging die de Moslimbroeders vertegenwoordigen, concludeerde het Comité dat een overleg tussen deze diensten noodzakelijk is. Het Comité verbaasde zich erover dat dit overleg nog niet had plaatsgevonden, gelet op de prioriteit die de VSSE en de ADIV aan dit dossier toekennen.

I.12.2.4. Welke strategieën hanteren de inlichtingendiensten om de geïdentificeerde dreiging in te dammen?

Om te strijden tegen de strategie van de Moslimbroeders en te vermijden dat de beweging de positie kan innemen van bemiddelaar tussen de moslimgemeenschappen en overheden, is de VSSE van mening dat het van groot belang is om te investeren in sensibilisering van de overheden en de administraties. De reeds genomen en toekomstige initiatieven getuigden dat deze strategie wordt gevolgd door de Veiligheid van de Staat. De dienst heeft twee nota's verspreid; één bestemd voor de inlichtingendiensten en de geassocieerde partners van de strafrechtsketen, de andere voor de bevoegde ministers, met als doel te informeren en te sensibiliseren.

De ADIV stelt dat de bewustmaking van de institutionele actoren voor de pogingen tot beïnvloeding door de Moslimbroeders buiten België deel uitmaakt van de doelstellingen van de briefings die door hen worden gegeven in verband met de terroristische dreiging en het risico dat verbonden is aan radicale religieuze bewegingen. Het Comité beschikt over geen bijkomende informatie op basis waarvan het zich kan uitspreken over de kwantiteit of de kwaliteit van deze bewustmakingsbriefings.

Het Comité is van mening dat deze sensibiliseringsstrategie versterkt kan worden door het organiseren van een structureel overleg tussen de inlichtingendiensten en hun partners (onder andere het OCAD) aangaande deze thematiek. Het sensibiliseren van de politieke overheden en de administraties zal meer effectief zijn als dit wordt gedragen door de drie diensten die voorafgaand overeenstemming hebben bereikt over een gezamenlijke definitie van het fenomeen, zijn samenstellende delen, en de dreiging die ze vertegenwoordigt voor België.

I.13. INFORMATIE- EN COMMUNICATIETECHNOLOGIE IN HET INLICHTINGENPROCES BIJ DE DIRECTIE CYBER VAN DE ADIV EN BIJ DE VSSE

I.13.1. DE *CORE BUSINESS* VAN EEN INLICHTINGENDIENST

Informatie-en communicatietechnologieën (ICT) spelen een steeds belangrijkere rol in de inlichtingenprocessen, zowel bij het verzamelen en de analyse van de basisinformatie als bij de verspreiding van de inlichtingen. De informatie is afkomstig van steeds grotere gegevensstromen, ongeacht de bron. Informatie kan afkomstig zijn van menselijke bronnen (Humint), van partners of van digitale bronnen zoals met name open bronnen of *open sources* (Osint), afluisteroperaties (Sigint) of beeldmateriaal (GeoInt)… De constante groei van de gegevensstromen vereist passende systemen die geschikt zijn om die stromen te absorberen en om een correcte, snelle en doeltreffende analyse mogelijk te maken. De informatica-omgeving moet dus een stabiele en toekomstgerichte tool zijn die ondersteuning kan bieden aan de verschillende actoren die een rol spelen in de inlichtingencyclus. Deze omgeving, zowel de *hardware* als de *software*, moet beantwoorden aan de normen ter zake en de goede IT-praktijken, en moet tegelijk rekening houden met de nieuwe en toekomstige technologische ontwikkelingen[137] zoals 'big data'.[138]

In eerdere onderzoeken stelde het Vast Comité I vast dat de inlichtingendiensten het hoofd moeten bieden aan grote uitdagingen in dit domein. Vooral wat betreft de ADIV is in het verleden al gebleken dat ICT een teer punt is. Het Comité stelde vast dat de inlichtingenactiviteiten niet (langer) voldoende werden ondersteund door ICT. De voorwaarden voor een goed beheer van de informatie werden niet (langer) volledig vervuld.[139] [140]

Daarop startte het Vast Comité I in mei 2019 een 'Toezichtonderzoek betreffende de informaticamiddelen die de Belgische inlichtingendiensten gebruiken om

---

137 Ook voor de toezichthouders is op dat vlak een belangrijke rol weggelegd. Hierover: K. VIETH en T. WETZLING, *Data-driven Intelligence Oversight. Recommendations for a System Update*, Stiftung Neue Verantwortung, November 2019, 63 p.

138 Het begrip '*big data*' verwijst naar de wetenschap van het verzamelen en analyseren van grote volumes gegevens met als doel bepaalde interessante '*patterns*' te ontdekken op basis van een rangschikking ('*clustering*') en statistische analyses die zo hulp kunnen bieden bij de besluitvorming. Deze gegevens worden gewoonlijk gekenmerkt door een grote verscheidenheid, een grote snelheid en een groot volume.

139 VAST COMITÉ I, *Activiteitenverslag 2011*, 7-14 ('II.1. Een audit bij de militaire inlichtingendienst'); *Activiteitenverslag 2018*, 2-18 ('I.1. De werking van de Directie Counterintelligence (CI) van de ADIV').

140 Ook werd in het verslag van de parlementaire onderzoekscommissie naar de aanslagen in Zaventem en Maalbeek de aanbeveling geformuleerd om het informatiebeheer van de diensten te verbeteren om meer bepaald de 'infobesitas' onder controle te houden. Zie 'Onderzoekscommissie naar de terroristische aanslagen van 22 maart 2016. *Parl. St.* Kamer, 2016-2017, nr. 54-1752/008, 15 juni 2017, p. 53 en 180 e.v.

informatie te verzamelen, te analyseren en te communiceren in het kader van de inlichtingencyclus'. Het onderzoek spitste zich toe op de informaticamiddelen die specifiek worden gebruikt ter ondersteuning van de inlichtingencyclus. Het gaat om systemen die worden gehanteerd om gegevens te verzamelen of ook om specifieke analysetools en databanken.[141] Het Vast Comité I voerde geen onderzoek naar de (generieke/standaard) faciliteiten inzake kantoorautomatisering die de diensten gebruiken (bijv. Windows, Word, Excel ...), voor zover ze niet specifiek zijn voor de inlichtingendiensten. Het Comité voerde evenmin een gedetailleerd onderzoek naar het informaticamateriaal (*hardware*) waarover de diensten beschikken, tenzij het specifiek was voor de betrokken inlichtingendienst. Het onderzoek had tot doel de risico's[142] te identificeren waarmee de diensten te maken kregen en die risico's te verminderen door gepaste aanbevelingen te formuleren.

In een eerste luik maakte de ADIV voorwerp uit van onderzoek, en dit omwille van de impact van de herstructurering van deze dienst op het vlak van ICT-tools en werkmethoden. Het onderzoek werd gefinaliseerd in mei 2020 en de resultaten werden opgenomen in het Activiteitenverslag 2020.[143]

Een tweede luik betrof de Directie Cyber van de ADIV en een derde luik de VSSE. De onderzoeksbevindingen van deze laatste twee luiken maken het voorwerp uit van voorliggend onderdeel.

De onderzoeksvragen die werden voorgelegd aan de Directie Cyber van de ADIV en aan de VSSE, luidden als volgt:

- Welke technologieën en tools op het vlak van ICT gebruikt de ADIV/VSSE om zijn activiteiten mee te ondersteunen?
- In hoeverre worden de instrumenten intern ontwikkeld of door externe partners aangeleverd?
- Worden de 'goede praktijken' die inzake ICT gangbaar zijn (hierna 'ITIL')[144] toegepast (meer bepaald: *'change management'*, *'inventory management'*, *'business continuity'*, *'incident management'*, *'problem management'* …)?

---

141 Bij de ADIV worden deze systemen *'weapon systems'* genoemd – naar analogie met bijvoorbeeld systemen die zijn geïntegreerd in de defensieplatformen bij Landsverdediging (bijv. de *software* voor de radarsystemen of *'battle management'*).

142 Een 'risico' werd gedefinieerd als het eventuele bestaan van een min of meer voorzienbare tekortkoming of een bedreiging die een impact kan hebben op de verwezenlijking van de doelstellingen van een organisatie of de efficiënte uitvoering van die doelstellingen, gekoppeld aan de waarschijnlijkheid dat er zich als gevolg van deze tekortkoming of bedreiging een schadelijke gebeurtenis voordoet.

143 VAST COMITÉ I, *Activiteitenverslag 2020* ('I.6. Informatie- en communicatietechnologie in het inlichtingenproces bij de ADIV').

144 ITIL is het acroniem voor '*Information Technology Infrastructure Library*', wat kan worden vertaald als 'Bibliotheek voor de infrastructuur van de informatietechnologieën'. Het gaat om goede praktijken voor het beheer van de IT-diensten die wereldwijd het meest worden gebruikt (bron: www.heflo.com/fr/blog/technologie/definition-itil).

– Is er een *'business continuity plan'*-beleid (BCP) en bestaan er *'disaster recovery plan'*-procedures (DRP) met inbegrip van *back-ups* en zijn die actueel?[145]

Het onderzoek had dus tot doel de risico's te identificeren waarmee de ADIV/VSSE te maken kregen en die risico's te verminderen door aanbevelingen te formuleren. Daarbij was het zogenaamde 'CIA-model'[146] van toepassing en werden drie types risico's onderscheidden:
– *Confidendiality*: het risico van kennisname van al dan niet geclassificeerde gegevens;
– *Integrity*: het risico van ongeoorloofde wijziging van al dan niet geclassificeerde gegevens;
– *Availability*: het risico dat de gegevens niet beschikbaar zijn, wat een obstakel zou vormen voor de goede uitvoering van de opdrachten van de dienst.

I.13.2. DE ICT-OMGEVING EN -ORGANISATIE BIJ DE DIRECTIE CYBER VAN DE ADIV

I.13.2.1. Context

I.13.2.1.1. Equipe en personeel

De informatica voor de Cyber-directie van de ADIV wordt beheerd door een team dat speciaal daarvoor werd samengesteld, aangezien dit de *core business* is van deze directie. Het team is opgesplitst in diverse onderdelen die zich over specifieke materies bekommeren.

Eind maart 2021 beschikte de ICT-cyberafdeling over te weinig personeel: slechts 80% van het totale aantal ICT-medewerkers dat was voorzien, werd aangeworven. Het aanzienlijk personeelsverloop is voornamelijk toe te schrijven aan de personeelswijzigingen in het Egov-kader[147], maar ook aan het vertrek van burgerpersoneel.[148]

---

145 Er bestaan algemeen aanvaarde goede praktijken over hoe het best *back-ups* worden genomen en over welke procedures in geval van een ramp moeten gevolgd worden. Het beheer van *back-ups* is, net als de DRP-procedures (*'disaster recovery plan'*), opgenomen in een algemeen *'business continuity plan'* (BCP).

146 Het gebruik van het CIA-model wordt aanbevolen als basis voor de risicoanalyse volgens de internationale normen ISO 270 betreffende de veiligheid van de informatie, en meer bepaald de norm 27005 die het beheer definieert van risico's in verband met de veiligheid van de informatie. Dit model wordt ook gebruikt door tal van andere normen zoals TCSEC – Orange Book (1983 – VS) of nog Common Criteria (1994 – internationaal).

147 Egov staat in voor de rekrutering en selectie van gespecialiseerde ICT-ers voor overheidsdiensten en instellingen.

148 Het Cyber-personeel bestaat immers uit militairen, ambtenaren met het Camu-statuut en externe medewerkers die via Egov Select worden aangeworven.

De 'servercapaciteit' (fysieke *resources*) volstond op het ogenblik van het onderzoek, maar beantwoordde niet aan de ambities op lange termijn van de dienst (*management plan*). Er werden nieuwe *resources* aangekocht, maar de beslissingen daarover waren afhankelijk van de budgetten die eraan worden toegewezen en dus van de prioriteiten die aan de dienst worden opgelegd.

Wat het beroep op onderaanneming en overheidsopdrachten betreft: aangezien het overgrote deel van de gebruikte *software* afkomstig is van de *opensourcewereld*, wordt er niet systematisch een beroep gedaan op onderaannemers of overheidsopdrachten voor de aankoop van *software*. De ontwikkelingen binnen Cyber gebeuren intern.

I.13.2.1.2. Servers en netwerken

De toegang tot de serverlokalen wordt beheerd door een beveiligd mechanisme. Er worden regelmatig *back-ups* uitgevoerd.

Een *Component Management Database* (CMDB)[149] is voorzien en wordt manueel geüpdatet. Het zou beter zijn als die CMDB automatisch zou worden geüpdatet – niet alleen omdat op die manier de juistheid van de gegevens zou worden gewaarborgd, maar ook omdat op die manier onregelmatigheden zouden worden gedetecteerd.

De monitoring wordt uitgevoerd door verschillende softwareprogramma's. Het gebruik van steeds meer verschillende softwareprogramma's zou echter wel een negatief effect kunnen hebben op de reactiviteit na een waarschuwing. Het zou dan ook aangewezen zijn om zich te concentreren op een centrale *software*.

I.13.2.1.3. Softwaresystemen in de inlichtingenopdracht

Voor wat betreft de belangrijkste softwaresystemen die te maken hebben met de collecte, analyse en verspreiding van inlichtingen (inlichtingencyclus), kon het Comité vaststellen dat de Cyber-divisie haar volledige infrastructuur heeft opgebouwd op basis van een strategisch plan op lange termijn en precieze actieterreinen. Bovendien levert ze zowel op het vlak van de *hardware* als van de *software* de nodige inspanningen om de 'goede ITIL-praktijken' op het terrein toe te passen.

De divisie Cyber gebruikt een aanzienlijk aantal vakspecifieke applicaties, die samen het volledige spectrum van haar opdrachten omvatten. Het Vast Comité I heeft een representatief deel van die applicaties gekozen met verzoek om demonstratie of uitleg.[150]

---

149 Een databank waarin alle ICT-componenten zijn opgenomen – zowel netwerken (switches, routers enz.) als systemen (*servers*, pc's enz.) en *software* (met versienummer).

150 De applicaties die niet werden gekozen voor een demonstratie zijn ofwel vergelijkbaar met de applicaties die wel worden getoond, of zijn bekend in de IT-wereld. De voorkeur werd ook gegeven aan de intern ontwikkelde applicaties of de apparatuur waarvoor het personeel van de Cyber-divisie specifieke scripts moet aanmaken.

De belangrijkste vaststellingen waren de volgende:

- Er zijn slechts weinig *tools* voor *big data* en *datamining*, aangezien Cyber deze in het kader van zijn opdrachten niet nodig heeft: deze divisie houdt zich immers bezig met het opzoeken en het analyseren van bedreigingen, bewustmaking, bescherming van netwerken, enz. Toch beschikken bepaalde *tools* over interne mechanismen die erop lijken.
- Voor de applicaties die door de Cyber-directie worden beheerd, werd een verwerkingsregister samengesteld dat wordt vermeld in de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.[151] Het register was nog niet volledig operationeel, maar de aanpassingen die eraan moeten worden aangebracht, waren slechts beperkt. Voor die tekortkomingen hoefden dus geen dwingende maatregelen te worden getroffen.
- Het Comité heeft vastgesteld dat het Cyber-netwerk stabiel is en snel werkt. Er werd een monitoringsysteem voor het netwerk en de infrastructuur in het algemeen ingevoerd waarmee storingen kunnen worden gedetecteerd.
- Er worden regelmatig *back-ups* uitgevoerd. Voor de belangrijkste applicaties bestaat een *Disaster Recovery Process* (DRP) met een niet-gestructureerde documentatie. Dat zou moeten worden aangevuld en bijgewerkt naarmate wijzigingen in de infrastructuur worden aangebracht.

I.13.2.1.4. Vulnerability testing en veiligheid

Het Vast Comité I kon vaststellen dat zowel bij de intern ontwikkelde *tools* als bij de aangekochte *tools* bijzondere aandacht wordt besteed aan de veiligheid en de applicatietests. De applicaties ondergaan een hele reeks automatische standaardtests en in voorkomend geval manuele tests, waarbij gebruik wordt gemaakt van producten die algemeen worden erkend om hun doeltreffendheid.

Ook bij de fysieke implementatie van de infrastructuur wordt met de veiligheid rekening gehouden.

Bovendien worden de analyses van potentieel offensieve elementen (bijv. mogelijke *malware*) in beveiligde omgevingen uitgevoerd.

I.13.2.2. Evaluatie van de risico's

Voor elke ICT-onderdeel van de Directie Cyber van de ADIV werden een aantal aandachtspunten opgesomd. In de loop van het onderzoek detecteerde het Comité een aantal risico's, de waarschijnlijkheid dat deze risico's zich voordoen en een

[151] Dit register moet de gegevensbeschermingsautoriteit die het Vast Comité I is in staat stellen om op elk moment op de hoogte te blijven van de manier waarop de persoonsgegevens worden verwerkt, om welke soorten gegevens het gaat, hoelang die gegevens worden bewaard en wie verantwoordelijk is voor de verwerking.

aantal pistes voor beheersing ervan (*mitigation).*[152] De belangrijkste risico's voor de dienst waren:
- het personeelstekort en de rotatie van het personeel;
- de versterking van de fysieke infrastructuur;
- netwerkbewakingstools;
- en de samenwerking met externe diensten.

I.13.3. DE ICT-OMGEVING EN -ORGANISATIE BIJ DE VSSE

I.13.3.1. Context

I.13.3.1.1. Equipe en personeel

Informatica wordt bij de VSSE door een beperkt team beheerd. Dit team vervult een centrale rol, aangezien de steun verleent aan verschillende diensten en bureaus, die de informatie en de inlichtingen verzamelen, analyseren en verspreiden.

Op 1 juni 2021 was het aantal ICT-personeelsleden onvoldoende. Dat geldt des te meer voor het bijzonder beperkte aantal *developpers*.

Wat het inzetten van onderaannemers en het uitschrijjven van overheidsopdrachten betreft, eist de VSSE een veiligheidsmachtiging voor de inschrijvers. De *software* wordt meestal via overheidsopdrachten door externe partijen ontwikkeld of door de dienst aangekocht. De ontwikkelingen die via overheidsopdrachten worden besteld, leveren echter niet noodzakelijkerwijs de gewenste resultaten op ten gevolge van vertragingen op de termijnen, veranderende specificaties, overschrijding van de budgetten, veranderende technologieën, enz.

I.13.3.1.2. Servers en netwerken

De serverlokalen en de back-upsystemen beantwoorden aan strenge veiligheidsnormen, werken efficiënt en werden ontworpen op basis van een specifieke risicoanalyse die regelmatig wordt geüpdatet.

Er is een CMDB voorzien die manueel wordt geüpdatet. Het zou beter zijn als die CMDB automatisch zou worden geüpdatet – niet alleen omdat op die manier de juistheid van de gegevens zou worden gewaarborgd, maar ook omdat op die manier onregelmatigheden beter zouden worden gedetecteerd.

Het beheer van de configuraties en de monitoring worden uitgevoerd door een commerciële tool die in de volledige architectuur is geïntegreerd en gebeuren op de meest kritieke controlepunten (applicaties, *hardware*, netwerk, enz.). Het systeem

[152] Omwille van het vertrouwelijke karakter kon geen gedetailleerde analyse worden gepubliceerd in het openbare activiteitenverslag.

werkt erg goed, maar zou meer performant kunnen zijn voor wat betreft de proactieve detectie van onregelmatigheden.

I.13.3.1.3. Softwaresystemen in de inlichtingenopdracht

Wat betreft de belangrijkste *software*systemen die te maken hebben met de collecte, analyse en verspreiding van inlichtingen (inlichtingencyclus), kon het Comité vaststellen dat de VSSE één enkele 'gespecialiseerde' databank gebruikt. Het is mogelijk dat er andere databanken bestaan die deel uitmaken van applicaties, maar dit zijn slechts technische databanken die de werking van die applicaties mogelijk maken. Deze gespecialiseerde databank werd regelmatig verbeterd en onlangs naar een recentere technologie gemigreerd.

De optie die begin 2020 werd genomen voor de modernisering van de gespecialiseerde databank was een consolidatie en een reorganisatie van de databanken (van het SQL-type) met de toevoeging van zoekindexen. Die methode is relatief goedkoop (*hardware*, implementatietijd) en levert resultaten op voor de vaakst uitgevoerde SQL.

Het Atlas-project werd in 2015 (budgetdossier) en 2017 (ontwikkeling) opgestart met de bedoeling om de laatste levering tegen eind 2021 uit te voeren. Het doel van dit project was om alle gegevens van de VSSE te centraliseren, ongeacht of ze van een externe verzender afkomstig zijn of binnen de dienst werden aangemaakt. Zoekopdrachten zullen hierdoor niet langer per entiteit gebeuren, maar wel op basis van relevantie ten opzichte van de inhoud (van een bestaande fiche, een document, een rapport…).[153] Dit project, uitgewerkt met het bedrijf Smals, beantwoordt ook aan de vereisten van de analyse van *big data*. Nog niet alle componenten zijn geleverd of in productie genomen. Het Vast Comité I kon een demonstratie bijwonen van de reeds ontwikkelde stabiele functionaliteiten. Er werden aan het Comité problemen gemeld in verband met de behandeling van bepaalde behoeften van de gebruikers en zorgen in verband met de planning.[154]

Wat betreft de applicaties die door de VSSE worden beheerd, was het verwerkingsregister dat wordt vermeld in de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, in uitvoering. Het Comité kon vaststellen dat dit register niet volledig operationeel was, maar de aanpassingen die eraan moesten worden aangebracht, slechts beperkt waren. Deze tekortkomingen vereisten geen specifieke maatregelen.

---

153 De gegevens worden dan onderling met elkaar in verband gebracht via een correlatiegrafiek die een weging toekent op basis van de vermelde relevante thema's of woorden.

154 Daaruit blijkt dat de communicatie tussen het projectteam en de essentiële gebruikers over specifieke behoeften (en dan meer bepaald in verband met BIM) veel te beperkt is, als ze al plaatsvindt. Het Atlas-project lijdt ook in zijn geheel aan vertragingen, terwijl ook het voorziene budget al is overschreden. Er moesten dan ook keuzes in verband met de implementatieprioriteit worden gemaakt.

Het Comité heeft vastgesteld dat het netwerk stabiel is en snel werkt. Er werd een monitoringsysteem voor het netwerk en de infrastructuur in het algemeen ingevoerd waarmee storingen kunnen worden gedetecteerd. Deze monitoring doet aan detectie van problemen die zich hebben voorgedaan, eerder dan proactief te werken.

De *back-ups* worden dagelijks vakkundig gemaakt. Voor de belangrijkste applicaties bestaat een *Disaster Recovery Process* (DPR). Aangezien de andere applicaties meer *support*-elementen zijn die in *standalone* werken op vaste stations, volstaat de documentatie die door de firma wordt geleverd. Het DRP-proces past in het kader van een algemener *Business continuity plan* (BCP).

Tot slot heeft het Comité verschillende bestaande of in ontwikkeling zijnde softwarepakketten bekeken, waaronder het Tardis-project (ook Bavak genoemd), dat eind 2016 van start is gegaan. Deze te ontwikkelen software moest online acties op de verschillende sociale netwerken automatiseren, informatie extraheren (met automatische vertaling van de informatie), analyseren en in een rapport exporteren. Na verloop van tijd werd het project complexer omdat verschillende functies werden toegevoegd. Het project werd uiteindelijk begin 2021 door de VSSE stopgezet, nadat duidelijk was geworden dat het niet aan de verwachtingen voldeed. De sociale netwerkaccounts waarop de *software* actief was, werden snel verwijderd omdat de aanwezigheid van de *software* was ontdekt. [155]

I.13.3.1.4. Vulnerability testing en veiligheid

Het Vast Comité I kon vaststellen dat op de intern ontwikkelde programma's veiligheidstests worden uitgevoerd. De andere *applicaties* zijn afkomstig van de *opensource*-wereld, of zijn commerciële oplossingen. Voor sommige is een certificatie aanwezig; voor andere bestaat geen enkele waarborg dat een penetratietest werd uitgevoerd. Er worden frequent updates aangeleverd dewelke door de VSSE worden toegepast. De VSSE werkt voornamelijk op een 'secure' netwerk dat niet met het internet is verbonden en onderworpen is aan een homologatie van de NVO.

Een ander punt in verband met de beveiliging betreft het *loggen*. Elke applicatie wordt gelogd (toegangen en acties van de gebruikers).

[155] Zie hierover in het bijzonder de Vraag van S. THEMONT aan de minister van Binnenlandse Zaken over 'Le logiciel de détectage de menaces terroristes ou de radicalisation' (Vr. en Ant., Kamer, 2020-2021, 3 mei 2021, n°50, p.306, Vr. nr.456) ; de Vraag van V. SCOURNEAU aan de minister van Buitenlandse Zaken en Defensie over 'OSINT' (Vr. en Ant., Kamer, 2019-2020, 5 augustus 2020, n°24, p.465, Vr. nr. 407).

I.13.3.2. Evalutie van de risico's

Voor elke ICT-onderdeel van de VSSE werden een aantal aandachtspunten opgesomd. In de loop van het onderzoek detecteerde het Comité een aantal risico's, de waarschijnlijkheid dat deze risico's zich voordoen en een aantal pistes voor beheersing ervan (*mitigation).*[156] De belangrijkste risico's voor de dienst waren:
- het personeelstekort en enkele specifieke profielen in het bijzonder;
- de beveiligde communicaties;
- het project Atlas en meer in het bijzonder de aan het Comité gemelde problemen aangaande het te weinig rekening houden met de noden van het personeel alsook omtrent de timing.

I.14. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2021ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2021 WERDEN OPGESTART

I.14.1. 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 de gebruik van telecommunicatie (art. 16/2 W.I&V) alsook de toegang tot PNR-gegevens (art. 16/3 W.I&V).

Eind 2020 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.

---

156 Omwille van het vertrouwelijke karakter kon geen gedetailleerde analyse worden gepubliceerd in het openbare activiteitenverslag.

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)).[157] 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*'. Na ontvangst en analyse van de statistieken van de twee inlichtingendiensten met betrekking tot de inzet van deze methode, wordt het onderzoeksrapport geredigeerd.

I.14.2 DE OPVOLGING VAN VRIJGELATEN TERRO-VEROORDEELDEN DOOR DE VSSE

In België werden tussen 2015 en 2020 zowat 500 personen veroordeeld voor feiten die verband hielden met terroristische activiteiten.[158] Sommigen onder hen werden veroordeeld bij verstek, en konden dus ook niet in hechtenis worden genomen. Een aantal van die veroordeelden genieten van penitentiair verlof, hebben inmiddels hun straf in de gevangenis uitgezeten of werden, na beslissing van de strafuitvoeringsrechtbank, voorwaardelijk (voor het strafeinde) vrijgelaten.

Gezien het door de Belgische en Europese inlichtingendiensten ingeschatte potentiële gevaar voor recidive, besliste het Comité halfweg 2019 een toezichtonderzoek te openen naar '*de wijze waarop de Belgische inlichtingen- en veiligheidsdiensten de opvolging verzekeren van enerzijds personen die in België verdacht worden van terroristische misdrijven die in België of elders zijn gepleegd en die genieten van een maatregel bedoeld in de Wet van 20 juli 1990 en anderzijds personen, die in België veroordeeld zijn voor terroristische misdrijven en die de Belgische gevangenis verlaten in het kader van één van de maatregelen bedoeld in de Wet van 17 mei 2006, hetzij die definitief vrijgelaten werden (art. 71 van genoemde wet)*'.

Er wordt bestudeerd op welke wijze beide inlichtingendiensten (VSSE en ADIV) deze thematiek opvolgen, welke middelen en methoden er daartoe worden ingezet en hoe de samenwerking verloopt met de partners (o.m. het OCAD, het

---

157 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.

158 *Parl. St*. Kamer 2021-22, CRIV55PLEN148, 25.

Directoraat-generaal Penitentiaire Inrichtingen, de Justitiehuizen, de Lokale en de Federale Politie…) en binnen welke structuren (*Local Task Forces,* de Werkgroep gevangenissen…). Ten slotte werd via *benchmarking* de Franse en Engelse manier van aanpak bestudeerd.

In 2021 werd, na de eerste resultaten, beslist het spectrum van het onderzoek te verruimen. Om het wijze van aanpak van de opvolging van deze gedetineerden *na* hun vrijlating te doorgronden, zag het Comité zich genoodzaakt om zich ook te verdiepen in hun opvolging door de inlichtingendiensten *tijdens* de detentie. Er diende eveneens rekening te worden gehouden met wetgevende evoluties en nieuwe reglementeringen, zoals bijvoorbeeld de publicatie in september 2021 door het OCAD van de 'Strategie Extremisme en Terrorisme' (kortweg Strategie TER). Het onderzoek wordt gefinaliseerd in het eerste semester van 2022.

I.14.3. 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.[159] De verwerking van de verzamelde informatie liep vertraging op, en dit in hoofdzaak omwille van de gezondheidscrisis en zijn impact op de effectieven van het Comité, maar ook omwille van andere, meer dringende dossier (de zaak-Conings, *supra*).

I.14.4. MOGELIJKE DREIGINGEN VOOR HET BELGISCHE WETENSCHAPPELIJK EN ECONOMISCH POTENTIEEL (PRISM/WEP): OPVOLGONDERZOEK

In 2016 werd een toezichtonderzoek afgerond naar de bescherming van het wetenschappelijk en economisch potentieel naar aanleiding van de zgn. 'Snowden-

[159] www.iso.org:fr/iso-31000-risk-management.html

onthullingen'.[160] Deze onthullingen gaven een inkijk in onder meer het bestaan van het PRISM-programma waarbij de Amerikaanse *National Security Agency* (NSA) (meta)data van telecommunicatie verkreeg en brachten verder aan het licht dat Amerikaanse maar ook Britse diensten inlichtingenoperaties hadden opgezet ten aanzien van bepaalde internationale instellingen en samenwerkingsverbanden (VN, EU en G20) waarbij ook 'bevriende landen' werden geviseerd. Het onderzoek behandelde de mogelijke implicaties van buitenlandse programma's op de bescherming van het wetenschappelijk en economisch potentieel van het land. Het ging na of de Belgische inlichtingendiensten aandacht besteedden aan dit fenomeen; een reële of mogelijke bedreiging detecteerden voor het Belgische wetenschappelijk en economisch potentieel; er de bevoegde overheden van in kennis hadden gesteld en beschermingsmaatregelen hadden voorgesteld; en over voldoende en adequate middelen beschikken om deze problematiek op te volgen. Ook werd bestudeerd welke de gevolgen waren van het PRISM-programma en/of andere analoge systemen voor het wetenschappelijk en economisch potentieel van het land.

Eind november 2019 verzocht de parlementaire Begeleidingscommissie het Vast Comité I om dit toezichtonderzoek terug op te nemen en te actualiseren. In 2020 werd, na het uitvoeren van de eerste onderzoeksopdrachten – meer in het bijzonder de verzameling en analyse van het open bronnenmateriaal – beslist om dit onderzoek te fusioneren met het toezichtonderzoek naar de operatie Rubicon (cf. I.14.6). In 2021 vonden tussen het Vast Comité I en beide inlichtingendiensten hieromtrent ontmoetingen en bevragingen plaats. Ook werden er vragen voorgelegd aan het Belgische Centrum voor Cybersecurity (CCB). Ook in deze liep de redactie van het toezichtrapport vertraging op omwille van meer urgent onderzoek, te weten de zaak-Conings (cf. I.9.). De resultaten worden verwacht voor begin 2022.

160 VAST COMITÉ I, *Activiteitenverslag 2016*, 52 e.v. Voluit 'Toezichtonderzoek over de aandacht die de Belgische inlichtingendiensten (al dan niet) besteden aan de mogelijke dreigingen voor het Belgische WEP uitgaande van op grote schaal door buitenlandse grootmachten en/of inlichtingendiensten gehanteerde elektronische bewakingsprogramma's op communicatie – en informatiesystemen'.

I.14.5. SPIONAGE VIA GEMANIPULEERDE CODEERAPPARATRUUR: DE OPERATIE RUBICON

De 'Operatie Rubicon'[161] of de inlichtingenoperatie waarbij Amerikaanse en Duitse inlichtingendiensten met het Zwitserse bedrijf Crypto AG als dekmantel meerdere decennia meeluisterden met versleutelde communicatie van overheden in tientallen landen, geraakte halfweg februari 2020 in de openbaarheid.[162] Onder andere Nederland, Frankrijk, Zweden en Denemarken (de 'Maximator-landen') waren zgn. '*cognescenti*': ingewijden in de cryptologische details van bepaalde apparaten. Onder meer België, "*waardevol voor de verheldering die zijn rapporten bood over diplomatieke gebeurtenissen*" en vooral interessant als diplomatiek centrum van de NATO en de (toenmalige) Europese Economische Gemeenschap, zou zijn afgeluisterd.

Het Comité besloot een toezichtonderzoek te openen, waarmee een antwoord werd gezocht naar vragen als[163]: in welke mate waren de Belgische inlichtingendiensten op de hoogte waren (of in welke mate dienden ze er – gezien hun wettelijke opdrachten – van op de hoogte te zijn van deze operatie? Werden hierover inlichtingen verzameld of werd dit niet wenselijk geacht? Maar belangrijker nog: bieden de diensten op dit ogenblik voldoende bescherming ter zake? Zijn er risico-analyses voorhanden? Als crypto-materiaal wordt gebruikt, welke voorzorgsmaatregelen worden er dan genomen? Hoe wordt heden ten dage omgegaan met deze crypto-problematiek… Eind september 2020 werd beslist om dit onderzoek samen te voegen met het opvolgonderzoek PRISM/WEP (cf. I.14.4).

I.14.6. (BIJKOMENDE) INLICHTINGENCAPACITEITEN IN HET BUITENLAND VOOR DE BELGISCHE INLICHTINGENDIENSTEN?

Gelet op de door de wetgever omschreven inlichtingenopdracht bevindt de voor de inlichtingendiensten relevante informatie zich zowel in het binnen- als in het

---

161 Het tijdschrift *Intelligence and National Security* (Volume 35, August 2020, Issue 5) wijdde hieraan een themanummer. Zie daarin onder meer R. ALDRICH et al., 'Operation Rubicon: sixty years of German-American success in signals intelligence'; M.J. DOBSON, 'Operation Rubicon: Germany as an intelligence 'Great Power" en B. JACOBS, 'Maximator: Europan signals intelligence cooperation from a Dutch perspective'.

162 Er werd ruchtbaarheid gegeven aan evaluatierapporten van de Amerikaanse en Duitse inlichtingendiensten door de Duitse televisiezender ZDF en de Washington Post. Het Nederlandse onderzoeksplatform Argos kreeg inzage in de rapporten, dewelke onder meer door De Tijd werden overgenomen (L. BOVÉ, *De Tijd*, 13 februari 2020, ('Geheime documenten onthullen spionage van België door CIA en Duitse BND')).

163 Maar bijvoorbeeld ook: wat is de betekenis/waarde van de notie 'bevriende Staat' in de context van inlichtingendiensten en in welke mate bepaalt die notie de houding van de eigen inlichtingendiensten?

buitenland. In september 2020 werd daarom een toezichtonderzoek geopend 'naar de behoefte voor (bijkomende) inlichtingencapaciteiten voor de Belgische inlichtingendiensten in het buitenland'. De doelstelling van het onderzoek is divers:

- Nagaan of de VSSE/ADIV actueel enige operationele informatiegaring in het buitenland verrichten, en zoja, onder welke vorm en via welke concrete inlichtingenactiviteiten;
- Toetsen van deze buitenlandse activiteiten aan het bestaand regelgevend kader;
- Nagaan of de diensten nood hebben aan bijkomende bevoegdheden waaronder juridische mogelijkheden (m.a.w. onderzoeksbevoegdheden) om in het buitenland informatie te kunnen inwinnen.

In 2021 werden, op basis van een analyse van het betreffende juridische kader, de VSSE en de ADIV bevraagd over de eventuele inlichtingenactiviteiten die zij uitvoeren in het buitenland. Omwille van andere prioriteiten en gezien de impact van de gezondheidscrisis op de effectieven van het Comité, werd de analyse van deze antwoorden onderbroken. Het onderzoek zal worden afgesloten in de loop van 2022.

I.14.7. CONTROLE OP DE SPECIALE FONDSEN: OPVOLGONDERZOEK

Zoals elke overheidsdienst, krijgen ook de inlichtingendiensten overheidsgeld toegekend voor de uitoefening van hun wettelijke opdrachten. De normale 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 'normale 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[164] 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 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.

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

Sinds 2018 (VSSE) en 2020 (ADIV) uitte het Rekenhof het voornemen om eveneens een periodieke controle te doen van deze fondsen.[165] Daarbij kon het Rekenhof beroep doen op de technische ondersteuning zoals voorgeteld door het Vast Comité I.[166] 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, worden de onderzoeksactiviteiten hernomen in 2022.

I.14.8. ONDERZOEK NAAR DE OPVOLGING DOOR DE INLICHTINGENDIENSTEN VAN 'DES MOUVEMENTS SECTAIRES À OBÉDIENCE RELIGIEUSE AYANT DES VISÉES POLITIQUES'

In juli 2021 opende het Vast Comité I op verzoek van de Voorzitster van de Kamer van volksvertegenwoordigers een onderzoek naar "*la manière dont les services de renseignement s'intéressent aux activités des mouvements sectaires à obédience religieuse ayant des visées politiques (autres mouvements salafistes politiques, Opus Dei, mouvement Civitas, etc.)*".[167]

Dit was het derde onderzoek van een drieluik en volgde als dusdanig twee eerder door het Comité gerealiseerde onderzoeken op, te weten het onderzoek naar de wijze waarop de VSSE de regeringscommissaris Ihsane Haouach had opgevolgd[168] en het onderzoek naar de aandacht van de inlichtingendiensten voor de Moslimbroederschap.[169]

Eind 2021 en na enkele incoherenties te hebben verduidelijkt, werd in samenspraak het spectrum van het onderzoek geherdefineerd naar '*les organisations à obédience religieuse ayant des visées politiques*'.

---

165 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.

166 "*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*".

167 Brief van 19 juli 2021 van de Voorzitster van de Kamer, E. TILLIEUX, aan de voorzitter van het Vast Comité I.

168 Zie 'I.11. De opvolging van een regeringscommissaris door de VSSE' (*supra*).

169 Zie 'I.12. Een vernieuwde aandacht voor de Moslimbroederschap' (*supra*).

HOOFDSTUK II.

DE CONTROLE OP DE BIJZONDERE EN BEPAALDE GEWONE INLICHTINGENMETHODEN

Het Vast Comité I is gehouden tot transparantie over de inzet van de zogenaamde 'bijzondere inlichtingenmethoden'(BIM) door de inlichtingendiensten: artikel 35 §1, 1° 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) – zoals gewijzigd door artikel 25 BIM-Wet[170] vermeldt immers dat het Comité in zijn activiteitenverslag "*specifiek aandacht besteedt 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 […]*". En verder (art. 35 §2 W.Toezicht) dient het Comité jaarlijks verslag uit te brengen *"aan de Kamer van Volksvertegenwoordigers over de toepassing van artikel 16/2 en artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten […].*[171] *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.*[172] *Het verslag vermeldt ook de activiteiten van het Vast Comité I.*"

Voorliggend hoofdstuk bevat dan ook cijfermateriaal over de inzet door enerzijds de Veiligheid van de Staat (VSSE) en anderzijds de Algemene Dienst Inlichting en Veiligheid (ADIV) van de specifieke en de uitzonderlijke methoden (gegroepeerd als de zgn. 'bijzondere inlichtingenmethoden') én van de gewone methoden waarin aan het Comité een bijzondere controleopdracht wordt toegekend (de zgn. 'gewone methoden plus').

---

170 Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, *BS* 10 maart 2010.

171 Een afschrift van dit jaarlijks verslag wordt eveneens bezorgd aan de ministers van Justitie en Landsverdediging alsook aan de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid, die de mogelijkheid hebben de aandacht van het Vast Comité I te vestigen op hun opmerkingen (art. 35 §2 W.Toezicht).

172 Een specifiek verslag over de 'behaalde resultaten' is vooralsnog niet aan de orde. Het Comité is zich bewust van het gegeven dat hier een belangrijke opdracht ligt: *"there will be an important job for oversight bodies to measure the effectiveness of these new techniques while nonetheless providing public assurance that any new powers or resources are proportionate to the threat and not abused"*, in: I. LEIGH and N. WEGGE, *Intelligence oversight in the twenty-first century. Accountability in a changing world*, Routledge, 2020, 18.

Tevens wordt verslag gedaan over de wijze waarop het Vast Comité I zijn (jurisdictionele) controletaak op deze methoden heeft waargenomen. Destijds heeft het Comité de keuze gemaakt om zijn rechtspraak te publiceren in de jaarlijkse activiteitenverslagen. De beslissingen die soms geclassificeerde elementen bevatten, worden uiteraard niet *in extenso* gepubliceerd. Alleen de juridisch relevante elementen en de hoogstnodige feiten worden weergegeven. Dergelijke transparantie is (vrij) uniek. De afgelopen jaren hebben ondertussen echter bewezen dat dit kan zonder daardoor de werking van de inlichtingendiensten in het gedrang te brengen.

Merk ten slotte op dat het Comité ook kan gevat worden in zijn hoedanigheid van 'pre-judicieel adviesverlener' (art. 131*bis*, 189*quater* en 279*bis* Sv.).[173] In dat geval geeft het Comité een advies over de al dan niet rechtmatigheid van specifieke of uitzonderlijke methoden die inlichtingen hebben opgeleverd die in een strafzaak worden gebruikt. Tot op heden blijft dit evenwel een louter theoretisch concept; afgelopen decennium werd nog nooit van deze mogelijkheid gebruik gemaakt.[174]

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

II.1.1. ALGEMENE TRENDS

II.1.1.1. Inzet van bijzondere inlichtingenmethoden door de VSSE en de ADIV

De wetgever opteerde er destijds voor om een duidelijke onderverdeling aan te brengen tussen de verschillende methoden van gegevensverzameling, in de wet geduid als gewone, specifieke of uitzonderlijke methoden. Deze zijn (of beter: zouden moeten zijn) in de zwaarte van de inbreuk op het privéleven oplopend en hebben ieder hun eigen toetsingskader en controlemechanisme, eveneens oplopend in

173 Hierover: VAST COMITE I, *Activiteitenverslag 2010*, 59.

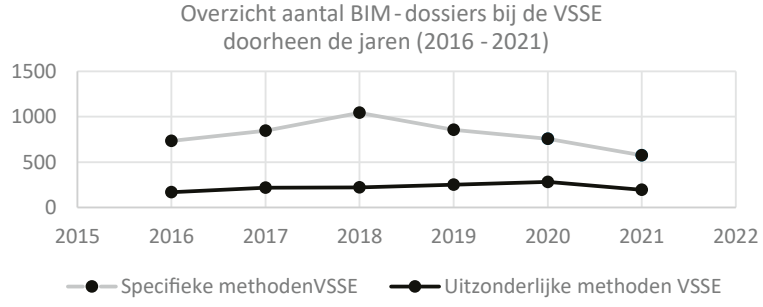
174 De beslissing om een advies te vragen berust bij de onderzoeksgerechten of de strafrechters. Over de beperkte toepassing ervan, zie: VANDERBORGHT, J., '*If you torture the data long enough, it will confess. Enkele cijfers over de inzet van bijzondere inlichtingenmethoden*', in VANDERBORGHT, J. (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, Intersentia, Antwerpen, 2020, 25.

'zwaarte'.[175] Hiermee werd beoogd te verhinderen dat de diensten niet meteen naar het zwaarste middel zouden grijpen.

Tussen 1 januari en 31 december 2021 werden door de twee inlichtingendiensten samen 1823 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 1570 door de VSSE (waarvan 1220 specifieke en 350 uitzonderlijke) en 253 door de ADIV (waarvan 166 specifieke en 87 uitzonderlijke).[176]

175 Deze opdeling blijkt voor sommige experten 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 onderzoeksbevoegdheden als gewone methoden worden gekwalificeerd, is de inmenging in de privacy en de gegevensbescherming bij deze methoden vaak groter dan bij 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. De inlichtingendiensten op hun beurt wijzen in dit kader op de noodzaak tot instandhouding van het gelijkheidsbeginsel met de bijzondere opsporingsmethoden (BOM).

176 De inlichtingendiensten houden er een andere wijze van telling op na. Bij de VSSE wordt gerekend in 'BIM dossiers', waarbij één dossier meer dan één methode kan bevatten. Eenzelfde tendens blijft evenwel merkbaar:

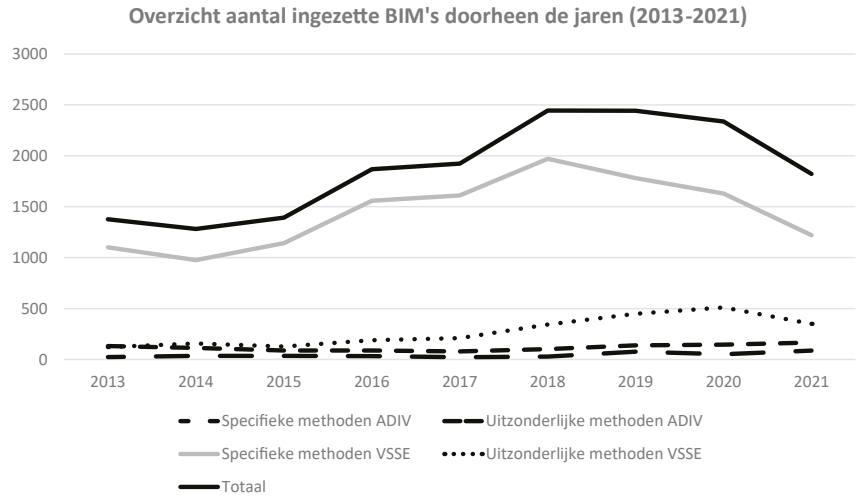


Ook de ADIV telt anders: de dienst telt de methoden per artikel, zonder een onderscheid te maken tussen de verschillende paragrafen, wat het Comité wel doet. De ADIV-cijfers omvatten ook het geheel van alle ingediende aanvragen (inclusief deze dewelke intern werden afgewezen). Ten slotte wordt door de ADIV een methode meegeteld in het jaar waarin de aanvraag werd ingediend, ongeacht wanneer de methode effectief werd toegelaten.

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

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

Dit kan als volgt grafisch worden weergegeven:



Na een constante stijging van het aantal ingezette BIM's tot 2018 en een stagnatie in 2019-2020, diende in 2021 een significante daling te worden opgetekend.[177] Let wel, als de cijfers worden uitgesplitst naar de diensten, dient voor 2021 een aanzienlijke stijging te worden vastgesteld (circa 30%) van het aantal door de ADIV ingezette BIM's. Daartegenover staat een aanzienlijke daling (circa 28%) bij de VSSE (*infra*).

177 Per toegelaten methode kunnen wel meerdere targets (zoals personen, organisaties, plaatsen, voorwerpen, communicatiemiddelen…) worden geviseerd.

Niettegenstaande een kleine inhaalbeweging wordt vastgesteld, blijft de VSSE het leeuwendeel van de ingezette methoden voor zijn rekening te nemen (86%). Beide diensten kregen weliswaar dezelfde bevoegdheden, maar hun opdrachten zijn dermate verschillend (bijv. de grote 'buitenlandopdracht' van de ADIV) dat uit een vergelijking van de twee diensten wat dit betreft, weinig lering kan worden getrokken. Bijkomende reden voor deze verschillen door de diensten aangehaald, is bijvoorbeeld het gegeven dat de door het gemeenschappelijk contraterrorisme-platform (Platform CT) uitgevoerde BIM's inzake de dreiging 'terrorisme' voor rekening worden genomen van de VSSE.

Als deze cijfers worden uitgesplitst, kan worden vastgesteld dat bij de ADIV de vorig jaar ingezette stijging van specifieke methoden (van 146 naar 166) blijft voortduren. Het aantal ingezette uitzonderlijke methoden stijgt sterk (een toename van 51 in 2020 naar 87 in 2021).[178] Naar luid van de ADIV zijn de redenen hiertoe de interne herstructuring van de BIM-cel, wat een vlottere dienstverlening[179] impliceert en de aanwerving van bijkomende *case-managers*, met bijgevolg meer '*request for operations*'. Inhoudelijk had de zaak-Jurgen Conings (cf. *supra*) en de uitlopers van dit dossier (extreemrechts in het leger) een grote impact. Maar zelfs zonder de zaak-Conings, kon een aanzienlijke toename worden opgetekend van het aantal ingezette BIM's, aldus de ADIV.

De VSSE daarentegen laat het tegenovergestelde optekenen. Er wordt zowel een opmerkelijke daling vastgesteld van het aantal ingezette specifieke methoden (van 1629 in 2020 naar 1220 in 2021) als een daling van het aantal ingezette uitzonderlijke methoden (van 511 in 2020 naar 350 in 2021 of een daling van meer dan 30%). Daartoe zijn, aldus de VSSE, meerdere redenen: het aantal zgn. 'gewone methoden plus' nam toe (communicerende vaten); bij de dienst vond een grote rekrutering plaats met een arbeidsintensieve opleiding waardoor bijgevolg tijdelijk minder personeel bij de buitendiensten beschikbaar was voor onderzoeken; de voortdurende gevolgen van de COVID-maatregelen…

II.1.1.2. De inzet van gewone methoden plus, in het bijzonder artikel 16/2 W.I&V

De identificatie van de abonnee of de gewoonlijke gebruiker van telecommunicatiedienst of -middel (bijv. gsm-nummer of IP-adres[180]) wordt als een gewone methode beschouwd in de mate waarin dit gebeurt via een vordering aan telecomope-

178 Belangrijk in dit kader is dat de ADIV eveneens bijzondere bevoegdheden heeft tot het inwinnen van gegevens zoals geregeld in de artikelen 44 ev. W.I&V. Zie hieromtrent: 'Hoofdstuk III. Het toezicht op buitenlandse intercepties, beeldopnamen en IT-intrusies' (*infra*).

179 Toch blijft de procedure tot indienen van BIM's bij de ADIV merkelijk (administratief) omslachtiger dan bij de VSSE, wat volgens de ADIV aanleiding zou geven tot een vorm van 'zelfcensuur'.

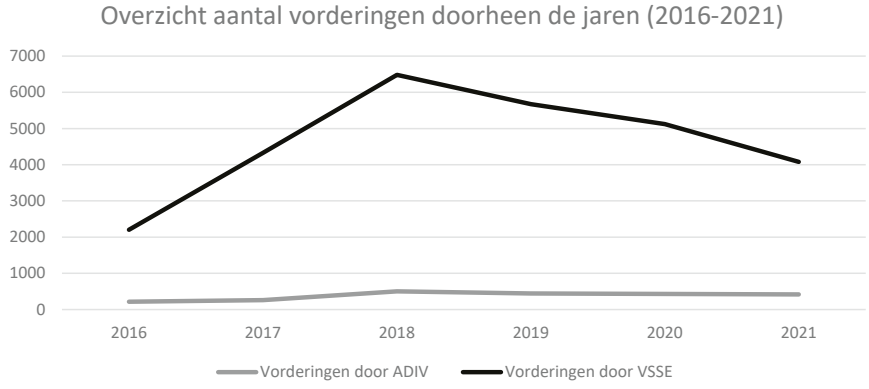
180 Vanaf 2022 wordt ook het aantal vorderingen opgesplitst in 'vorderingen IP' en 'vorderingen non-IP'.

ratoren of -providers of via een rechtstreekse toegang tot hun klantenbestanden.[181] 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.[182] Er werd ook bepaald dat het Comité maandelijks een lijst van de gevorderde identificaties en van elke toegang moet ontvangen.

Wat betreft deze methode, blijft de ingezette daling van het aantal vorderingen voortduren (een tiental vorderingen minder bij de ADIV in vergelijking met 2020, tegenover meer dan 1000 vorderingen minder bij de VSSE).[183]

	Vorderingen door ADIV	Vorderingen door VSSE
2016	216	2203
2017	257	4327
2018	502	6482
2019	442	5674
2020	433	5123
2021	420	4080

In een grafiek weergegeven geeft dit volgend beeld:



181 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).

182 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.

183 Vanuit zijn algemene toezichtsbevoegdheid onderzocht het Comité de redenen hiertoe; de resultaten werden opgenomen in het in 2019 geopende *'toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten die recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld*' (cf. I.14.1. De toepassing van nieuwe (bijzondere) inlichtingenmethoden').

Een aantal belangrijke kanttekeningen zijn hier op zijn plaats. Uit bovenstaande tabel kan inderdaad worden afgeleid dat na de implementatie van de wetsaanpassingen in 2016 en 2017, het aantal vorderingen een piek kende in 2018. Niettegenstaande het aantal vorderingen een indicatie vormt voor de werklast, kan hieruit niets worden afgeleid wat betreft de toe- of afname van het aantal selectoren (telefoonnummers, namen, IP-adressen…). Daar waar bij bijv. de militaire inlichtingendienst een daling van het aantal vorderingen dient te worden vastgesteld (van 433 in 2020 naar 420 in 2021), steeg het aantal selectoren opmerkelijk: van 5334 in 2020 naar 6385 in 2021 (of een stijging van bijna 20%). Bij de VSSE bleef ondanks de daling van het aantal vorderingen, het aantal selectoren vrij stabiel (31.730[184] in 2021 tegenover 31.204 in 2020).

Verder wordt door beide diensten in de telling geen onderscheid gemaakt tussen artikel 16/2 §1 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (W.I&V) en artikel 16/2 §2 W.I&V[185] (identificatie van een pre-paid kaarthouder).

II.1.1.3. Gevolgen van de vernietiging van de Dataretentiewet?[186]

Met zijn arrest van 22 april 2021 vernietigde het Grondwettelijk Hof de zogenaamde Dataretentiewet.[187] Het Hof oordeelde dat de algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie het recht schendt op eerbiediging van het privéleven en op bescherming van persoonsgegevens. Dit arrest betekent een obstakel voor onder meer inlichtingenonderzoeken.

Het hoeft geen betoog dat identificatie-, verkeers- en locatiegegevens een belangrijke rol speelt in het inlichtingenwerk. Onder meer hiervoor werd destijds in art. 126 Wet electronische communicatie (WEC)[188] 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.[189]

---

184 Bij de VSSE bedroeg het aantal identificaties van IP-adressen 4925, terwijl het 'aantal identificaties anders dan IP' 26.805 bedroeg (in 2020 waas dat respectievelijk 3188 en 28.016).

185 Artikel 16/2 W.I&V vermeldt: '§ 2. *De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een bank of financiële instelling om over te gaan tot het identificeren van de eindgebruiker van de in artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie bedoelde voorafbetaalde kaart, op basis van de referentie van een elektronische banktransactie die verband houdt met de voorafbetaalde kaart en die voorafgaand meegedeeld is door een operator of verstrekker in toepassing van paragraaf 1.*'

186 Zie hierover 'Hoofdstuk VI.3. Advies over dataretentie'.

187 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. Persbericht Grondwettelijk Hof, "*Het Grondwettelijk Hof vernietigt de verplichting tot algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie*", 22 april 2021.

188 Wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 mei 2005, 28070.

189 De dataretentieplicht is niet alleen van toepassing op telefoonverkeer, maar ook op verscheidene soorten internetverkeer.

Concreet oordeelde het Grondwettelijk Hof dat het bewaren van gegevens voortaan de uitzondering moet worden; de gerichte bewaring van gegevens dient steeds evenredig te zijn met het nagestreefde doel.

Gevraagd naar de implicaties op de werking van beide inlichtingendiensten in 2021, lieten zowel de ADIV als de VSSE optekenen dat deze eerder verwaarloosbaar zijn en er vooralsnog geen ingrijpende gevolgen te noteren vielen.

Ondertussen heeft de regering een wetsontwerp neergelegd[190] dat er voornamelijk op gericht is weer een juridisch kader in te stellen dat voldoet aan de rechtspraak inzake bewaring van de 'metagegevens' of 'verkeers- en locatiegegevens' door operatoren. De regering uitte de wens dat deze reparatiewet voor de zomer van 2022 in voege zou treden. Het nieuwe voorstel zou in het voorjaar 2022 aan de Ministerraad worden voorgelegd.[191]

II.1.2. METHODEN AANGEWEND DOOR DE ADIV

II.1.2.1. Gewone methoden 'plus'

De identificatie van de abonnee of de gewoonlijke gebruiker van telecommunicatiedienst of -middel

De ingezette daling van het aantal vorderingen blijft voortduren (een tiental vorderingen minder bij de ADIV in vergelijking met 2020) (*supra*).

Toegang tot PNR-gegevens

Naast de identificatie van de abonnee of de gewoonlijke gebruiker van telecommunicatie als gewone methoden 'plus' (*supra*), werd begin 2017[192] 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 (art. 16/3 W.I&V en art. 27 van de Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens (PNR-Wet).[193] Het Comité wordt

190 Wetsontwerp van 17 maart 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. *Parl. St.* Kamer 2021-22, 55K2575/001.

191 Vraag van E. GILISSEN aan de minister van Telecommunicatie over 'de wet op de bewaring van gegevens' (*Hand.* Kamer 2021-22, 9 maart 2022, CRIV55COM715, 11).

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

193 De BIM-cel van de ADIV heeft in deze geen functie; alles verloopt via de bij BELPIU gedetacheerde ADIV-medewerker.

in kennis gesteld van de aanwending van deze methode en kan ze desgevallend verbieden.[194]

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). Het aantal gerichte opzoekingen in PNR-gegevens bleef in 2021 stabiel (28 in 2020, 29 in 2021). Voor meer dan de helft betrof dit dossiers gelieerd aan de dreiging 'spionage'.

Gebruik van politionele camerabeelden

Bij Wet van 21 maart 2018 (*BS* 16 april 2018) werd de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten aangepast om de inlichtingendiensten toe te laten gebruik te maken van politionele camerabeelden. Daartoe werd er een nieuwe gewone methode ingevoerd (art. 16/4, §2 W.I&V).[195] [196] Er werd door de ADIV in 2021 (voor het eerst) vijftien maal van deze methode gebruik gemaakt. Drie van de vijftien aanvragen betroffen aanvragen voor een periode van minder dan één maand.

De cijfers

Gewone methoden plus (ADIV)	Aantal toelatingen 2020	Aantal toelatingen 2021
Identificatie van de 'abonnee of de gewoonlijke gebruiker' van telecommunicatie	433	420
Gerichte opzoekingen PNR-gegevens	28	29
Gebruik van politionele camerabeelden[197]	Niet in werking	15

194 Anders dan voor de methoden opgenomen in artikel 16/2 W.I&V werd niet voorzien in een verplichte verslaggeving aan het Parlement; artikel 35 § 2 W.Toezicht werd immers niet aangepast. Op suggestie van de Begeleidingscommissie besliste het Comité om deze cijfers mee op te nemen in zijn jaarlijkse verslaggeving en niet te wachten op een eventuele wetswijziging. Pas in 2020 werden de eerste twee stopzettingen bevolen.

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

196 Begin 2019 keurde de Ministerraad een ontwerp van koninklijk besluit goed ter uitvoering van artikel 16/4 W.I&V. Het werd aan het advies van het Vast Comité I voorgelegd. Dit advies 002/VCI-BTA/2019 van 9 april 2019 is te consulteren op de website van het Comité (www.comiteri.be).

197 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).

II.1.2.2. De specifieke methoden

Onderstaande tabel geeft de cijfers weer over de toepassing van de specifieke methoden door de ADIV. Er worden daarbij zeven specifieke methoden onderscheiden.

Specifieke methoden (ADIV)	Aantal toelatingen 2020	Aantal toelatingen 2021
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)[198]	6	12
Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (art. 18/5 W.I&V)	0	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	0	0
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	2	0
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)	2	6
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	0
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8, §1, 1° W.I&V)	69	75
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator (art. 18/8, §1, 2° W.I&V)	67	73
TOTAAL	**146**	**166**

198 Bij Wet van 21 maart 2018 (*BS* 16 april 2018) werd een nieuwe paragraaf toegevoegd aan art. 18/4 W.I&V om de inlichtingendiensten toe te laten gebruik te maken van politionele camerabeelden om *real time*-observaties uit te voeren. Deze methode, die een rechtstreekse toegang vereist tot de bedoelde informatie, werd nog niet geoperationaliseerd.

Wat betreft de inzet van specifieke methoden, spannen het 'opsporen van lokalisatiegegevens 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), beiden met het vorderen van de medewerking van een telecomoperator of -provider, duidelijk de kroon (148 van de 166 ingezette specifieke methoden). Er vonden dubbel zoveel observaties plaats in publiek toegankelijke plaatsen met een technisch middel dan in 2020 (van 6 naar 12 in 2021).

Volgens de ADIV werd 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 worden ingezet. Om aan dit euvel te verhelpen, werden begin 2022 interne briefings georganiseerd.

II.1.2.3. De uitzonderlijke methoden

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

Uitzonderlijke methoden (ADIV)	Aantal toelatingen 2020	Aantal toelatingen 2021
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) [199]	2	3
Al dan niet met behulp van technische middelen niet voor het publiek toegankelijke plaatsen doorzoeken, evenals al dan niet vergrendelde voorwerpen die zich daar bevinden (art. 18/12 W.I&V)	0	2
Een rechtspersoon als bedoeld in art. 13/3 § 1 W.I&V inzetten om gegevens te verzamelen (art. 18/13 W.I&V)	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	0	2
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	6	8

[199] Bij Wet van 21 maart 2018 (*BS* 16 april 2018) werd een nieuwe paragraaf toegevoegd aan art. 18/11 W.I&V om de inlichtingendiensten toe te laten gebruik te maken van politionele camerabeelden om real time-observaties uit te voeren. Deze methode, die een rechtstreekse toegang vereist tot de bedoelde informatie, werd nog niet geoperationaliseerd.

Uitzonderlijke methoden (ADIV)	Aantal toelatingen 2020	Aantal toelatingen 2021
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	4	14
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	39	60
TOTAAL	**51**	**89**

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 4 in 2020 naar 14 in 2021) en voor wat betreft het afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V) (van 39 in 2020 naar 60 in 2021). 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*".[200]

Het Comité wees de ADIV eerder[201] 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.

II.1.2.4. De opdrachten en de dreigingen die de inzet van (de gewone en) bijzondere methoden rechtvaardigen[202]

De ADIV mag de specifieke en uitzonderlijke methoden aanwenden in het kader van vier opdrachten[203] daarbij rekening houdend met verschillende dreigingen.

---

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

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

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

203 Deze methoden kunnen dus niet ingezet worden in het kader van veiligheidsonderzoeken of andere door of krachtens bijzondere wetten aan de ADIV toevertrouwde opdrachten (bijv. het verrichten van veiligheidsverificaties voor kandidaat-militairen).

1. **De inlichtingenopdracht (art. 11, 1° W.I&V)**
   Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties. Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die volgende belangen bedreigt of zou kunnen bedreigen:
   - de onschendbaarheid van het nationaal grondgebied of het voortbestaan van de gehele of een deel van de bevolking;
   - de militaire defensieplannen;
   - het wetenschappelijk en economisch potentieel op vlak van defensie;
   - de vervulling van de opdrachten van de strijdkrachten;
   - de veiligheid van de Belgische onderdanen in het buitenland.
2. **De zorg voor het behoud van de militaire veiligheid (art. 11, 2° W.I&V)**
   - de militaire veiligheid van het personeel dat onder de minister van Landsverdediging ressorteert;
   - de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen;
   - in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten.
3. **De bescherming van geheimen (art. 11, 3° W.I&V)**
   Het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de minister van Landsverdediging beheert.
4. **Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied (art. 11, 5° W.I&V).**

De inzet van bijzondere methoden is sinds de inwerkingtreding van de Wet van 30 maart 2017 niet meer beperkt tot het Belgische grondgebied (art. 18/1, 2° W.I&V). Door de ADIV werd meegedeeld dat er in 2021 geen BIM's werden

ingezet in het buitenland.[204] Deze bevoegdheid, dewelke nog nooit werd toegepast, werd nochtans in de memorie van toelichting van de Wet van 30 maart 2017 voorgesteld als zijnde een noodzakelijkheid om de ADIV toe te laten zijn 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.[205] 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 2022 nagaan of de ADIV (verkeerdelijk?) exclusief gebruik maakt van de INT-regeling beschreven in artikel 44 W.I&V.[206]

Er werden ook geen bijzondere inlichtingenmethoden ingezet op vraag van buitenlandse partnerdiensten.[207] Wel kan, aldus de ADIV, informatie verkregen 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 lichte daling worden opgetekend voor wat betreft de inzet van BIM's in het kader van de dreigingen 'spionage' en 'terrorisme'. Opmerkelijk is de sterke stijging van het aantal uitzonderlijke methoden ingezet in het kader van de dreiging 'extremisme' (van 20 in 2020 naar 82 in 2021). Het zal niet verbazen dat deze steile opgang te wijten is aan de zaak-Jurgen Conings[208] en de bijzondere aandacht voor extreemrechts binnen de Krijgsmacht als gevolg hiervan. Voor het eerst komen ook 'criminele organisaties' als dreiging aan de bod (29 ingezette methoden).[209]

---

204 Wel werd beroep gedaan op de mogelijkheden geboden door art. 44 W.I&V (zie hierover Hoofdstuk III. Het toezicht op buitenlandse intercepties, beeldopnamen en IT-intrusies).

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

206 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*".

207 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).

208 Zie 'Hoofdstuk I.9. Het opsporen en opvolgen van de radicalisering van een militair: de zaak-Jürgen Conings'.

209 Hiervoor bleken twee specifieke dossiers voor verantwoordelijk; één met betrekking tot wapenhandel/*organised crime* en een ander tot drugshandel (initieel opgestart in het kader van de opvolging van extreemrechts).

AARD DREIGING	AANTAL 2020	AANTAL 2021
Spionage	139	120
Inmenging	19	16
Extremisme - radicalisme	20	82
Terrorisme	19	9
Criminele organisatie	-	26
Andere	-	0
Totaal	**197**	**253**

Anders dan voor de inzet van bijzondere methoden, beschikt het Comité niet over de cijfers met betrekking tot de geviseerde dreiging en de te verdedigen belangen wat betreft de in dit hoofdstuk bedoelde gewone methoden. In zijn vorig activiteitenverslag beveelde het Comité de diensten aan ook deze gegevens te registreren en ter beschikking te stellen.[210] Dit gebeurde vooralsnog niet; het Comité herhaalt in dat kader dan ook zijn eerder geformuleerde aanbeveling.

II.1.3. METHODEN AANGEWEND DOOR DE VSSE

II.1.3.1. De gewone methoden 'plus'

Gewone methoden plus (VSSE)	Aantal toelatingen 2020	Aantal toelatingen 2021
Identificatie van de 'abonnee of de gewoonlijke gebruiker' van telecommunicatie	5123	4080
Gerichte opzoekingen PNR-gegevens[211]	30	98[212]
Gebruik van politionele camerabeelden	Niet in werking	46

Wat betreft de zogenaamde 'gewone methoden plus' is voor het derde jaar op rij een sterk daling (+/- 1000 aangevraagde identificaties) merkbaar van het aantal 'identificaties van de abonnee of gewoonlijke gebruiker van telecommunicatie'.[213] De inzet van methoden op basis van artt. 16/3 en 16/4 W.I&V kent daarentegen een gestage opgang. Het aantal toelatingen voor gerichte opzoekingen in de passagiers-

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

211 Met *profiling* wordt (nog) niet gewerkt

212 Het jaarrapport van BELPIU stelt dat "*de VSSE heeft […] 133 gerichte opzoekingen gerealiseerd*". Zie: Nationaal Crisiscentrum, *Jaarrapport BELPIU 2021*, 14.

213 In de praktijk wordt eerst het '*commun reference database centre*' (CRDC) geconsulteerd. Deze gegevensbank verstrekt uitsluitend informatie over de operator die het opgevraagde nummer uitbaat zonder vermelding of dit nummer werd toegekend aan een eindgebruiker. Er worden in deze 'gegevensbank voor nummerlocatie toegankelijk voor het publiek' geen persoonlijke gegevens opgeslagen.

gegevens (PNR) (art. 16/3 W.I&V) werd meer dan verdrievoudigd (van 30 naar 98). Het nut van deze methode neemt ook gestaag toe, nu het aantal aangesloten luchtvaartmaatschappijen ook exponentieel is toegenomen.[214] Vanaf 2021 kon ook een beroep worden gedaan op art. 16/4 §2 W.I&V dat de retroactieve opvraging regelt van politionele camerabeelden door de inlichtingendiensten.[215] De procedurele vereisten zijn zowel van toepassing op de gerichte opvragingen van politionele camerabeelden via een rechtstreekse (online) toegang tot de betrokken politionele gegevensbanken (actueel nog niet mogelijk) alsook op de gerichte opvragingen via een schriftelijke bevraging van de bevoegde politiediensten[216] (*in casu* de Directie van de politonele informatie en de ICT-middelen bij de Federale Politie (DRI)). De methode werd 46[217] keer ingezet.

De identificatie van prepaid-kaarthouders als methode wordt niet apart geregistreerd.

II.1.3.2. De specifieke methoden

Specifieke methoden (VSSE)	Aantal toelatingen 2020	Aantal toelatingen 2021
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)	245	195
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	0

214 "*Het aantal verwerkte passagiersgegevens lag in 2021 lager dan in 2019. Er werden daarentegen wel meer gegevens verwerkt dan in 2020 omdat de eenheid de passagiersgegevens van meer luchtvaartmaatschappijen verwerkt. Op dit moment worden de gegevens van* 94% van het internationaal luchtverkeer *verwerkt. Binnen de BelPIU wordt bovendien gerichter gewerkt met de passagiersgegevens en zijn er meer samenwerkingen met andere Europese Passagiers Informatie Eenheden (PIU's)*", in: Nationaal Crisiscentrum, *Jaarrapport BELPIU 2021*, 14.

215 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.

216 Vanaf de inwerkingtreding van de Camerawet van 21 maart 2018 moet artikel 16/4, §2 W.I&V gehanteerd worden als rechtsgrond voor het schriftelijk opvragen van politionele camerabeelden en kunnen de inlichtingendiensten hiervoor niet langer gebruik maken van artikel 14, tweede lid W.I&V. Zie hierover DPA-beslissing n° VCI-DPA/2022/2 (*supra*).

217 In 2021 werd enkel melding gemaakt van methoden dewelke één maand overstegen. In zijn DPA-beslissing n° VCI-DPA/2022/2 benadrukte het Comité dat '*schriftelijke DRI-bevragingen slechts kunnen plaatsvinden met respect van beide vernoemde procedurele vereisten (schriftelijke bevestiging én kennisgeving), en dit ongeacht of de toegang tot de politionele camerabeelden plaatsvindt tijdens of na de eerste bewaarmaand*'.

Specifieke methoden (VSSE)	Aantal toelatingen 2020	Aantal toelatingen 2021
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	1	0
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	70	33
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)	46	22
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)	650	491
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator (art. 18/8, §1, 2° W.I&V)	617	477
TOTAAL	**1629**	**1220**

Opnieuw nam de inzet van het aantal specifieke methoden duidelijk af (van 1629 naar 1220). Deze daling doet zich voor bij zowat alle specifieke methoden. Naar luid van de VSSE zijn hiervoor naast de supra vermelde algemene redenen (personeelsuitbreiding, coronamaatregelen) een aantal redenen aan te halen. Zo blijkt de inzet van de specifieke methode op basis van art. 18/6/1 W.I&V (het vorderen van vervoers- en reisgegevens) gelinkt aan de PNR-opvraging; gezien de stijging van het aantal gerichte opzoekingen van PNR-gegevens, nam de inzet van deze specifieke methode af (communicerende vaten).[218] Wat het doorzoeken van publiek toegankelijke plaatsen (art. 18/5 W.I&V) en kennisnemen van identificatiegegevens van postverkeer (art. 18/6 W.I&V)[219] betreft, verkiest de VSSE net zoals in 2020 de inzet van een uitzonderlijke methoden om met zekerheid binnen het wettelijk kader te opereren.

218 Voor data van vliegtuigmaatschappijen dewelke (nog) niet zijn opgenomen in BELPIU, gebeuren de aanvragen vooralsnog via art. 18/6/1 W.I&V. Het is de uitdrukkelijke wens van de VSSE om in de toekomst ook de deeleconomie (Uber, deelsteps DOTT) in dit kader te kunnen bevragen.

219 Gezien de ontvangen informatie met betrekking tot het postverkeer, is het meer aangewezen een uitzonderlijke methode aan te vragen.

II.1.3.3. De uitzonderlijke methoden

Uitzonderlijke methoden (VSSE)	Aantal toelatingen 2020	Aantal toelatingen 2021
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)	9	13
Al dan niet met behulp van technische middelen niet voor het publiek toegankelijke plaatsen doorzoeken, evenals al dan niet vergrendelde voorwerpen die zich daar bevinden (art. 18/12 W.I&V)	8	11
Een rechtspersoon als bedoeld in art. 13/3 § 1 W.I&V inzetten om gegevens te verzamelen (art. 18/13 W.I&V)	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	11	13
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	186	73
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	74	61
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	223	192
TOTAAL	**511**	**363**

Net als de inzet van specifieke methoden, nam ook het aantal door de VSSE ingezette uitzonderlijke methoden af (van 511 in 2020 naar 363 in 2021). Deze sterke daling is bijna volledig te wijten aan een halvering van de inzet van de methoden tot 'verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen' (art. 18/15 W.I&V) (van 186 in 2020 naar 73 in 2021).

De inzet van deze methode (het verwerken financiële gegevens) blijkt bijzonder arbeidsintensief te zijn.[220] Daarnaast valt een zij het lichtere daling van het aantal ingezette methoden inzake het afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V) (van 223 in 2020 naar 192 in 2021) op te tekenen. Ook voor de VSSE blijkt het inzetten van een rechtspersoon (art. 18/13 W.I&V) te veel middelen vragen.

II.1.3.4. De opdrachten en de dreigingen die de inzet van (de gewone en) bijzondere methoden rechtvaardigen

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

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

AARD DREIGING	AANTAL 2020	AANTAL 2021
Spionage	816	478
Inmenging	27	121
Extremisme - radicalisme	296	279
Proliferatie	3	2
Schadelijke sektarische organisaties	0	0
Terrorisme	998	690
Criminele organisaties	0	0
Activiteiten buitenlandse diensten in België opvolgen	(inbegrepen in bovenstaande cijfers)	(inbegrepen in bovenstaande cijfers)
TOTAAL	**2140**	**1570**

Bovenstaande tabel toont aan dat wat betreft de inzet van BIM-methoden in 2021 de dreiging 'terrorisme' weliswaar afneemt (van 998 naar 690), maar toch de absolute prioriteit blijft voor de VSSE en dit gevolgd door spionage. Waar in 2020

220 Het voorontwerp van wet tot wijziging van de Inlichtingenwet, waarover het Comité in 2021 een advies formuleerde, stelt in dit kader voor een nieuwe gewone methode in te voeren Deze creëert een medewerkingsverplichting voor financiële instellingen in de meeste ruime zin van het woord om over te gaan tot de identificatie van financiële producten of diensten waarover een persoon beschikt of, omgekeerd, om te identificeren welke persoon kan gelinkt worden aan bepaalde financiële producten of diensten. In de memorie van toelichting wordt deze keuze verantwoord door te stellen dat '*de intrusiviteit van een dergelijke methode […] gering tot zeer gering is*'. Het Comité is het hier niet mee eens. In zijn advies beveelt het Comité aan deze methode te kwalificeren als een specifieke methode (Advies nr. 001/VCI/2021 van 12 juli 2021 – Wijzigingen Inlichtingenwet).

nog sprake was van een sterke afname van het aantal 'inmengingsdossiers', kan opnieuw een sterke stijging worden vastgesteld (van 27 in 2020 naar 121 in 2021). 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' bleef stabiel (279 dossiers). Gezien schadelijke sektarische alsook criminele organisaties sinds 2015 niet meer het voorwerp uitmaken van actieve opvolging[221], hoeft het niet te verbazen dat deze dreigingen niet voorkomen in de cijfergegevens.

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.

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 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.

---

221 Zie hierover 'I.5. De opvolging van schadelijke sektarische organisaties en criminele organisaties' (*supra*).

II.2. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS (JURISDICTIONEEL) CONTROLEORGAAN EN ALS PREJUDICIEEL ADVIESVERLENER

II.2.1. CONTROLE OP BEPAALDE GEWONE METHODEN

II.2.1.1. Algemeen

De controle op bepaalde gewone methoden is voor elk van die methoden anders geregeld.

Wat betreft de identificatie van de gebruiker van telecommunicatie (en daarmee verbonden, de identificatie van de gebruiker van een prepaid-kaart), voerde de wet geen specifieke controle in. In artikel 16/2 §4 W.I&V werd alleen bepaald dat het Comité maandelijks in het bezit wordt gesteld van de lijst van de gevorderde identificaties en van de rechtstreekse toegang. Zoals hoger gesteld, ontvangt het Comité in dit kader alleen het aantal vorderingen. Het Comité nam zich echter voor om jaarlijks steekproefsgewijs een aantal vorderingen te controleren.[222]

Wat betreft de toegang tot PNR-gegevens die berusten bij de Passagiersinformatie-eenheid, bepaalt artikel 16/3 W.I&V dat die toegang alleen kan na beslissing van het diensthoofd en '*mits afdoende motivering*'. Het Comité moet hiervan in kennis worden gesteld en '*verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen*'. In 2021 werd door het Comité vier dergelijke verboden uitgesproken. Zowel drie beslissingen van de VSSE als een beslissing van de ADIV voldeden niet afdoende aan de wettelijk opgelegde motiveringsplicht. Beide diensten werd verboden de in het kader van deze dossiers verzamelde informatie te exploiteren.

Ten slotte werden aan het Comité bijzondere controlemodaliteiten toegekend in het kader van de mogelijkheid voor de inlichtingendiensten om toegang te

222 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.'*

krijgen tot informatie afkomstig van politionele camerabeelden (artikel 16/4 W.I&V): een *a priori*-controle[223] en een *a posteriori*-controle.[224]

II.2.2. CONTROLE OP BIJZONDERE METHODEN

II.2.2.1. De cijfers

In dit onderdeel wordt ingegaan op de activiteiten van het Vast Comité I met betrekking tot de specifieke en uitzonderlijke inlichtingenmethoden. Daarbij wordt uitsluitend aandacht besteed aan de ter zake genomen jurisdictionele beslissingen en niet aan de operationele gegevens. Vooraf dient evenwel te worden onderlijnd dat het Comité *alle* toelatingen tot de inzet van bijzondere methoden aan een *prima facie*-onderzoek onderwerpt, en dit met het oog op de al dan niet vatting. Tot vóór de coronamaatregelen, woonde een commissaris-auditor van de Dienst Enquêtes de (tweewekelijkse) vergaderingen bij waarop de betrokken inlichtingendienst de BIM-Commissie inlicht over de uitvoering van de uitzonderlijke methoden. Omwille van de voor de hand liggende redenen werden deze vergaderingen opgeschort. Zoals eerder vermeldt, wordt dit initiatief opnieuw opgenomen in het voorjaar van 2022.

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.

---

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

224 *'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.*'

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
1. Op eigen initiatief	16	12	16	3	1	1	4	2	1
2. Gegevensbeschermingsautoriteit	0	0	0	0	0	0	0	0	0
3. Klacht	0	0	0	1	0	0	0	0	0
4. Exploitatieverbod door BIM-Commissie[225]	5	5	11	19	15	10	12	9	8
5. Toelating minister	2	1	0	0	0	0	0	0	0
6. Prejudicieel adviesverlener	0	0	0	0	0	0	0	0	0
TOTAAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**	**9**

Het aantal door het Comité genomen beslissingen blijft dalen (van 11 in 2020 naar 9 in 2021). Bovendien zijn – één uitzondering niet te na gesproken – alle vattingen het gevolg van een schorsing door de BIM-Commissie. Het Comité werd in deze nog nooit gevat door de Gegevensbeschermingsautoriteit noch door een klacht.

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);

[225] Ze vloeien voort uit opnameproblemen of bij de verwijdering van apparatuur.

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
Beslissingen voorafgaand aan de vatting								
1. Nietige klacht	0	0	0	0	0	0	0	0
2. Kennelijk ongegronde klacht	0	0	0	0	0	0	0	0
Tussenbeslissingen								
3. Schorsing methode	3	2	1	0	0	0	1	0
4. Bijkomende informatie van BIM-Commissie	0	0	0	0	0	0	0	0
5. Bijkomende informatie van inlichtingendienst	1	1	4	0	0	0	1	1
6. Onderzoeksopdracht Dienst Enquêtes[226]	54	48	60	35	52	52	24	33
7. Horen BIM-Commissieleden	0	2	0	0	0	0	0	0
8. Horen leden inlichtingendiensten	0	2	0	0	0	1	1	0
9. Beslissing m.b.t. geheim van onderzoek	0	0	0	0	0	0	0	0
10. Gevoelige informatie tijdens verhoor	0	0	0	0	0	0	0	0

[226] 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.

AARD VAN DE BESLISSING	2014	2015	2016	2017	2018	2019	2020	2021
Eindbeslissingen								
11. Stopzetting methode	3	3	6	9	4	11	10	5
12. Gedeeltelijke stopzetting methode	10	13	4	6	6	4	0	3
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	0	4	11	0	0	0	0	0
14. Onbevoegd	0	0	0	0	0	0	0	0
15. Wettige toelating / Geen stopzetting methode / Ongegrond	4	6	2	1	1	0	0	1
Prejudicieel advies								
16. Prejudicieel advies	0	0	0	0	0	0		0

II.2.2.2. De rechtspraak

Hieronder wordt de essentie weergegeven van de eindbeslissingen die het Vast Comité I in 2021 nam binnen zijn jurisdictionele controle op de aanwending van de bijzondere inlichtingenmethoden.[227] De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk worden opgenomen.
De beslissingen werden gegroepeerd onder volgende rubrieken:
– De wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode;
– De wettigheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van de dreiging;
– De wettigheid van de uitvoering van een wettige methode.

[227] In sommige dossiers werd het Comité gevat in 2020, maar werd een eindbeslissing genomen in 2021.

De wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode

SUBSIDIARITEIT, PROPORTIONALITEIT EN DREIGINGSORIËNTATIE

Krachtens artikel 18/3, §1, eerste lid W.I&V kan een specifieke methode slechts door een inlichtingendienst worden aangewend ingeval er een tot de bevoegdheid van de betrokken dienst behorende potentiële dreiging voor de fundamentele belangen van het land aanwezig is. Daarnaast kan een dergelijke BIM-methode slechts worden ingezet indien de gewone methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die nodig is om de inlichtingenopdracht te volbrengen (de subsidiariteitseis). Tot slot eist vernoemde wetsbepaling dat een specifieke methode moet worden gekozen in functie van de graad van ernst van de potentiële dreiging waarvoor ze wordt aangewend (de proportionaliteitseis).

In dossier 2021/10548 wenste een inlichtingendienst de verkeers- en lokalisatiegegevens te bekomen die verliepen via een welbepaald telefoonnummer.[228] De inzet ervan kaderde binnen een door de inlichtingendienst gestarte operatie om na te gaan of een bepaalde ambtenaar betrokken was, bewust dan wel onbewust, bij spionageactiviteiten van een vreemde mogendheid. De medewerker was immers gedurende vele jaren in het betrokken land tewerkgesteld en aantal specifieke gedragingen van deze medewerker deden bij de inlichtingendienst de vraag rijzen of er door een inlichtingendienst van deze vreemde mogendheid ten aanzien van betrokkene gebruik werd gemaakt van de zogenaamde '*honey trap*'. Hierbij trachten buitenlandse inlichtingendiensten door middel van manipulatieve, amoureuze en seksuele avances informatie te bekomen van een persoon. Het profiel van deze medewerker sloot, *dixit* betrokken Belgische inlichtingendienst, aan bij het profiel dat door buitenlandse inlichtingendiensten als interessant beschouwd wordt voor de inzet van een dergelijke werkwijze. Via het vorderen van de verkeers- en lokalisatiegegevens wou de Belgische inlichtingendienst de sociale en professionele contacten van de betrokken medewerker in kaart brengen. Vervolgens kon dan nagegaan worden of deze contacten geoorloofd waren in het kader van de uitoefening van zijn functie, dan wel of het ging om onofficiële, ongepaste en/of niet-geoorloofde contacten waarvan een eventuele dreiging uitging.

De BIM-Commissie besloot de uitvoering van deze specifieke methode te schorsen. Ze was van oordeel dat de door de inlichtingendienst aangehaalde argumenten en feitelijke gegevens niet aantoonden dat er ernstige en op feiten beruste gronden bestonden om aan te nemen dat er tegen betrokkene aanwijzingen bestonden dat hij zich zou inlaten met clandestiene inlichtingenactiviteiten voor een buitenlandse inlichtingendienst. De Commissie stelde dat de door de inlichtingendienst ingeroepen gedragingen onvoldoende waren om hieruit te kunnen

[228] *Cf.* artikel 18/8, §1, eerste lid, 1° en 2° W.I&V.

concluderen dat deze mogelijks het voorwerp was geweest van een *Honey Trap*. Tevens was de Commissie van oordeel dat de inlichtingendienst onvoldoende omstandig motiveerde dat de gevraagde methode in verhouding stonden met de ernst van de dreiging (proportionaliteit) en dat het door de methoden na te streven doel, in acht genomen de stand van het inlichtingenonderzoek, niet op minder ingrijpende wijze kon worden bereikt (subsidiariteit). Wat dit laatste aspect betreft, was de Commissie van oordeel dat nog heel wat informatie kon bekomen worden via gewone methoden (bv. een persoonlijkheidsonderzoek van target).

Krachtens artikel 43/4 W.I&V is het Vast Comité I van rechtswege gevat telkens wanneer de Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden. In tegenstelling tot de Commissie was het Comité echter van oordeel dat de door de inlichtingendienst ingeroepen gedragingen wél afdoende waren om het bestaan van een potentiële dreiging aan te tonen, althans in combinatie met de specifieke functie van betrokkene, de gevoelige positie die hiermee gepaard ging alsook het specifieke (privé-)profiel van betrokkene. Ook oordeelde het Comité dat de vereisten inzake subsidiariteit en proportionaliteit door de inlichtingendienst waren gerespecteerd.

BIJZONDERE TOELATINGSPROCEDURE BIJ BESCHERMDE BEROEPSCATEGORIEËN

In zijn *Activiteitenverslag 2020* deelde het Vast Comité I mee dat het in dat jaar voor het eerst sinds de inwerkingtreding van de BIM-Wet van 4 februari 2010, een prejudiciële vraag gesteld had aan het Grondwettelijk Hof aangaande de BIM-wetgeving (dossier 2020/9606).[229] De aanleiding was een beslissing van een inlichtingendienst om de in artikel 18/8, §1, 1° en 2° W.I&V bedoelde specifieke methoden aan te wenden tegen een door een arts gebruikte telefoonnummer. Via een gewone methode bleek het geviseerde telefoonnummer enkel op naam van betrokkene in België te zijn geregistreerd. Hoewel de inlichtingendienst wist dat het om een arts ging, volgde ze de gewone toelatingsprocedure voor specifieke methoden.[230] De BIM-Commissie was het hiermee niet eens en schorste de lopende methoden. Gelet op de hoedanigheid van de geviseerde persoon, zijnde arts, moest volgens de Commissie gebruik gemaakt worden van de bijzondere toelatingsprocedure voor beschermde beroepscategorieën voorzien in artikel 18/3, §5 W.I&V: *'(d)e specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen- en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief*

229 VAST COMITÉ I, *Activiteitenverslag 2020*, 94-97.

230 Meteen nadat de inlichtingendienst zijn fout had ingezien, werd een nieuwe aanvraag ingediend, rekening houdende met het gegeven van de beschermde beroepscategorie.

meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële dreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op het ontwerp van beslissing van het diensthoofd'. Deze bijzondere procedure komt er dus op neer dat wanneer een inlichtingendienst een specifieke methode wenst aan te wenden jegens artsen, advocaten of journalisten de toelatingsprocedure voor uitzonderlijke methoden dient gevolgd te worden. Op deze wijze wordt elke methode vóór zijn aanwending onderworpen aan een voorafgaande controle van de BIM-Commissie. Naast de schorsing van de betrokken methode, legde de BIM-Commissie een exploitatieverbod op voor de, desgevallend, reeds verkregen gegevens.

Het schorsingsbevel van de BIM-Commissie zorgde voor de ambtshalve vatting van het Vast Comité I. Gelet op het belang van het bijzondere beschermingsregime van vernoemde beroepscategorieën en vanuit zijn hoedanigheid van rechtsprekend orgaan[231] binnen het toezicht op de specifieke en uitzonderlijke methoden, besloot het Comité om volgende prejudiciële vraag te stellen aan het Grondwettelijk Hof: *'Schendt artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten de artikelen 10 en 11 van de Grondwet, alleen gelezen of in samenhang met artikel 22 van de Grondwet en/of al dan niet gecombineerd met artikel 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden, ondertekend te Rome op 4 november 1950 en goedgekeurd bij wet van 13 mei 1955, in zoverre het een advocaat, arts of journalist geen bijzondere bescherming biedt bij communicatiemiddelen die hij voor andere dan beroepsdoeleinden gebruikt?'*.[232] Het Comité merkte immers op dat artikel 18/2, §3, eerste en tweede lid W.I&V de aan advocaten, artsen en journalisten verleende bescherming beperkt tot de communicatiemiddelen die zij voor beroepsdoeleinden gebruiken. Uit de huidige tekst van vernoemde bepaling volgt dat communicatiemiddelen die zij voor andere dan beroepsdoeleinden gebruiken niet onder de wettelijke bescherming (lijkt te) vallen.

In april 2021 deed het Grondwettelijk Hof uitspraak: *'Onder voorbehoud van de in B.15.2 vermelde interpretatie schendt artikel 18/2, § 3, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten niet de artikelen 10, 11 en 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens'*.[233] Overweging B.15.2 stelt: *'Gelet op de bijzondere bescherming die voor alle medische gegevens moet gelden, met name krachtens de rechtspraak van het Europees Hof voor de Rechten van de Mens en het Belgische strafrecht, moet artikel 18/2, § 3, van de wet van 30 november 1998 in die zin worden geïnterpreteerd dat het de inlichtingen- en veiligheidsdiensten verplicht om de door de wetgever geboden bescherming voor de communicatiemiddelen die voor beroepsdoeleinden worden gebruikt, toe te passen wanneer het niet vaststaat*

231 GwH 22 september 2011, nr. 145/2011, overw. B.38.1.
232 Vrije vertaling.
233 GwH 22 april 2021, nr. 64/2021.

dat het door een arts gebruikte communicatiemiddel uitsluitend werd aangewend om andere doeleinden dan beroepsdoeleinden.'.

Volgend op het arrest van het Grondwettelijk Hof neemt het Vast Comité I een eindbeslissing in voorliggend BIM-dossier: *'Gelet op de hoedanigheid van [persoon X] als arts en indachtig het arrest n° 64/2021 van 22 april 2021 van het Grondwettelijk Hof, is de [betrokken inlichtingendienst] in voorliggend dossier verplicht om aan te tonen dat betrokken communicatiemiddel door [persoon X] uitsluitend wordt aangewend om andere doeleinden dan beroepsdoeleinden, opdat [betrokken inlichtingendienst] op rechtmatige wijze de gewone procedure voor specifieke methoden mag aanwenden. Het Comité stelt vast dat de motivering van de [betrokken inlichtingendienst] in de bestreden beslissing zich beperkt tot de mededeling dat « de selector XXX de enige bleek te zijn die in België op zijn naam geregistreerd stond ». Deze vaststelling is niet afdoende om aan te tonen dat betrokken communicatiemiddel door [persoon X] uitsluitend wordt aangewend om andere doeleinden dan beroepsdoeleinden. Ten gevolge hiervan heeft de [betrokken inlichtingendienst] op onregelmatige wijze gebruik gemaakt van de gewone procedure voor specifieke methoden.'.*[234]

NIET-TIJDIGE NOTIFICATIE AAN DE BIM-COMMISSIE

Een inlichtingendienst wenste over te gaan tot de verlenging van een specifieke methode, meer bepaald een observatie met technische hulpmiddelen van een voor het publiek toegankelijke plaats (dossier 2021/10346). Krachtens artikel 18/3, §4 W.I&V kan een verlenging (of hernieuwing)[235] van een specifieke methode slechts plaatsvinden na een nieuwe beslissing van het diensthoofd én na een kennisgeving hiervan aan de BIM-Commissie. De toegelaten uitvoeringsperiode van de eerste specifieke methode liep af de 25e van de maand om 24h. De beslissing van het diensthoofd tot verlenging van de observatie, hoewel genomen op de 25e van de maand, werd echter pas op de 26e van de maand om 9h45 aan de BIM-Commissie genotificeerd. Het Comité instrueerde, in navolging van het door de BIM-Commissie uitgesproken exploitatieverbod, dat de gegevens verkregen gedurende de niet gedekte periode niet mochten worden geëxploiteerd en moesten worden vernietigd.

234 Vrije vertaling.

235 Hoewel artikel 18/3, §4 W.I&V geen onderscheid maakt tussen een 'verlenging' van een specifieke methode en een 'hernieuwing' wat betreft de na te leven formele voorwaarden (*i.c.* beslissing van het diensthoofd én notificatie aan de BIM-Commissie) dient een inlichtingendienst in het beheer van betrokken methode een grotere aandacht aan de dag te leggen bij een verlenging. Zo niet bestaat het gevaar dat er periodes zijn waarin een lopende specifieke methode niet gedekt wordt door een genotificeerde beslissing waardoor er op onrechtmatige wijze gegevens ingewonnen worden. Zie ook: VAST COMITÉ I, *Activiteitenverslag 2020*, 98.

GEEN MONDELING EENSLUIDEND ADVIES VAN DE VOORZITTER VAN DE BIM-COMMISSIE

Krachtens artikel 18/10, §4, eerste lid W.I&V kan, in geval van hoogdringendheid, een uitzonderlijke methode door het diensthoofd van een inlichtingendienst mondeling gemachtigd worden doch slechts na een mondeling eensluidend advies van de voorzitter van de BIM-Commissie. In dossier 2021/10612 werd door een inlichtingendienst, per vergissing en binnen een context van hoogdringendheid, een afluistering (*ex* art. 18/17, §§ 1 en 3 W.I&V) zonder eensluidend advies van de voorzitter van de Commissie opgestart. De betrokken inlichtingendienst stelde deze vergissing zelf vast, waarschuwde daaropvolgend onmiddellijk de BIM-Commissie en zette de onrechtmatig verkregen gegevens reeds in quarantaine. Zoals wettelijk voorzien, verbood de Commissie de exploitatie van de betrokken gegevens en verwittigde ze het Vast Comité I, waarop deze het bevel gaf om de onrechtmatig verkregen gegevens te vernietigen.

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

VERKEERD VOORWERP VAN DE METHODE

In dossier 2020/10180 bleek de inlichtingendienst in zijn toelating per vergissing een telefoonnummer te hebben vermeld dat niet geviseerd werd door de betrokken specifieke methode (*i.c.* het opvragen van de verkeers- en lokalisatiegegevens inzake elektronische communicatie bedoeld in artikel 18/8, §1, eerste lid, 1° en 2° W.I&V). Ook in de daaropvolgende vordering aan de telecomoperator werd dit verkeerd oproepnummer vermeld. De dienst merkte dit zelf op, evenwel nadat de gevorderde gegevens reeds van de telecomoperator werden verkregen. De inlichtingendienst plaatste eigenmachtig de verkregen gegevens in elektronische quarantaine en bracht de BIM-Commissie van de vergissing op de hoogte. De Commissie verbood de exploitatie van de onrechtmatig verkregen gegevens, verwittigde het Vast Comité I, waarop laatstgenoemde het bevel gaf om de onwettelijk bekomen gegevens te vernietigen.

DUUR VAN DE METHODE

Krachtens artikel 18/10, §2 W.I&V moet het ontwerp van machtiging aangaande de aanwending van een uitzonderlijke methode op straffe van onwettigheid de periode vermelden waarin de methode kan worden aangewend. De wettelijke toelatingsprocedure voor uitzonderlijke methoden vereist vervolgens een eensluidend advies van de BIM-Commissie. Voorafgaand aan dit advies gaat de Commissie de

wettigheid, de subsidiariteit en de proportionaliteit na. Eén van de door de Commissie te controleren aspecten vormt de voorgestelde uitvoeringsperiode.

In dossier 2021/10428 had een inlichtingendienst een verlenging aangevraagd voor een afluistering zoals bedoeld in artikel 18/17, §§ 1 en 2 W.I&V. In het ontwerp van machtiging werden evenwel twee verschillende uitvoeringsperioden vooropgesteld (nl. één maand vs. twee maanden). De Commissie leverde een eensluidend advies op dit ontwerp van machtiging en verleende haar akkoord voor een uitvoeringsperiode van twee maanden. Van belang is dat de Commissie in zijn eensluidend advies evenwel niet nader ingaat op het feit dat het ontwerp van machtiging twee verschillende uitvoeringsperiodes vermeldde. Het was bijgevolg niet duidelijk of een doelbewuste keuze werd gemaakt tussen de twee door de betrokken dienst voorgestelde periodes. Het Vast Comité I vatte zich in dit dossier ambtshalve. Het stelde *'dat de vermelding van deze verschillende data (1 maand, respectievelijk 2 maanden) in het ontwerp van machtiging waarschijnlijk op een materiële vergissing berust.'*. Aangezien echter het Comité van oordeel was *'dat, zelfs bij een materiële vergissing, met het oog op het streven naar duidelijkheid en rechtszekerheid, een uitzonderlijke methode enkel kan worden toegestaan voor de kortste periode vermeld in het ontwerp van machtiging.'*. Het Comité besloot dat de uitzonderlijke methode wettig was voor een periode van één maand vanaf de machtiging van het diensthoofd.

De wettigheid van de uitvoering van een wettige methode

VERKEERDE ONTVANGEN GEGEVENS

In drie afzonderlijke dossiers (2021/10533, 2021/10550 en 2021/10982) had de betrokken inlichtingendienst op wettige wijze beslist tot het opsporen van elektronische communicatie[236] en tot het lokaliseren van de oorsprong of de bestemming van elektronische communicatie.[237] Maar er stelde zich een probleem bij de overmaking van de gevorderde gegevens in de zin dat de door de dienst NTSU-CTIF[238] overgemaakte gegevens geen betrekking hadden op de gevorderde gegevens. *In casu* werd telkenmale door een foutieve manipulatie bij de dienst NTSU-CTIF in plaats van een lokalisatie een afluistering[239] opgestart. Het betrof dus een onwettigheid buiten de wil van de inlichtingendienst om. In alle drie de gevallen werd dit door de betrokken inlichtingendienst zelf vastgesteld. De BIM-Commissie en de dienst NTSU-CTIF werd telkenmale na de vaststelling onmiddellijk in kennis

236 *Cf.* artikel 18/8, §1, eerste lid, 1° W.I&V (specifieke methode).
237 *Cf.* artikel 18/8, §1, eerste lid, 2° W.I&V (specifieke methode).
238 De dienst NTSU-CTIF (*National Technical & Tactical Support Unit – Central Technical Interception Facility*) is de Centrale Technische Interceptiefaciliteit van de geïntegreerde politie. Zie : Koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie.
239 *Cf.* artikel 18/17 W.I&V (uitzonderlijke methode).

gesteld. In alle drie de gevallen besliste de betrokken inlichtingendienst ook uit eigen beweging om de onregelmatig verkregen gegevens ontoegankelijk te maken. De BIM-Commissie sprak telkenmale een exploitatieverbod uit, gevolgd door een vernietigingsbevel van het Vast Comité I.

II.3. ALGEMENE VASTSTELLINGEN

Het Vast Comité I formuleert volgende algemene vaststellingen:

- Tussen 1 januari en 31 december 2021 werden door de twee inlichtingendiensten samen 1823 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 1570 door de VSSE (waarvan 1220 specifieke en 350 uitzonderlijke) en 253 door de ADIV (waarvan 166 specifieke en 87 uitzonderlijke). Na een constante stijging van het totale aantal ingezette BIM's de afgelopen jaren en een stagnatie in 2019-2020, dient een significante daling te worden opgetekend.
- De VSSE blijft het leeuwendeel van de ingezette methoden voor zijn rekening nemen (86 %). Afgelopen jaar kon een lichte inhaalbeweging door de ADIV worden vastgesteld.
- Als de globale cijfers worden uitgesplitst, dient voor 2021 een aanzienlijke stijging (ca. 30%) bij de ADIV worden opgetekend van de inzet van zowel specifieke (van 146 naar 166) als uitzonderlijke methoden (van 51 in 2020 naar 87 in 2021). De VSSE laat een opmerkelijke daling optekenen (circa 28%) van het aantal ingezette specifieke (van 1629 naar 1220 in 2021) alsook uitzonderlijke methoden (van 511 naar 350) ten overstaan van 2020.
- Wat betreft de gewone methoden van vorderingen gericht aan operatoren om bepaalde communicatiemiddelen te identificeren betreft, wordt opnieuw – en dit voor zowel de ADIV als de VSSE – een daling opgetekend. Desalniettemin steeg het aantal selectoren bij de ADIV met bijna 20%. Voor de Veiligheid van de Staat bleef het aantal selectoren eerder stabiel.
- Er werd door beide inlichtingendiensten voor het eerst de gewone methode plus 'gebruik van politionele camerabeelden' ingezet. Het aantal gerichte opzoekingen van PNR-gegevens nam voor beide diensten gestaag toe.
- Er konden nog voorlopig geen gevolgen van de door het Grondwettelijk Hof vernietigde Dataretentiewet worden vastgesteld.
- Verder kan voor de VSSE worden genoteerd dat het aantal ingezette BIM's voor wat betreft de dreigingen 'terrorisme' en 'spionage' in belangrijkheid afnamen, maar nog steeds de belangrijkste dreigingen vormen. Er werd opnieuw een stijging vastgesteld van het aantal inmengingsdossiers; de dreiging 'extremisme-radicalisme' bleef stabiel.
- Bij de ADIV was een opmerkelijke stijging zichtbaar bij de inzet van BIM-methoden voor de dreiging 'extremisme-radicalisme', te wijten aan het dossier

Jurgen Conings en de bijzondere aandacht voor extreemrechts binnen de Krijgsmacht als gevolg hiervan. De dreiging 'spionage' was evenwel het meeste aan de orde.

- De ADIV heeft (nog) geen BIM's in het buitenland ingezet. Een meer diepgaand onderzoek moet toelaten vast te stellen of de militaire inlichtingendienst effectief nog geen BIM's heeft ingezet in het buitenland dan wel of er (verkeerdelijk) beroep wordt gedaan op de mogelijkheden geboden in artikel 44 W.I&V. Een dergelijk onderzoek schrijft zich in in de filosofie van de memorie van toelichting van de Wet van 30 maart 2017 dat stelt 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"*.
- Het Comité werd gevat in negen dossiers, waarvan één vatting op eigen initiatief en acht van rechtswege nadat de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid had geschorst (art. 43/4 W.I&V). Onwettigheden betroffen onder meer problemen met de duur en het voorwerp van de methoden, verkeerde ontvangen gegevens of nog, de niet-tijdige verwittiging van de BIM-Commissie.
- Het Vast Comité I heeft in 2020 voor het eerst sinds de inwerkingtreding van de BIM-wet een prejudiciële vraag gesteld aan het Grondwettelijk Hof aangaande de BIM-wetgeving. In april 2021 deed het Hof hierover uitspraak.

De keuze van de BIM-wetgever in 2010 om in de Inlichtingenwet een logische structuur in te stellen voor wat betreft de (onderzoeks)bevoegdheden van de inlichtingendiensten (o.m. een onderscheid in uitzonderlijke, specifieke en gewone methoden naargelang de graad van privacy inmenging) werd door de wetswijzigingen van de laatste jaren grotendeels verlaten. De recente voorstellen tot wijziging van de Inlichtingenwet[240] brengen op dat vlak weinig verbetering. Het Comité betreurt dat de regelgeving hierdoor als maar complexer en meer onsamenhangend wordt. Een wetgevend initiatief, waartoe het Vast Comité I steeds bereid kan worden gevonden om hieraan zijn bijdrage te leveren, dringt zich op. Dit kan, voor zowel de burger als de inlichtingendiensten, een grotere rechtszekerheid bieden.

[240] Hierover 'Hoofdstuk VI.4. Advies betreffende het voorontwerp van wet tot wijziging van de Inlichtingenwet'.

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[241]

Al in 2017 werd de bevoegdheid van de Algemene Dienst Inlichting en Veiligheid (ADIV) in het kader van de veiligheidsintercepties uitgebreid.[242] 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.[243] Dit betekent dat er naast een jaarlijks interceptieplan, ook een intrusie- en beeldplan dient te worden opgesteld door de ADIV.[244] 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

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

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

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

244 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[245] die op zijn beurt de lijsten, voorzien van de toelating van de minister, overzendt aan het Vast Comité I.[246]

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[247], werd evenwel nog steeds geen dergelijk interceptie-KB getroffen.[248] Het Comité beveelt dan ook opnieuw aan om dit zo spoedig mogelijk te doen.

---

245 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.

246 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.

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

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

III.2. HET IN 2021 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 midden januari 2021.

Voorafgaand aan het toezenden van deze documenten, organiseerde de ADIV een werkvergadering hierover met het Comité. Tijdens deze vergadering werden er door het Comité een aantal opmerkingen geformuleerd aangaande de na te leven wettelijke vereisten. Bij de ontvangst van de plannen op het Comité kon worden vastgesteld dat, conform zijn aanbevelingen, de drie plannen (het interceptie-, beeldopname- en intrusieplan) werden gebundeld in één document. Op deze wijze trachtte de ADIV op korte termijn het geheel van plannen dat de dienst realiseert in uitvoering van artikel 44 W.I&V, te uniformiseren. Het Comité kon vaststellen dat, met inbegrip van de geformuleerde opmerkingen waarmee rekening werd gehouden, de plannen voldeden aan alle wettelijke vereisten.

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

In de loop van 2021 heeft het Comité de installaties van waaruit de intercepties gebeuren, bezocht. Tijdens het bezoek werd, onder meer, nagegaan of het logboek in overeenstemming was met de desbetreffende wetten en richtlijnen. Het Vast Comité I diende kleine gebreken vast te stellen, dewelke meteen werden rechtgezet door de verantwoordelijke ter plaatse.

Het Comité realiseerde tevens, en voor het eerst, een controle op de site van de dienst van ADIV belast met de uitvoering van het intrusieplan. Bij deze gelegenheid kon het Comité vaststellen dat de dienst geleidelijk aan zijn volledige operationele capaciteit bereikt. Ook hier werd aan de toepasselijke wettelijke vereisten herinnerd (en meer bepaald aan de verplichting tot het bijhouden van een *logbook*) en werd de dienst verzocht deze na te leven. Dit element zal zeker de aandacht krijgen van het Comité bij de eerstvolgende bezoeken.

Wat betreft het beeldopnameplan kon het Vast Comité I in 2021 geen controle uitvoeren van de installaties. Deze controle zal prioritair worden uitgevoerd in 2022.

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

Het Comité ontving twaalf '*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°*'.

Het Vast Comité I ontving dus het geheel van de lijsten zoals wettelijk voorzien. De vorm en de inhoud van deze lijsten zullen, in samenspraak met de ADIV, het voorwerp uitmaken van een evaluatie in 2022.

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)[249] en de Richtlijn 2016/680 (Richtlijn)[250] 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)[251] – de opvolger van de Privacycommissie – opgericht en in juli 2018 werd een nieuwe Gegevensbeschermingswet (GBW) gestemd.[252] 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).[253]

---

249 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.

250 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.

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

252 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.

253 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. Achtereenvolgens worden volgende thema's besproken:

- 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;
- de melding in het kader van een mogelijke *data breach*;
- de werkzaamheden in het kader van de evaluatie van de Gegevensbeschermingswet.

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.

Om ontvankelijk te zijn, moet het verzoek geschreven, gedateerd, ondertekend en met redenen omkleed zijn (art 51/2 W.Toezicht).[254] 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.[255]

---

254 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).

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

De onderstaande tabel bevat een overzicht van de in 2021 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 (TA).[256]

[256] In de tabel zijn dus niet de hypothesen opgenomen waarin er kon worden samengewerkt met een andere toezichthoudende autoriteiten (bijv. het COC) wanneer de bevoegdheden van elke TA duidelijk zijn onderscheiden.

Tabel 1. Behandeling van individuele verzoeken[257]

2021	Vast Comité I		Vaste Comités I en P	Vaste Comités I en P en het COC	Totaal
1. Dossiers geopend in 2021	14		2	0	16
2. Onontvankelijke verzoeken 2021	3		0	0	3
3. Ontvankelijke verzoeken 2021	8		0	0	8
	t. ADIV	2			
	t. VSSE	6			
	t. VSSE&ADIV	-			
4. Hangende verzoeken in 2021	3		0	0	0
5. Lopende dossiers in 2021	10[258]		1	2[259]	13
6. Afgesloten dossiers in 2021[260]	10[261]		2[262]	1[263]	13
7. Corrigerende maatregelen	3		0	1	4
8. Totaal behandelde verzoeken	20		3	3	26

In 85% van de verzoeken beweren de betrokkenen[264] dat er sprake is van concrete inmenging in hun rechten en vrijheden als gevolg van, of in ieder geval in verband met, een verwerking van gegevens door een verwerkingsverantwoordelijke

257 De eerste regel geeft aan hoeveel dossiers er in 2021 werden geopend. Regels 2 en 3 verdelen de dossiers naargelang de beslissing tot ontvankelijkheid of ontontvankelijkheid. 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. Regel 4 betreft dossiers waarbij de ontvankelijkheidsbeslissing nog hangende is. De regels 5 en 6 tonen de vooruitgang in de dssiers aan (nog lopende of reeds afgesloten). Regel 7 ten slotte geeft het aantal dossiers aan waarin door het Comité corrigerende maatregelen werden opgelegd.

258 Waarvan één dossier geopend in 2020.

259 Waarvan twee dossiers geopend in 2020.

260 Volledig afgesloten. Wanneer corrigerende maatregelen werden opgelegd, sluit het Vast Comité I het dossier af wanneer kon worden vastgesteld dat de maatregelen werden uitgevoerd.

261 Waarvan vijf dossiers geopend in 2020.

262 Waarvan één dossier geopend in 2020.

263 Waarvan één dossier geopend in 2020.

264 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 (bv. 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.

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 is geweigerd, wanneer gegevens van een inlichtingendienst zijn gebruikt in strafrechtelijke procedures, enz.

In 2021 diende het Comité 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.

Een in 2020 ingediend verzoek heeft ook geleid tot de opening van een informatiedossier in 2021. Tijdens de behandeling van het verzoek kon het Vast Comité I immers praktijken vaststellen die niet in overeenstemming waren met de wettelijke voorschriften. Op basis van dat individuele verzoek, heeft het Comité de algemene verwerking van persoonsgegevens door de inlichtingendiensten in een specifieke context aan een onderzoek onderworpen.

De resterende 15% 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 (85-15%) 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.

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 betrek-

king 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 2021 in totaal drie adviezen verleend in deze hoedanigheid, waarvan twee wat betreft de uitwisseling van geclassificeerde informatie[265] en één aangaande een voorontwerp van wet tot wijziging van de W.OCAD als gezamenlijk bevoegde toezichthoudende autoriteit (met het Vast Comité P)[266]:

- Advies 005/VCI/2021 van 1 december 2021 aangaande een vraag tot advies van de voorzitter van de Nationale Veiligheidsoverheid met betrekking tot het '*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*';
- Advies 006/VCI/2021 van 1 december 2021 aangaande een vraag tot advies van de voorzitter van de Nationale Veiligheidsoverheid met betrekking tot het '*Wetsontwerp houdende instemming met de Overeenkomst tussen het Koninkrijk België en het Verenigd Koninkrijk en Noord-Ierland inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 1december 2020*'.
- Gezamenlijk advies VCI-VCP 001/2021 van 8 oktober 2021 over '*het voorontwerp van wet tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging*'.

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.[267] 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).

---

265 In 2019 en 2020 werden in die zin al adviezen verleend over de uitwisseling van geclassificeerde informatie met de Republiek Cyprus, Hongarije, de Republiek Finland, het Koninkrijk Spanje, de Franse Republiek en de Italiaanse Republiek.

266 Zie *in extenso* op de website van het Vast Comité I.

267 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.

In 2021 werd in de pers gewag gemaakt van een *hacking* van het computernetwerk van de FOD Binnenlandse Zaken.[268] Daarop meldde de directeur van Belgische Passagiersinformatie-eenheid (BELPIU) spontaan dat het afgescheiden Passenger Name Record (PNR) IT-systeem niet was gecompromitteerd. Dit bleek uit een door het Centrum voor Cybersecurity België (CCB) uitgevoerde scanning.

IV.5. EVALUATIE VAN DE GEGEVENSBESCHERMINGSWET

Artikel 286 GBW bepaalt dat de Gegevensbeschermingswet in het derde jaar na de inwerkingtreding ervan moet worden onderworpen aan een gezamenlijke evaluatie door de bevoegde ministers. In deze context richtte staatsecretaris Mathieu Michel een schrijven tot het Comité met de vraag zijn medewerking te verlenen aan het door hem opgerichte oriëntatiecomité. Het Vast Comité I bezorgde daarop verschillende documenten met daarin zowel meer algemene als zeer specifieke, technisch-juridische voorstellen ter versterking van de dataprotectie.[269]

[268] H. DECREM en L. BELGHMIDI, www.vrt.be, 26 mei 2021 ("Twee jaar lang 'doelbewuste cyberaanval op overheidsdienst Binnenlandse Zaken: 'Dit is spionage").

[269] Zie hiervoor: VAST COMITÉ I, *Activiteitenverslag 2020*, 119-125 ('V.7. Evaluatie van de gegevensbeschermingswet').

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 (verder 'de toezichthoudende autoriteiten'). Dit resulteerde in een gemeenschappelijk verslag dat begin oktober 2021 werd besproken in de schoot van de parlementaire Begleidingscommissie.[270]

V.1. DE CONTROLEOPDRACHT EN HET VOORWERP VAN CONTROLE

Voor wat betreft 2020/2021 beslisten het Vast Comité I en het COC om de gezamenlijke controle te focussen op, enerzijds, de verificatie van de rechtstreekse toegang toegekend aan de Nationale Veiligheidsoverheid (NVO) en, anderzijds, op de opvolging van bepaalde aanbevelingen die in de rapporten van de afgelopen jaren werden geformuleerd.

---

270 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.

Daarnaast werd eveneens de coördinatie van de gegevensverwerking van informatie in de GGB TF en HP aan een grondig onderzoek onderworpen, onder meer met aandacht voor de rol van de *data protection officer* (DPO). Het stijgend aantal diensten dat een toegang heeft tot de GGB TF en HP werd daarbij eveneens in rekening genomen.

Vanuit methodologisch oogpunt werd, met de sanitaire crisis in het achterhoofd en om de diensten voldoende tijd te geven om de aanbevelingen uit het verslag over de in 2019 uitgevoerde controle uit te kunnen voeren, besloten om de nieuwe bevraging pas in het vierde kwartaal van 2020 te laten plaatsvinden. Verschillende diensten werden bevraagd, waaronder de NVO, het OCAD (operationeel beheerder van de gemeenschappelijke gegevensbanken), de Federale Politie (technisch beheerder) en de *data protection officers* (DPO). Het onderzoek werd afgesloten met een vergadering met de waarnemend directeur van OCAD en de DPO van de gemeenschappelijke gegevensbanken.

V.2. ONDERZOEKSVASTSTELLINGEN

V.2.1. HET GEBREK AAN TOEGANG VAN DE NVO

Ten tijde van de controle hebben het COC en het Vast Comité I vastgesteld dat de NVO niet verbonden was met de GGB en daartoe ook niet de minste actie had ondernomen.

Het COC en het Vast Comité I waren van mening dat de NVO blijk gaf van kennelijke en onverantwoorde nonchalance. Haar gebrek aan handelen, dat in strijd was met de toepasselijke regelgeving deed veiligheidsrisico's ontstaan, niet alleen wat betreft de stelselmatige raadpleging van de GGB maar ook wat betreft de gegevensinvoer in de GGB. De Federale Politie verklaarde dat ze geen gegevens invoerde in de GGB in het kader van de veiligheidsverificaties (en evenmin van de veiligheidsmachtigingen). Niets wees erop dat dergelijke invoer op stelselmatige wijze werd verricht door de inlichtingendiensten wat betreft de veiligheidsmachtigingen. Bijgevolg konden mogelijkerwijs diverse interessante of zelfs cruciale inlichtingen ontsnappen aan de aandacht van de diensten.

Anderzijds, rekening gehouden met het feit dat de NVO geen exclusieve bevoegdheid geniet als veiligheidsoverheid, en teneinde garanties te bieden voor de volledigheid van de GGB, bevolen het COC en het Vast Comité I aan de verschillende veiligheidsautoriteiten zoals bedoeld in de artikelen 15, lid 2 en 22*ter*, lid 2 van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheids-adviezen (W.C.&VM) en 9, lid 1,

9° van de Wet van 28 februari 2007[271] aan zich te vergewissen van de effectieve raadpleging van de GGB in de verschillende processen waarvoor ze bevoegd zijn en om hun beslissingen in te voeren in de GGB, hetzij op basis van hun rechtstreekse toegang tot de GGB of door daartoe contact op te nemen met een basisdienst (in het geval waarin ze geen rechtstreekse toegang hebben).

Het COC en het Vast Comité I kondigden aan deze verschillende aspecten te verifiëren in het kader van latere controles.

V.2.2. DE OPVOLGING VAN DE VROEGERE AANBEVELINGEN

V.2.2.1. Aanbevelingen waaraan gevolg werd gegeven

Beschikbaarheid en onafhankelijkheid van de DPO

De controle wees uit dat de DPO van de GGB over de vereiste juridische kennis beschikte om de functie te bekleden. Het geleverde werk schonk voldoening, des te meer daar de omstandigheden (pandemie) niet bevorderlijk waren voor de uitvoering van alle opdrachten. Eerder werd het probleem van de werklast en de beschikbaarheid van de DPO aangekaart.[272] In het kader van de controle kon worden vastgesteld dat deze laatste ondertussen om een '*aanpassing van de werktijd*' had gevraagd. De vraag werd geanalyseerd door de dienst HR van het OCAD. Het COC en het Vast Comité I legden de nadruk op het feit dat de DPO alle mogelijke vrijheid moet genieten nu zijn opdracht delicaat en complex is als gevolg van het grote aantal gebruikers en de techniciteit van de materie. De vaststelling of goedkeuring van de prioriteiten (opgenomen in een opdrachtbrief) door de verwerkingsverantwoordelijken was eveneens een kritische succesfactor. Wat betreft het risico van belangenconflict bleek uit de verrichte controle dat dit risico kon worden geweerd: verschillende adviezen van de DPO van de GGB gaven aan dat hij over de vereiste onafhankelijkheid beschikt.

---

271 Wet van 28 februari 2007 tot vaststelling van het statuut van de militairen en kandidaat-militairen van het actief kader van de Krijgsmacht, ingevoegd door de wet van 31 juli 2013 tot wijziging van voornoemde wet, *B.S.*, 20 september 2013.

272 Hierover: VAST COMITÉ I, *Activiteitenverslag 2019*, 131 (XI.2.4.1. Evaluatie van de belangenconflicten en de tijdsbesteding van de functionaris van de gegevensbescherming').

V.2.2.2. Aanbevelingen waaraan geen gevolg werd gegeven

Melding van de veiligheidsincidenten

Het COC en het Vast Comité I herhaalden, ter attentie van de Federale Politie, hun aanbeveling om hen formeel kennis te geven van veiligheidsincidenten. De verrichte controle bracht een veiligheidsincident aan het licht dat niet onmiddellijk werd gesignaleerd. Deze melding behoort tot de verantwoordelijkheid van de Federale Politie, in haar hoedanigheid van technisch beheerder van de GGB. Bovendien vestigden de toezichthoudende autoriteiten de aandacht van de Federale Politie op het feit dat het begrip '*veiligheidsincident*' niet enkel betrekking heeft op de vertrouwelijkheid, maar ook op de beschikbaarheid en de integriteit van de GGB.

Wat betreft de opvolging van de tweede aanbeveling (passende informatie van de gebruikende diensten wat betreft de rapportering van vastgestelde incidenten), stelden het COC en het Vast Comité I vast dat er in 2020 geen significante vooruitgang werd geboekt. Ook deze aanbeveling werd herhaald.

V.2.2.3. Aanbevelingen waaraan deels gevolg werd gegeven

Uitvoering van IT-ontwikkelingen

Het COC en het Vast Comité I stelden vast dat er gevolg leek te worden gegeven aan hun aanbeveling met betrekking tot de uitvoering van IT-ontwikkelingen om de opvolging te verzekeren van de termijnen voor bewaring van de gegevens in de GGB. De Federale Politie kondigde een opvolging aan in het begin van het tweede semester van 2021. Ze drongen erop aan dat dit aspect, dat sinds het begin van de gezamenlijke controles regelmatig in herinnering werd gebracht, definitief zou worden geregeld binnen de door de Federale Politie aangekondigde termijn. In dit verband kon een latere controle worden uitgevoerd.

Controle van de loggings

Anderzijds stelden het COC en het Vast Comité I vast dat hun aanbeveling wat betreft de controle van loggings werd uitgevoerd. De Federale Politie nam een initiatief dat tot doel had de controle van de loggings door de politiediensten aan te moedigen. Het COC en het Vast Comité I wensten dat de DPO van de GGB erover zou waken – in het kader van zijn opdracht van stimuleren van de informatiebeveiliging – dat dit initiatief werd uitgebreid tot alle (DPO's van de) gebruikers, des te meer daar sommige van hen het niet gewoon zijn om gevoelige informatie te verwerken. Tijdens de controle werd meegedeeld dat de functionaliteit van controle van de loggings werd opgenomen in versie '3.0' van de GGB. Het COC en het Vast

Comité I drongen erop aan dat, bij een volgende controle, alle diensten bij machte zouden zijn aan te tonen dat ze een controle van de loggings hebben uitgevoerd.

De uitzondering op de verplichting van politionele informatie op te nemen in de GGB

Uit eerdere controles is gebeleken dat politionele informatie afkomstig van 'RIR, code 01 of 00' niet werd opgenomen in de GGB.[273] De toezichthoudende autoriteiten hadden de politie gevraagd de regelgeving betreffende de gegevensinvoer in de GGB op grondige wijze te analyseren. Het COC en het Vast Comité I waren van mening dat de analyse van de Politie slechts deels bevredigend was. Er werd een meer grondige analyse ingewacht, waarbij ook de gerechtelijke overheden moesten worden geraadpleegd.

Doorgifte van de lijsten

Het COC en het Vast Comité I stelden vast dat er initiatieven waren genomen om, enerzijds, (gedeeltelijk) een einde te maken aan de doorgifte van lijsten die niet beantwoordde aan de regelgeving en, anderzijds, duidelijke principes te definiëren en protocolakkoorden op te stellen betreffende de doeleinden, de modaliteiten en de veiligheidsaspecten van dergelijke doorgifte. Ze hadden waardering voor de bijzondere initiatieven die de DPO van de GGB nam. Gelet op de actuele regelgeving (en onder voorbehoud van een wijziging daarvan als gevolg van de door het OCAD gevoerde enquête), is het afsluiten van protocollen vereist voor alle diensten die geen rechtstreekse toegang tot de GGB hebben; daarbij dient voorrang te worden gegeven aan de diensten die geen enkele toegang hebben. Het COC en het Vast Comité I bevolen aan om de voorstellen van protocolakkoorden van de DPO te analyseren en vervolgens snel ten uitvoer te leggen.

Raadpleging van het openbaar ministerie door het OCAD m.b.t. de gerechtelijke maatregelen

Gezien het onafhankelijk statuut van het Openbaar Ministerie, bestaat er voor die partnerdienst geen verplichting (maar wel een mogelijkheid) om de GGB TF en HP te voeden, ook al heeft ze een rechtstreekse toegang tot de gegevensbank. De wetgever heeft geoordeeld dat de gerechtelijke gegevens voornamelijk afkomstig zijn van de politiediensten. In die zin is de verplichting voor de politiediensten om de gemeenschappelijke gegevensbank te voeden, voldoende opdat de pertinente

[273] Een 'RIR 01' heeft betrekking oppoliotnele informatie die enkel mag wworden gebruikt voor zover de opsteller daarmee akkoord gaat. Een 'RIR 00' heeft betrekking op politionele informatie die in geen geval mag worden gebruikt.

gegevens van de gerechtelijke politie worden geregistreerd.[274] Om zich ervan te vergewissen dat de voeding van de gegegevensbank goed wordt uitgevoerd, hebben de gerechtelijke overheden instructies verstuurd. Er bleek echter niet dat het OCAD de beginselen toepaste zoals die waren opgenomen in de COL 18/2020. Het COC en het Vast Comité I bevolen het OCAD aan om de beginselen toe te passen die zijn opgenomen in deze COL, om te komen tot een stelselmatige gegevensinvoer en actualisering van de GGB.

Bovendien en onverminderd het beginsel van de scheiding der machten en de autonomie van de gerechtelijke overheden nodigden het COC en het Vast Comité I de minister van Justitie uit om aan het College van procureurs-generaal de opdracht te geven om de omzendbrief COL 18/2020 aan te passen wat betreft de mededeling van de gerechtelijke maatregelen ten aanzien van de potentieel gewelddadige extremisten (PGE).

V.2.3. NIEUWE AANBEVELINGEN

Als gevolg van een veiligheidsincident - de dienst Erediensten en Vrijzinnigheid van de FOD Justitie beschikte over een toegang tot de GGB HP die ruimer was dan de toegang waarin het KB HP voorziet - interpelleerden het COC en het Vast Comité I de verwerkingsverantwoordelijken. Er werd de verwerkingsverantwoordelijken verzocht een einde te stellen aan de gevallen van onregelmatige toegang. De toezichthoudende autoriteiten bevolen de Federale Politie aan om de technische oplossingen te ontwikkelen die nodig zijn om de toegang door deze dienst in overeenstemming te brengen met de geldende wetgeving (i.e. enkel onrechtstreekse toegang tot de GGB HP). Het COC en het Vast Comité I wensten hierover grondig te worden geïnformeerd.

Voorts bevolen ze de verwerkingsverantwoordelijken aan om op juridisch en operationeel vlak na te gaan of de regelgeving betreffende de toegang van de dienst Erediensten en Vrijzinnigheid al dan niet moest worden herzien.

V.3. 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 verwer-

[274] Het COC en het Vast Comité I hebben evenwel opgemerkt dat deze redenering niet geldt voor vonnissen en arresten waarvan politiediensten geen kennis hebben.

kingsmodaliteiten, 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 2021 niet om een dergelijk advies verzocht.

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*.'

In 2021 werd het Comité zes maal om advies verzocht.[275] De Commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken vroeg het Comité twee maal om advies (over de oprichting van een federaal inlichtingenagentschap (VI.1.) enerzijds en over de strafbaarstellingen ter bevordering van de democratische weerbaarheid (V.5) anderzijds). Ook de Kamer van volksvertegenwoordigers diende een verzoek tot advies bij het Vast Comité I in over de notificatieplicht (VI.2). De minister van Justitie op zijn beurt verzocht het Comité tweemaal om advies (over de dataretentie (VI.3) en over de wijzigingen van de Inlichtingenwet (VI.4)). Ten slotte vroeg de minister van Binnenlandse Zaken de Vaste Comités I en P om een gemeenschappelijk advies aangaande de wijzigingen van de OCAD-Wet (VI.6).[276] Alle adviezen, die hieronder werden opgenomen in chronologische volgorde, zijn intregraal consulteerbaar op de website van het Comité.[277]

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). Deze laatste twee adviesbevoegdheden worden respectievelijk behandeld in Hoofdstuk IV en Hoofdstuk V.

---

275 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.

276 De Vaste Comités I en P formuleerden dit advies als gemeenschappelijke toezichthouder ten aanzien van het OCAD zoals voorzien in de W.Toezicht en in hun hoedanigheid van gegevensbeschermingsautoriteiten ten overstaan van de verwerking van persoonsgegevens door het OCAD.

277 www.comiteri.be

VI.1. ADVIES OVER DE OPRICHTING VAN EEN FEDERAAL INLICHTINGENAGENTSCHAP

In december 2020 werd het Vast Comité I door de Commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken van de Kamer van Volksvertegenwoordigers om advies gevraagd in het kader van het onderzoek van het voorstel van resolutie over de oprichting van een federaal inlichtingenagentschap.[278]

Het voorstel van resolutie had voor ogen om de federale regering te vragen:

- om een audit uit te voeren van zowel de inlichtingendiensten als van de Federale Politie (OA3) voor wat betreft de informatiestroom binnen en tussen die diensten;
- om, op basis van deze audit, een federaal inlichtingenagentschap te creëren waarin alle inlichtingendiensten worden samengebracht onder de bevoegdheid van de Premier;
- de nodige menselijke en technische middelen ter beschikking te stellen van dit agentschap voor de uitvoering van zijn opdrachten.

In zijn advies stelde het Vast Comité I zich (in samenwerking met het Vast Comité P en het Controleorgaan op de politionele informatie) ter beschikking van de Kamer van volksvertegenwoordigers met het oog op zijn deelname aan een audit, waarvan de reikwijdte echter nog beter moest worden bepaald. Gezien de pluraliteit van de hierboven vermelde actoren en partners achtte het Vast Comité I het voorbarig om een conclusie te trekken over de noodzaak om een nieuwe instelling op te richten die één enkele federale inlichtingendienst en één enkele federale politiedienst verenigt (en de middelen die aan deze instellingen ter beschikking moeten worden gesteld) zonder dat de resultaten van de gevraagde audit beschikbaar zijn.

VI.2. ADVIES OVER HET INSTELLEN VAN EEN ACTIEVE KENNISGEVINGSPLICHT VOOR DE INLICHTINGENDIENSTEN

Eind januari 2021 werd een wetsvoorstel neergelegd tot wijziging van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (W.I&V), met het oog op het invoeren van een actieve kennisgevingsplicht met betrekking tot bepaalde specifieke methoden voor het verzamelen van gege-

[278] Dit voorstel van resolutie werd in september 2019 neergelegd in de Kamer. In april 2022 was het nog steeds hangende (*Parl. St.* Kamer 2019-20, 55K0287).

vens.[279] Het wetsvoorstel wenste, enerzijds en in hoofdorde een 'actieve kennisgevingsplicht' en anderzijds een 'passieve kennisgevingsplicht' in te voeren in hoofde van de Belgische inlichtingendiensten.

Een *actieve kennisgevingsplicht*, ook wel gekend als de '(actieve) notificatieplicht', houdt in dat de inlichtingendiensten onder bepaalde voorwaarden uit eigen beweging een geviseerde persoon op de hoogte moeten brengen dat hij of zij het voorwerp van onderzoek is geweest, meer in het bijzonder dat in het verleden een bepaalde inlichtingenmethode op hem of haar werd toegepast.

De *passieve notificatieplicht* impliceert dan weer dat de betrokken inlichtingendienst op verzoek van iedere persoon die een persoonlijk en legitiem belang heeft en onder de Belgische rechtsmacht valt, hem onder bepaalde voorwaarden en volgens bepaalde procedures meedeelt dat op hem een van de inlichtingenmethoden is toegepast.

VI.2.1. DE ACTIEVE NOTIFICATIE

De vraag of een Europees land de verplichting heeft om een actieve notificatieplicht in te voeren, vindt een antwoord in het Europees Verdrag voor de Rechten van de Mens (EVRM), de toepasselijke rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM), het Verdrag nr. 108 van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (bijgewerkt tot Verdrag 108+[280]) alsook, desgevallend, in een betrokken Grondwet en de toepasselijke rechtspraak van een betrokken Grondwettelijk Hof.

Het Comité kon in zijn advies vaststellen dat het EVRM noch de betrokken EHRM-rechtspraak een expliciete verplichting in hoofde van de verdragspartijen bevat om te allen tijde een dergelijke *actieve* kennisgevingsplicht in te voeren. Het gewicht van zo'n plicht moet volgens het Hof wel worden afgezet tegen het geheel van de aanwezige rechtswaarborgen. Daarom moeten alle relevante regels van het nationale recht, met inbegrip van de regels inzake transparantie ten aanzien van de betrokkene, worden beoordeeld.

---

279 *Parl. St.*, Kamer 2020-21, 55K1763/001. Het Comité mocht het verzoek tot advies van de Kamer van volksvertegenwoordigers ontvangen op 6 mei 2021 en bracht advies uit op 31 mei 2021. De voorzitter van het Vast Comité I gaf op 2 juni 2021 toelichting bij het advies in de Kamercommissie Justitie. In april 2022 was het wetsvoorstel nog steeds hangende in de Kamer.

280 Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108), gewijzigd door het Protocol nr. 223 van 18 mei 2018 (Verdrag 108+). Het Verdrag 108+ trad nog niet in voege in België (reden waarom de « + » verder tussen haakjes wordt weergegeven). Zie https://www.coe.int/fr/web/data-protection/convention108-and-protocol).

Zich baserende op de twee arresten van het Grondwettelijk Hof[281] en op de rechtspraak van het Europees Hof, stelde de toelichting van het wetsvoorstel dat er nog steeds een plicht tot herinvoering van de actieve notificatieplicht bestaat. Het Comité was evenwel van oordeel dat deze stelling nuancering behoefde aangezien de wetgever nieuwe procedurele waarborgen[282] had ingebouwd sinds de wetten van 2010 en 2017.[283]

De rechtsbescherming van de burger, en dan in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, het recht op bescherming van persoonsgegevens én het recht op een effectief rechtsmiddel, werd sinds de Wet van 30 maart 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van gegevens (de Gegevensbeschermingswet, afgekort: GBW) omstandig gewijzigd. Niet enkel heeft de wetgever met deze wet het regelgevend kader t.a.v. de inlichtingendiensten uitgebreid en verduidelijkt (artt. 72 tot 104 GBW[284]), er werd ook een versterkt corrigerend toezichtmechanisme in het leven geroepen. Meer bepaald werd het Vast Comité I aangewezen als de bevoegde gegevensbeschermingsautoriteit (DPA) binnen het 'nationale veiligheid'-domein.[285] Sinds de GBW staat m.a.w. elke daad van informatiegaring, -behandeling, -analyse en -doorgifte alsook elke gegevensbewaring onder het corrigerend toezicht van het Comité ingeval er sprake is van een persoonsgegevensverwerking.[286] Betekenisvol in het licht van het recht op een effectief rechtsmiddel is dat – in tegenstelling tot bij de uitoefening van het (reeds gedurende de arresten van het Grondwettelijk Hof

281 De notificatieverplichting werd al in 2010 en 2017 ingevoerd door de wetgever in art. 263 W.I&V. Het Grondwettelijk Hof vernietigde evenwel tweemaal dit artikel aangezien zij de bestaande procedurele rechtswaarborgen onvoldoende achtte om het ontbreken van een actieve kennisgevingsplicht in hoofde van de inlichtingendiensten te rechtvaardigen.

282 Het Comité wenste op te merken dat de memorie van toelichting van de Wet van 30 maart 2017 noch het Grondwettelijk Hof gewag maken van de procedurele waarborgen voorzien in de Wet van 11 april 1994 betreffende de openbaarheid van bestuur (WOB). Nochtans kan de problematiek van de actieve notificatie eveneens gesitueerd worden binnen het recht op toegang tot bestuursdocumenten en informatie van de inlichtingendiensten, aangezien deze wetgeving, tot op zekere hoogte, kennisgeving aan de betrokkene toelaat. Zowel de Raad van State als de Commissie Openbaarheid van Bestuur hebben immers al herhaaldelijke malen bevestigd dat de WOB van toepassing is op de VSSE en de ADIV

283 De Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (*B.S.* 10 maart 2010) en 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, *B.S.* 28 april 2017.

284 Ondertitel 1 van titel 3 (artt. 72 tot 104 GBW) regelt de verwerking van persoonsgegevens door de VSSE en de ADIV in het kader van de uitvoering van haar opdrachten, met uitzondering van de persoonsgegevensverwerkingen in het kader van de Classificatiewet van 11 december 1998. Laatstgenoemde aangelegenheid wordt geregeld in ondertitel 3 van titel 3 van de GBW (artt. 106 tot 137 GBW).

285 VAST COMITÉ I, *Activiteitenverslag 2019*, 75-80.

286 Gelet op de ruime verdragsrechtelijke invulling van het begrip 'verwerking van persoonsgegevens' (*cf.* artikel 8 EVRM *i.o.* Verdrag nr. 108(+)) staan zodoende alle persoons-gegevensverwerkingen verricht door de inlichtingendiensten onder het DPA-toezicht van het Comité. In zijn rol van gegevensbeschermingsautoriteit treedt het Vast Comité I ofwel op uit eigen beweging, ofwel op verzoek van een andere gegevensbeschermingsautoriteit, ofwel op verzoek van elke betrokkene.

bestaande) BIM-klachtenrecht[287] waarbij een klacht de grieven dient te vermelden van de verzoeker die tevens een persoonlijk en rechtmatig belang moet kunnen aantonen – er bij de uitoefening van het verzoek bedoeld in artikel 51/2 W.Toezicht geen dergelijke formele voorwaarden vereist worden: *"Om ontvankelijk te zijn, is het verzoek geschreven, gedateerd, ondertekend en met redenen omkleed en rechtvaardigt het de identiteit van de betrokkene*". In de praktijk heeft het Comité een zeer soepele houding aangenomen wat betreft de motiveringsplicht. In tegenstelling tot de situatie van voor de Gegevensbeschermingswet, is het recht op toegang tot een effectief rechtsmiddel gevoelig verbeterd.

Volgens het Comité zal de versterking van zijn bevoegdheden na de goedkeuring van de GBW in 2018, in combinatie met de invoering van een systeem van passieve kennisgeving[288] waarin dit voorstel voorziet, voldoen aan de transparantievereiste uit hoofde van het internationaal recht. In het licht van deze vaststelling was het Comité van oordeel dat er geen verdragsrechtelijke verplichting bestaat in hoofde van de federale wetgever om een actieve kennisgevingsplicht in te voeren, op voorwaarde dat enerzijds in het voorstel een verplichting tot passieve kennisgeving wordt opgenomen daarbij rekening houdend met de opmerkingen van het Comité (*infra*).

Niettemin wenste het Comité hier wel onmiddellijk aan toe te voegen en te benadrukken dat het de federale wetgever in België steeds vrijstaat om een dergelijke regeling desondanks in te voeren.[289] In de eventualiteit dat de wetgever hiervoor zou kiezen, formuleerde het Comité een aantal opmerkingen op de verschillende artikels over de verplichting tot actieve notificatie. Deze gingen onder meer over:

- de (niet toegelichte) keuze om de werkingssfeer van de vooropgestelde bepalingen tot slechts enkele methoden te beperken;
- het vastgestelde verschil met de bestaande actieve notificatieverplichting in de strafrechtsprocedure (art. 90novies Sv.);
- de uitzonderingsgronden die bij voorkeur moeten worden afgestemd op deze uit bestaande regelgeving (WPA, W.C&HS, W.I&V, W.Beroepsorgaan);
- de te notificeren personen;
- de notificatietermijnen;
- de toezichthoudende instantie, waarbij het Comité van oordeel was dat één toezichtsorgaan afdoende is.

---

287 Bedoeld in artikel 43/4, eerste lid, derde streepje W.I&V.

288 Rekening houdend met de opmerkingen in dit advies.

289 Een beslissing tot invoering van (een of andere vorm van) actieve kennisgevingsplicht werd zodoende genomen in 6 van 47 lidstaten van de Raad van Europa.

VI.2.2. DE PASSIEVE NOTIFICATIE

Weliswaar ingenomen met het voorstel om de passieve kennisgeving te herintroduceren, wees het Comité erop dat er reeds verschillende systemen, bevoegdheden en procedures bestaan inzake de transparantie van informatie waarover inlichtingendiensten beschikken. In dit verband merkte het Comité op dat de mogelijkheden om actie te ondernemen voor de burger ingewikkeld zijn en moeilijk uitvoerbaar en dat de keuze van een procedure gevolgen zal hebben voor zijn of haar mogelijkheden om (al dan niet) toegang te krijgen tot informatie. Een harmonisatie van de procedures voor toegang tot informatie en de uitzonderingen van mededeling van informatie – en dus een harmonisatie van de uitkomst van de verschillende procedures – is wenselijk.

Het Comité vestigt er dan ook de aandacht van de wetgever op dat in de memorie van toelichting van het passieve kennisgevingssysteem moeten worden toegelicht en gepreciseerd, alsook de manier waarop het zal worden gekoppeld aan de bestaande procedures.

VI.3. ADVIES OVER DATARETENTIE

Door de minister van Justitie werd bij het Vast Comité I een adviesaanvraag ingediend met betrekking tot het voorontwerp van wet 'betreffende het verzamelen en het bewaren van de identificatie-, verkeer- en localisatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten' (hierna: het wetsontwerp).[290] [291] Ten gevolge de annulatie door het Grondwettelijk Hof van de artikelen 2, b), 3 tot 11 en 14 van de Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie[292], had het voorstel tot doel om een systeem van bewaring van communicatiegegevens in te voeren dat voldeed aan de vereisten zoals opgelegd door het Hof van Justitie van de Europese Unie (HvJEU). Om dit te bewerkstelligen drongen er zich wijzigingen op aan onder meer de Wet van 13 juni 2005 betreffende de elektronische communicatie (Telecomwet, WEC) en aan de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (Inlichtingenwet, W.I&V).

---

290 Het Comité ontving de vraag op 7 mei 2021 en bracht op 15 juni 2021 zijn advies uit.

291 Het voorontwerp werd door de Ministerraad in december 2021 in tweede lezing goedgekeurd en neergelegd in de Kamer in maart 2022. Nog in maart 2022, werden 18 amendementen goedgekeurd op de Ministerraad (ten gevolge van het arrest van het Grondwettelijk hof nr. 158/2021 d.d. 18 november 2021). Er werd aan de Raad van State en de GBA om advies op deze amendementen gevraagd. De GBA gaf zijn advies op 1 april 2022 (Zie advies nr. 66/2022 van de GBA).

292 Deze wet werd geannuleerd omwille van tegenstrijdigheden met het Europees recht en de rechtspraak van het Hof van Justitie van de Europese Unie. (HvJEU).

Het Vast Comité I richtte zijn advies op de wijzigingen aan de Inlichtingenwet alsook op de wijzigingen relevant voor zijn bevoegdheid aan de Telecomwet.[293]

VI.3.1. WIJZIGINGEN AAN DE INLICHTINGENWET

VI.3.1.1. Gerichte bewaring van verkeers- en lokalisatiegegevens

De regering stelde voor om in het kader van het gericht bewaren van verkeers- en lokalisatiegegevens in de sector van de elektronische communicatie een nieuwe gewone methode in de Inlichtingenwet in te schrijven.

Het Comité stelde vast dat niet eenzelfde niveau van rechtsbescherming in het wetsontwerp wordt ingebouwd en was van oordeel dat er geen objectieve rechtvaardiging bestaat om de burger minder te beschermen in de inlichtingenprocedure dan in de strafprocedure.

Ook de als controlemechanisme voorgestelde procedure – m.n. een maandelijkse notificatie van de gedane methoden (dus na de uitvoering van meerdere methoden) – correspondeerde volgens het Comité geheel niet met de graad van inmenging die een dergelijke methode met zich meebrengt en beantwoordt niet aan de vereisten van het Hof van Justitie waarin werd gesteld dat een gerichte bewaring van verkeers- en lokalisatiegegeven een effectieve rechterlijke toetsing vereist.

Het Comité wees er tevens op dat de uitgewerkte delegatiebevoegdheid in het kader van deze nieuwe gewone methode met betrekking tot verkeers- en lokalisatiegegevens inzake elektronische communicatie niet voldeed. De regering stelde voor dat de betrokken vorderingsbevoegdheid uitgeoefend mag worden door *"het diensthoofd of zijn gedelegeerde"*. Net zoals het Grondwettelijk Hof en het EHRM is het Comité van oordeel dat dergelijke gegevens zeer intrusief zijn. Er kan bijgevolg geen rechtvaardiging gevonden worden om een bijkomende delegatiebevoegdheid te voorzien naast deze die al werd ingeschreven in de Inlichtingenwet. Bijgevolg werd de regering gevraagd deze keuze te motiveren.[294]

---

293 Het Comité sprak zich niet uit over de vraag of de door het wetsontwerp in de Telecomwet aangebrachte wijzigingen al dan niet voldoen aan de vereisten van de rechtspraak van het Hof van Justitie en het Belgische Grondwettelijk Hof. Daartoe wordt verwezen naar het advies van de Gegevensbeschermingsautoriteit over het wetsontwerp https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-108-2021.pdf

294 Betekenisvol is dat de wettelijke definitie van het begrip diensthoofd reeds een delegatiebevoegdheid in zich draagt: *bij verhindering* van de administrateur-generaal van de VSSE of van de chef van de ADIV, hebben de respectievelijke hoofden de mogelijkheid om hun beslissingsbevoegdheid te delegeren naar de *dienstdoende* administrateur-generaal respectievelijk de *dienstdoende* chef. Een dergelijke delegatie beperkt zich niet tot de adjunct-administrateur-generaal van de VSSE en de adjunct-chef van de ADIV. Wanneer laatstgenoemden op hun beurt verhinderd zijn, kan opnieuw een delegatie toegekend worden aan een hiërarchisch lager niveau.

VI.3.1.2. Toegang tot verkeers- en lokalisatiegegevens

Het wetsontwerp beoogde het grotendeels door het Grondwettelijk Hof[295] vernietigde artikel 18/8 W.I&V te herstellen dat de toegang tot de verkeers- en lokalisatiegegevens met betrekking tot elektronische communicatie door de inlichtingendiensten regelde.

Het Comité bracht de regering in herinnering dat het Grondwettelijk Hof het gehele artikel 18/8 W.I&V had vernietigd. Stellen dat enkel de vernietiging van paragraaf 2 zich opdringt in het licht van de betrokken arresten van het Grondwettelijk Hof en het EHRM, was naar het oordeel van het Comité een voorbarige conclusie. Het is het geheel aan procedurele rechtswaarborgen dat in overweging genomen moet worden.

VI.3.1.3. Algemene en ongedifferentieerde bewaring van verkeers- en lokalisatiegegevens

Het wetsontwerp voorzag om in het kader van het bewaren van verkeers- en lokalisatiegegevens in de sector van de elektronische communicatie een nieuwe uitzonderlijke methode in de Inlichtingenwet in te schrijven in geval van een reële, actuele of voorzienbare ernstige bedreiging van de nationale veiligheid. In dat geval, voorzag het ontwerp dat de inlichtingendiensten de medewerking zouden (kunnen) vorderen van operatoren voor het algemeen en ongedifferentieerd bewaren van verkeers- en lokalisatiegegevens van elektronische communicatie die door hen wordt gegenereerd en verwerkt.

Het Comité onderschreef ten volle het voorstel van de regering om de aanwending van deze bevoegdheid te onderwerpen aan alle controlemechanismen eigen aan de uitzonderlijke methoden.

Het Comité beval aan om de band tussen het actuele artikel dat de toegang regelt en het ontworpen artikel dat de algemene bewaring regelt, te verstevigen. Momenteel is het mogelijk dat een welbepaalde dreiging (bijv. terrorisme) de rechtvaardiging kan vormen om een algemene en ongedifferentieerde bewaring op te leggen aan de telecomoperatoren, zonder dat vervolgens enige beperking van toepassing is en dat bijgevolg de toegang tot deze gegevens ook kan worden gebruikt voor andere doeleinden (bijv. binnen de bestrijding van andere dreigingen).

De memorie van toelichting stelde hieromtrent: *"De machtiging van het betrokken diensthoofd om deze uitzonderlijke methode toe te passen, wordt ter informatie aan de bevoegde minister overgemaakt. Het doel is de bevoegde minister in kennis te stellen van het feit dat een ongedifferentieerde bewaring gestart is."*[296] Het Comité

---

295 G.H., arrest nr. 57/2021 van 22 april 2021.

296 Voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie-, verkeer-, en localisatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten, pp. 111-112.

beval aan om de betrokken minister niet enkel in kennis te stellen van de uiteindelijke "machtiging" van het diensthoofd maar eerder ook al van het "ontwerp van machtiging". Zowel de notificatie van het ontwerp van machtiging als de notificatie van de machtiging worden actueel niet voorzien in de BIM-procedure bij uitzonderlijke methoden. Het Comité is echter van oordeel dat een bevel van de inlichtingendiensten aan de telecomoperatoren tot het algemeen en ongedifferentieerd[297] bewaren van verkeers- en lokalisatiegegevens een dusdanige grote impact heeft op vlak van de inmenging in de persoonlijke levenssfeer van de burgers en inwoners van België dat dergelijke afwijkende vormvereisten zeker te rechtvaardigen zijn.[298]

Het Comité kon tevens geen reden terugvinden waarom de bewaarperiode[299] en de periodiciteit van verslaggeving[300] afweken van de geldende aanwendingsduur bij uitzonderlijke methoden.

Het Comité beval ten slotte aan om te verduidelijken wat de verhouding is tussen het ontworpen artikel 18/17/1 W.I&V en de bijzondere beschermingsregeling voor advocaten, artsen en journalisten ingericht in de Inlichtingenwet.[301]

VI.3.1.4. Verplichte kennisgeving aan de operatoren

Het Comité beval tevens aan om een verplichting in hoofde van de inlichtingendiensten te creëren om de betrokken operatoren op de hoogte te brengen wanneer het Vast Comité I de stopzetting van een algemene en ongedifferentieerde bewaring of van een gerichte bewaring heeft bevolen.

---

297 In tegenstelling tot de andere uitzonderlijke methoden die doelgericht zijn (cf. art. 18/10, §2, 2° W.I&V).

298 Een kennisgeving van de machtiging dient hierbij, zoals de memorie van toelichting duidelijk verwoord, om de regering op de hoogte te brengen dat een algemene en ongedifferentieerde bewaring gestart is. Een kennisgeving van het ontwerp van machtiging aan de betrokken minister beoogt niet om de beslissingsbevoegdheid op ministerieel niveau te brengen, maar om de regering verplicht op de hoogte te brengen dat volgens de betrokken inlichtingendienst er een gevaar voor de nationale veiligheid aanwezig is van een dermate hoog niveau dat een dergelijke verregaande maatregel van algemene en ongedifferentieerde bewaring van betrokken communicatiegegevens gerechtvaardigd lijkt te zijn.

299 Er werd een bewaarperiode voorgesteld van zes maanden in plaats van twee maanden die verlengd kunnen worden.

300 Er werd gekozen voor een tweemaandelijkse periodiciteit, terwijl nu om de twee weken wordt gerapporteerd.

301 Krachtens artikel 18/9, §4 W.I&V kunnen uitzonderlijke methoden slechts aangewend worden tegen een van deze beschermde beroepen of, onder meer, van hun communicatiemiddelen die ze voor beroepsdoeleinden gebruikten op voorwaarde dat de inlichtingendienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van een ernstige potentiële dreiging. Desgevallend dient een bijzondere procedure gevolgd te worden.

VI.3.2. WIJZIGINGEN AAN DE TELECOMWET (WEC)

Het Comité formuleerde eveneens meerdere opmerkingen wat de betreft de voorgestelde wijzigingen aan de Telecomwet. De ontworpen bepaling stelde een gerichte gegevensbewaring voor in geval van ernstige, reële en actuele bedreiging voor de nationale veiligheid op grond van een geografisch criterium, zijnde voor alle zones waar het algemeen dreigingsniveau ten minste niveau 3 bedraagt en zolang niveau 3 blijft bestaan voor deze zones. Het Comité vroeg om het begrip "zones" in deze bepaling nader te verduidelijken.

Het ontwerp belastte de inlichtingendiensten met het jaarlijks opstellen van een lijst van "*de gebouwen bestemd voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden*" en die op voorstel van de ministers van Justitie en Defensie dient goedgekeurd te worden door de Nationale Veiligheidsraad. Het Comité bracht de regering in herinnering van het bestaan van het Actieplan van de federale regering tot vrijwaring van het wetenschappelijk en economisch potentieel.[302] Ook dit actieplan bevat een lijst van entiteiten. Het Comité stelde vast dat deze lijst – gemaakt in 2007 – geen actualisering kende. In het licht van deze vaststelling stelde het Comité de vraag of een jaarlijkse actualisering van de lijst voorzien in het wetsontwerp realistisch is.

Het Comité stelde verder vast dat een verplichte kennisgeving ontbrak waarbij de gerichte geografische bewaring gebeurt op grond het algemene dreigingsniveau zoals bepaald door het Coördinatieorgaan voor de dreigingsanalyse (OCAD). Het Comité herinnerde er de regering aan dat het Vast Comité I en het Vast Comité P, gezamenlijk, de bevoegde gegevensbeschermingsautoriteiten zijn tegenover het OCAD. Het Comité beval aan om eenzelfde kennisgevingsplicht in te richten (minstens) aan het Vast Comité I en om hieromtrent eveneens het Vast Comité P te bevragen.

VI.4. ADVIES OVER HET VOORONTWERP VAN WET TOT WIJZIGING VAN DE INLICHTINGENWET

Op verzoek van de minister van Justitie gaf het Vast Comité I zijn advies over het voorontwerp van wet 'tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten'.[303] [304] Het wetsontwerp voorzag onder meer in een uitbreiding van de mogelijkheden voor de agenten van de

---

302 Op 16 maart 2007 goedgekeurd door het Ministerieel Comité voor inlichting en veiligheid (heden: de Nationale Veiligheidsraad), afgekort: het Plan WEP.

303 De minister verzocht het Comité om advies op 31 mei 2021; het Comité bracht zijn advies uit op 15 juni 2021. Het betrof het tweede advies van het Comité in deze context. Het Comité gaf al op 16 november 2018 een advies over een wetsontwerp waarin grotendeels dezelfde voorstellen werden geformuleerd.

304 In april 2022 werd dit voorstel in tweede lezing nog niet goedgekeurd door de Ministerraad.

inlichtingendiensten om misdrijven te plegen alsook in een bijzondere procedure voor de aanwending van een fictieve identiteit. Tevens werd de mogelijkheid gecreëerd opdat ook menselijke bronnen bepaalde misdrijven zouden kunnen plegen alsook om bijzondere inlichtingenmethoden in te zetten om de betrouwbaarheid van bronnen na te gaan. Er zou tevens een nieuwe bevoegdheid worden toegekend aan de Algemene Dienst Inlichting en Veiligheid (ADIV) in het kader van een nationale cybersecuritycrisis. Ten slotte werd ook een herschikking voorgesteld inzake de reeds bestaande methode van collecte bij de banken en financiële instellingen.

VI.4.1. EEN TE COMPLEXE REGELGEVING

Algemeen, stelde het Comité vast dat de voorgestelde wetswijzigingen de regelgeving van toepassing op de Veiligheid van de Staat (VSSE) en op de ADIV er een stuk complexer en onsamenhangender op maken. De keuzes van de BIM-wetgever in 2010 om in de Inlichtingenwet een logische structuur in te stellen voor wat betreft de (onderzoeks)bevoegdheden van de inlichtingendiensten (o.m. een onderscheid tussen uitzonderlijke, specifieke en gewone methoden naargelang de graad van privacy-inmenging) werd door de wetswijzigingen van de laatste jaren grotendeels verlaten. Het Comité betreurde dat het wetsontwerp zich inschakelde binnen deze evolutie.

Het Comité stelt vast dat bepaalde keuzes in voorliggend wetsontwerp nodeloos ingewikkeld en onvolledig zijn. Een gegeven dat volgens het Comité niet bevorderlijk is voor een goede toekomstige toepassing van betrokken regelgeving.

VI.4.2. CYBERSECURITY - OPDRACHT VAN DE ADIV

Het wetsontwerp gaf de ADIV een nieuwe opdracht, namelijk *"het neutraliseren, in het kader van een nationale cyber security 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"*.

Deze nieuwe opdracht vormt een aanvulling op de bestaande cybersecurity-opdracht[305] door de ADIV de mogelijkheid te bieden op te treden tegen een cyberaanval op informatica- en verbindingssystemen die niet worden beheerd door de minister van Defensie. De materiële bevoegdheid van de ADIV in het kader van deze niet-militaire *cybersecurity*-opdracht wordt bepaald door het voorstel van

[305] Deze opdracht wordt bepaald in artikel 11, §1, 2° W.I&V en laat de ADIV toe te reageren op een cyberaanval op informatica- en communicatiesystemen dewelke worden beheerd door de minister van Defensie.

definitie van het begrip "nationale *cyber security* crisis" als "*elke cyber security 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.*[306]

Het Comité was van oordeel dat de door de ADIV te beschermen entiteiten in het kader van deze cybersecurity-opdracht te ruim omschreven werden. De woordengroep "*de vitale belangen van het land of de essentiële behoeften van de bevolking*" was te weinig afbakenend. Het Comité beval daarom aan in te zetten op de 'kritieke infrastructuren' als te beschermen entiteiten (*cf.* de Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren).

De ontworpen bepaling geeft de ADIV niet enkel de bevoegdheid om een cyberaanval te 'neutraliseren', maar tevens om hierop te reageren met 'een eigen cyberaanval'. Een dergelijk recht bestaat ook reeds in het bestaande artikel 11, §1, 2° W.I&V. Het Comité stelde zich de vraag wat het exacte wettelijke kader is dat bij de uitoefening van een dergelijke aanvalsbevoegdheid gerespecteerd moet worden. Het Comité vroeg daarom om te verduidelijken hoe het oorlogsrecht zich hier verhoudt ten aanzien van het strafrecht.[307]

VI.4.3. HET PLEGEN VAN ONDERSTEUNENDE MISDRIJVEN

VI.4.3.1. Algemeen

Het plegen van misdrijven wordt in het wetsontwerp toegelaten bij diverse soorten opdrachten van de VSSE en de ADIV. Het Comité beval aan om de mogelijkheid te schrappen om misdrijven te plegen in het kader van de ADIV-opdracht inzake het zorgen voor het behoud van de militaire veiligheid en deze inzake het beschermen van het geheim. Het Comité zag geenszins enige redenen waarom deze mogelijkheid zou moeten ingevoerd worden bij deze opdrachten.

Het ontwerp bevatte een lijst van misdrijven die niet door de agenten van beide inlichtingendiensten respectievelijk door menselijke bronnen (HUMINT) gepleegd mogen worden. Het Comité stelde vast dat betrokken lijst niet afdoende

306 De memorie van toelichting verduidelijkt dat deze definitie van 'crisis' werd overgenomen uit artikel 2 van het koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie- en Crisiscentrum van de Regering.

307 Een cyberaanval op Belgische IT-infrastructuren is namelijk een misdrijf. De vraag rijst bijgevolg of een dergelijke cyberaanval geen inmenging betekent in de gerechtelijke opdrachten. De situatie waarin een misdrijf plaatsvindt met louter een binnenlandse dimensie moet aangepakt wordt via het strafrecht.

exhaustief was en stelde voor om een aantal misdrijven en misdrijfcategorieën aan deze verbodslijst toe te voegen.

Het Comité betreurde het dat de BIM-Commissie geen overeenstemmende sanctiebevoegdheden in het wetsontwerp kreeg wanneer ondersteunende misdrijven onrechtmatig worden gepleegd gedurende de aanwending van gewone methoden. De Commissie heeft hier – i.t.t. bij BIM-methoden – geen actiemogelijkheid tegen onrechtmatig verkregen gegevens. Het Comité beval aan om de BIM-Commissie eenzelfde controle- en sanctiebevoegdheden toe te kennen die ze heeft bij de controle van uitzonderlijke methoden (*cf.* artikel 18/10, §6 W.I&V). Hierdoor zou het 'plegen van misdrijven' geen uitzonderlijke methode worden, maar zou de controle erop wel plaatsvinden *zoals bij uitzonderlijke methoden*. Er zou aldus eenzelfde niveau van rechtsbescherming plaatsvinden.

VI.4.3.2. Lacune binnen de strafprocedure

Het Comité bracht eveneens een lacune binnen de strafprocedure onder de aandacht. Binnen de strafprocedure is de kamer van inbeschuldigingstelling bevoegd voor het toezicht op de regelmatigheid van het gerechtelijk onderzoek (*cf.* art. 235*bis* e.v. Sv). Buiten een procedure met een beperkt toepassingsgebied[308], bestaat er geen vergelijkbare procedure waarbij er gedurende de strafprocedure een toezicht wordt ingericht op de regelmatigheid van het inlichtingenonderzoek. Dit is nochtans noodzakelijk gezien een strafdossier eveneens nota's van inlichtingendiensten kan bevatten.

In het licht van de door de regering voorgestelde 'plegen van misdrijven'-procedure beval het Comité daarom aan om de 'prejudiciële adviesprocedure in strafzaken' te veralgemenen. Hierbij dienen dan de strafgerechten de mogelijkheid te hebben om het Comité te vatten en bevragen rond de wettigheid van 'intelligence'-gegevens die zich in het strafdossier bevinden.

VI.4.3.3. Het plegen van misdrijven door agenten

Om de opvolging door de commissie van een misdrijf van een agent dat werd toegelaten door de BIM-Commissie te kunnen realiseren, beval het Comité aan dat

[308] De beperkte procedure vormt de zgn. 'prejudiciële adviesprocedure' (*cf.* artt. 131*bis*, 189*quater* en 279*bis* Sv.) waarbij een strafgerecht aan het Vast Comité I de regelmatigheid kan vragen van de BIM-methoden die aanleiding gaven tot het opstellen van een zogenaamd 'niet-geclassificeerd proces-verbaal' (*cf.* art. 19/1 W.I&V). Dit proces-verbaal wordt door de BIM-Commissie opgesteld wanneer er aanwijzingen van misdrijven naar boven kwamen via het gebruik van BIM-methoden.

in het ontwerp van machtiging de naam van de persoon verantwoordelijk om de aanwending van de maatregel op te volgen, zou worden opgenomen.[309]

In het licht van de bescherming van de agenten, beval het Comité aan dat het betrokken diensthoofd een jurisdictioneel beroep kan instellen bij het Vast Comité I tegen een negatieve beslissing van de Commissie, indien door onvoorziene omstandigheden de procedure niet kon worden gevolgd en er een strafbaar feit gepleegd is dat strikt noodzakelijk was ter verzekering van de eigen vrijheid of die van derden.

VI.4.3.4. Het plegen van misdrijven door informanten

Wat betreft het plegen van misdrijven door menselijke bronnen, beval het Comité aan te preciseren dat deze enkel zouden zijn toegelaten in het kader van een inlichtingenopdracht. Omdat er geen 'wettelijke' definitie van het begrip 'menselijke bronnen' bestaat, is het materiële toepassingsgebied van deze strafuitsluitingsgrond onvoldoende duidelijk.

Om een daadwerkelijke controle toe te laten, beval het Comité aan om in het ontwerp van machtiging de naam van de behandelende officier van de betrokken menselijke bron op te nemen. Het Comité was ook van oordeel dat alle betrokken toezichthoudende instanties de bevoegdheid moeten hebben om kennis te nemen van de identiteit van de informant.[310]

VI.4.3.5. Schade opgelopen of veroorzaakt door een menselijke bron

Het ontwerp creëert een schaderegeling voor schade aan een informant alsook voor schade veroorzaakt door een informant tijdens zijn opdracht. Het Comité onderlijnde het gebrek aan duidelijkheid inzake de beschrijving van de te volgen procedure.

VI.4.3.6. Onvoldoende rechtsbescherming voor de menselijke bron

Het Comité stelde vast dat het voor advies voorgelegde wetsontwerp een onvoldoende graad van rechtsbescherming bood voor de menselijke bron die een toelating verkreeg om bepaalde misdrijven te plegen. Het wetsontwerp geeft namelijk geen antwoord op de vraag hoe de betrokken gerechtelijke overheden met zekerheid kunnen weten dat een geverbaliseerd persoon over een toelating van de

---

309 Het Comité erkent dat het niet altijd mogelijk is om voorafgaand de naam te kennen van de agent die belast wordt met de uitvoering van een inlichtingenmethode of beschermings- en ondersteuningsmaatregel. Maar dit is niet het geval voor de verantwoordelijke voor de opvolging van de maatregel.

310 Het geven van een akkoord aan een informant (een privépersoon aldus) om misdrijven te plegen, zonder dat de BIM-Commissie weet aan wie dat ze deze toestemming geeft, maakt een effectieve controle onmogelijk.

BIM-Commissie beschikt om bepaalde misdrijven te plegen.[311] Het Comité deed diverse voorstellen om hieraan te verhelpen.[312]

VI.4.4. FICTIEVE IDENTITEIT EN HOEDANIGHEID: ALS ONDERSTEUNINGSMAATREGEL BIJ EEN INLICHTINGENMETHODE OF LOUTER OM VEILIGHEIDSREDENEN

Het wetsontwerp wijzigt de bestaande procedure voor de creatie en het gebruik van een fictieve identiteit (heden: artikel 13/2 W.I&V), alsook creëert het een nieuwe bevoegdheid inzake het gebruik van een fictieve identiteit voor redenen van informatiegaring.

Het Comité suggereerde om de BIM-Commissie toe te laten een controle uit te voeren in alle mogelijke gevallen waar zij de mening toegedaan is dat een fictieve identiteit wordt gebruikt voor de informatiegaring (en dit, zelfs als de betrokken dienst andere motieven vooropstelt om het beroep op een fictieve identiteit te rechtvaardigen). Het Comité nodigde de wetgever tevens uit om de begrippen 'fictieve identiteit' en 'fictieve hoedanigheid' in te wet te verduidelijken.[313]

VI.4.5. INFILTRATIE IN DE REËLE EN VIRTUELE WERELD

Het wetsontwerp kiest ervoor om de controle op de infiltratiebevoegdheid onrechtstreeks te organiseren via de controle op het plegen van misdrijven en/of op het gebruiken van een fictieve identiteit. De hieruit voortvloeiende procedure is nodeloos ingewikkeld, onvolledig en voldoet geenszins aan de noodzakelijke rechtswaarborgen die aanwezig moeten zijn bij een dergelijk verregaande onderzoeksbevoegdheid. Het Vast Comité I adviseerde dan ook negatief. Voor wat betreft het onderdeel rechtsbescherming is het Comité van oordeel dat voorliggend

311 Dit is problematisch gelet op het feit dat het parket, het onderzoeksgerecht of, in laatste instantie, het vonnisgerecht de bevoegde instanties zijn om te oordelen over het concreet bestaan van een strafuitsluitingsgrond in hoofde van de geverbaliseerde persoon.

312 Zoals bijv. de mogelijkheid voor de BIM-Commissie om, in sommige gevallen, een akte op te stellen waarin haar akkoord tot het plegen van bepaalde misdrijven beschreven wordt; het afsluiten van een protocolakkoord tussen de inlichtingen- en veiligheidsdiensten, de BIM-Commissie en het College van procureurs-generaal om een communicatiekanaal in te richten tussen alle actoren.

313 Het Comité stelt zich bijvoorbeeld de vraag of het doelbewust niet meedelen aan een gesprekspartner van de hoedanigheid van lid van een inlichtingendienst gedurende het inwinnen van gegevens reeds een gebruik van een fictieve hoedanigheid is

wetsontwerp niet voldoet aan de eisen gesteld door de parlementaire onderzoekscommissie.[314]

Het wetsontwerp geeft deze nieuwe bevoegdheid de kwalificatie van gewone methode. Rekening houdende met de wijze waarop infiltratie wordt geregeld in de strafprocedure, stelde het Comité voor om de 'infiltratie in de reële wereld' te kwalificeren als uitzonderlijke methode en de 'infiltratie in de virtuele wereld' als specifieke methode.

Bovendien stelde het Comité vast dat via de procedure vastgelegd aangaande het gebruik van een fictieve identiteit voor informatiegaring, de schijn wordt gewekt dat een procedure wordt ingericht vergelijkbaar met de BIM-toelatingsprocedure voor uitzonderlijke methoden. Het Comité stelt vast dat deze werkwijze er echter voor zorgt dat diverse controlemechanismen van toepassing bij uitzonderlijke methoden achterwege worden gelaten.

Een kwalificatie van de infiltratiebevoegdheid als BIM-methode heeft daarenboven als gevolg dat er een gestructureerde controle door de BIM-Commissie mogelijk wordt op de bekomen onderzoeksresultaten.[315]

VI.4.6. GEWONE METHODEN PLUS

In zijn advies onderlijnde het Comité dat de procedurele garanties voor de inzet van gewone methoden plus niet meer voldeden, en dat de controle er op onvoldoende juridische bescherming bood. Er werd bijgevolg dan ook aanbevolen om de controle op de gewone methoden plus (MPLUS-methoden) te versterken, en dit door alle MPLUS-methoden op eenzelfde wijze te behandelen en om zodoende in hoofde van de inlichtingendiensten een verplichting te creëren waarbij elke aanwending van een dergelijke methode voorafgaat door een schriftelijke en gemoti-

314 De memorie van toelichting verwijst terecht naar het Derde tussentijdse verslag van de parlementaire onderzoekscommissie Terroristische aanslagen waarin de aanbeveling wordt gedaan om een infiltratiebevoegdheid voor de inlichtingendiensten in te richten. De aanbeveling stelt echter eveneens dat *"(i)n de uit te werken wettelijke regeling (…) echter de nodige waarborgen (moeten) worden voorzien, zowel inzake de rechtsbescherming van de burgers als inzake de veiligheid van de agenten van de VSSE die met de infiltratie worden belast."* Zie *Parl. St.*, Kamer, 2016-17, 54K1752/008.

315 Vroeger was de toelatingsprocedure wellicht niet afdoende aangepast aan de uitoefening van een infiltratiebevoegdheid. De wetgever heeft evenwel de laatste jaren in de Inlichtingenwet een aantal instrumenten in het leven geroepen die deze vroegere belemmeringen remediëren.

veerde beslissing, die de betrokken dienst ambtshalve en zo spoedig mogelijk ter kennis brengt aan het Comité.[316]

VI.4.7. VORDEREN VAN FINANCIËLE GEGEVENS

Het ontwerp voert een nieuwe gewone methode in. Ze creëert een medewerkingsverplichting voor financiële instellingen in de meest ruime zin van het woord om over te gaan tot de identificatie van financiële producten of diensten waarover een persoon beschikt of, omgekeerd, om te identificeren welke persoon kan gelinkt worden aan bepaalde financiële producten of diensten. Actueel is dit een uitzonderlijke methode.

Het Comité beval aan om deze methode te kwalificeren als een specifieke methode. In de memorie van toelichting verantwoordt de regering de keuze voor een gewone methode door te stellen dat *'de intrusiviteit van een dergelijke methode (…) gering tot zeer gering is'*.

VI.4.8. PERSONELE EN FINANCIËLE MIDDELEN

Het Comité was van oordeel dat de tenuitvoerlegging van de diverse uitgewerkte maatregelen niet alleen een bijkomend beslag creëert op de capaciteit van de inlichtingendiensten, maar ook op deze van de betrokken toezichthoudende instanties. Het Comité beval zodoende aan dat een goedkeuring van het wetsontwerp gepaard zou gaan met een uitbreiding van het personeel van de BIM-Commissie en het Vast Comité I.

VI.5. ADVIES OVER DE STRAFBAARSTELLINGEN TER BEVORDERING VAN DE DEMOCRATISCHE WEERBAARHEID

In september 2021 bracht het Vast Comité I op verzoek van de Voorzitter van de Commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken van

316 Door deze methoden niet als BIM-methoden te kwalificeren heeft de wetgever ervoor gekozen om de controle niet te laten uitvoeren door de BIM-Commissie. Ze heeft daarentegen het Comité hiermee belast. Bij zijn MPLUS-controle heeft het Comité, als regulator van de nationale veiligheidszorg wat betreft de gegevensbescherming in dit domein, eveneens de bevoegdheid om bindende corrigerende maatregelen te nemen ten aanzien van alle persoonsgegevensverwerkingen van de inlichtingendiensten. Ten gevolge hiervan heeft het Comité bijvoorbeeld de bevoegdheid om in het kader van zijn MPLUS-controle een verwerkingsverbod of een gegevenswissing op te leggen.

de Kamer van volksvertegenwoordigers een advies uit over drie wetsvoorstellen, zijnde:

- 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 waren wat het verbod van ondemocratische groeperingen betreft ;
- Wetsvoorstel tot wijziging van de wet van 29 juli 1934 waarbij de private milities verboden warden, 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.[317] [318]

De aan het Comité voor advies overgemaakte wetsvoorstellen strekten ertoe enkele nieuwe strafbaarstellingen in te voeren, met als overkoepelende doelstelling de bevordering van de democratische weerbaarheid. Het Comité beperkte zijn advies tot de aspecten van de betrokken wetsvoorstellen die een invloed hebben of kunnen hebben op de opdrachten en de werking van de inlichtingen- en veiligheidsdiensten.

VI.5.1. VOORAFGAANDE OBSERVATIE

Het Comité kon vooreerst vaststellen dat de voorgestelde strafbare gedragingen, in bepaalde gevallen, eveneens gekwalificeerd kunnen worden als dreigingen voor de nationale veiligheid, en dus overeenkomen met de activiteiten die door de VSSE, de ADIV en het OCAD dienen opgevolgd te worden. Betekenisvol is dat de strafbaarstelling van nationale veiligheidsdreigingen een invloed heeft op de werking van de vernoemde inlichtingen- en veiligheidsdiensten.

Immers, de VSSE heeft onder meer als opdracht het inwinnen, verwerken, analyseren en verspreiden van inlichtingen omtrent extremistische activiteiten die een gevaar vormen of kunnen vormen voor de nationale veiligheid. Ook de ADIV heeft als wettelijke taakstelling onderzoek te verrichten naar extremistische activiteiten ingeval hierin een militair aspect aanwezig is.

317 *Parl. St.* Kamer 2021-22, 55K450/001, 55K943/001 en 55K2024/001.

318 De drie wetsvoorstellen, nog hangende in de Kamer in april 2022, vormden in juni en juli 2021 het voorwerp van discussies in de Kamercommissie Binnenlandse Zaken. Een verslag van de debatten werd gepubliceerd in april 2022.

VI.5.2. SAMENWERKING EN UITWISSELING VAN INFORMATIE MET GERECHTELIJKE ACTOREN

Het Comité is van oordeel dat een (onrechtstreekse) uitbreiding van het strafrechtelijk arsenaal binnen de nationale veiligheidszorg de nood doet toenemen om te voorzien, op algemeen en geformaliseerde wijze, in een operationele samenwerking tussen het openbaar ministerie, de gerechtelijke politie, de VSSE, de ADIV en het OCAD.

Heden wordt deze operationele samenwerking en informatie-uitwisseling binnen het gerechtelijk ressort Brussel in belangrijke mate georganiseerd via het zogenaamde *Joint Intelligence Centre (JIC) /Joint Decision Centre (JDC)* systeem.[319] Het Comité adviseerde om te onderzoeken in welke mate het JIC/JDC-systeem dient uitgebreid te worden voor de opvolging van dreigingen andere dan terrorisme, meer in het bijzonder voor de opvolging van de strafbaarstellingen voorgesteld in de voor advies overgemaakte wetsvoorstellen. Aansluitend brengt het Comité in herinnering dat het JIC/JDC-systeem uitsluitend van toepassing is in het gerechtelijke ressort Brussel. Het Comité adviseerde te onderzoeken in welke mate dit systeem uitgebreid moet worden naar de andere ressorten. Gelet op zijn belang voor voorliggende aangelegenheid bracht het Comité tot slot de aanbeveling van de parlementaire onderzoekscommissie Terroristische Aanslagen in herinnering om een Kruispuntbank Veiligheid op te richten.

VI.5.3. SAMENWERKING EN UITWISSELING VAN INFORMATIE MET BESTUURLIJKE ACTOREN

De voorgestelde strafbaarstellingen raken in belangrijke mate de vrijheid van meningsuiting, de vrijheid van vereniging en de vrijheid van vergadering, aldus het Comité.

Het Comité herinnerde aan de wettelijke verplichtingen van de VSSE, de ADIV en het OCAD in het kader van de samenstelling van de lijsten van de door de politie op te volgen 'fenomenen' en op te volgen 'groeperingen' : krachtens artikel 44/5, §2 van de Wet op het politieambt (WPA) zijn de VSSE, de ADIV en het OCAD – logischerwijs samen met de Federale Politie – jaarlijks belast met het opstellen

[319] Het *Joint Intelligence Center* (JIC), samengesteld uit de Federale Gerechtelijke Politie Brussel (FGP Bxl), de Centrale Dienst Terrorisme binnen de federale politie (DJSOC/Terro), de VSSE, de ADIV en het OCAD, is belast met de structurele informatie-uitwisseling binnen de terrorismebestrijding. Het JIC is eveneens belast met de taak alle nieuwe inlichtingen in verband met de terroristische dreiging die verzameld werden door een van de partnerdiensten gemeenschappelijk te beoordelen en een voorstel te formuleren voor een geschikte opvolging (gerechtelijk/ inlichtingenopvolging/ andere opvolging). Het *Joint Decision Center* (JDC), samengesteld uit de vertegenwoordigers van de JIC-leden alsook het openbaar ministerie en de politionele bestuurlijke directeur-coordinator van Brussel, beslist vervolgens collegiaal over de opvolging.

van 'een gezamenlijk voorstel' aan de minister van Binnenlandse Zaken van een lijst met 'Fenomenen van bestuurlijke politie' alsook van een lijst van 'nationale en internationale groeperingen die de openbare orde zouden kunnen verstoren' en die politionele opvolging behoeven. De minister van Binnenlandse Zaken legt deze lijsten jaarlijks vast. In zijn advies beval het Comité aan te onderzoeken in welke mate de lijsten bedoeld in artikel 44/5, §2 WPA ingeschakeld moeten worden binnen de opvolging van de verboden organisaties en groeperingen bedoeld in de voor advies overgemaakte wetsvoorstellen.

VI.6. GEMEENSCHAPPELIJK ADVIES OP HET VOORONTWERP VAN WET TOT WIJZIGING VAN DE OCAD-WET

In augustus 2021 vroeg de minister van Binnenlandse Zaken, lnstitutionele Hervormingen en Democratische Vernieuwing alsook de Gegevensbeschermingsautoriteit aan de Vaste Comités P en I gevraagd om een gemeenschappelijk advies uit te brengen over het voorontwerp van wet tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging (W.OCAD).[320] Op bepaalde plaatsen formuleerde het Vast Comité I opmerkingen in eigen naam.

VI.6.1. UITBREIDING VAN DE LIJST VAN ONDERSTEUNENDE DIENSTEN

Het voorontwerp van wet beoogt in de W.OCAD de vier overheidsdiensten die bij koninklijk besluit van 17 augustus 2018 als ondersteunende dienst van het OCAD werden aangewezen, wettelijk te verankeren.[321]

De W.OCAD stelt immers dat het koninklijk besluit dat overheidsdiensten op voorstel van de Nationale Veiligheidsraad aanwijst als ondersteunende dienst van het OCAD binnen een termijn van een jaar, te rekenen vanaf de datum van de inwerkingtreding van dit KB worden bekrachtigd door een wet. De Vaste Comités P en I merkten op dat in onderhavig geval hieraan niet werd voldaan. Het voorontwerp van wet komt deze situatie dus verhelpen, zonder daarbij de reden te vermelden voor de laattijdige tussenkomst van de regering.

---

320 Het wetsontwerp werd in februari 2022 in de Kamer neergelegd en in tweede lezing door de Commissie Binnenlandse Zaken op 3 mei 2022 goedgekeurd (Parl. St. Kamer, 2021-22, 55K2443).

321 Dit uitvoeringsbesluit werd genomen in uitvoering van art. 2, 1ste alinea, 2°, g) W.OCAD. Het gaat om de Dienst Erediensten en Vrijzinnigheid binnen het Directoraat-Generaal Wetgeving, fundamentele rechten en vrijheden van de FOD Justitie, het Directoraat-Generaal Penitentiaire inrichtingen van de FOD Justitie, de Algemene Directie Crisiscentrum van de FOD Binnenlandse zaken en de Algemene Administratie van de Thesaurie binnen de FOD Financiën.

Het Vast Comité I drong daarbij aan op een evaluatie van de wettelijke mogelijkheid om een overheidsdienst als ondersteunende dienst bij KB aan te wijzen. De vraag rijst immers of een door het OCAD opgestelde dreigingsevaluatie met een onwettigheid behept is ingeval deze (o.m.) gebaseerd is op informatie afkomstig van een bij KB aangewezen ondersteunende dienst die overgemaakt werd na het verstrijken van de termijn waarbinnen deze aanwijzing wettelijk moest bekrachtigd worden. In aanvullende orde stelt het Vast Comité I zich de vraag of een maatregel die steunt op een in dergelijke omstandigheden tot stand gekomen dreigingsevaluatie desgevallend onwettig is.

Het Vast Comité I formuleerde tevens een aantal specifieke observaties in verband met de dienst BELPIU, bij KB van 21 december 2017 ondergebracht bij de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken.[322]

Het Vast Comité I bracht in herinnering dat het onderbrengen van deze dienst in de schoot van het Crisiscentrum geen enkele invloed heeft op het bestaande wettelijke kader rond de verwerking van passagiersgegevens door de dienst BELPIU. De memorie van toelichting laat uitschijnen dat de dienst BELPIU, ten gevolge van de aanduiding van het Crisiscentrum als ondersteunende dienst van het OCAD, eveneens (onrechtstreeks) onderworpen zou worden aan de samenwerkingsmodaliteiten uitgewerkt in de W.OCAD.

lndien er een nood bestaat om de dienst BELPIU als ondersteunende dienst van het OCAD aan te duiden dan dienen zowel de W.OCAD als de Wet van 25 december 2016 aangepast te worden.

Daarnaast is er problematiek van de verhouding tussen de werkzaamheden van het OCAD in zijn hoedanigheid van operationeel verantwoordelijke van de Gemeenschappelijke Gegevensbank (GGB) Terrorist Fighters en de GGB Haatpropagandisten *(cf.* de artikelen 44/11/3bis ev. WPA) enerzijds, en het OCAD in zijn hoedanigheid van dreigingsevaluatieorgaan anderzijds *(cf.* de Wet van 10 juli 2006).

322 Artikel 2 van het koninklijk besluit ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van de passagiersgegevens, houdende de verplichtingen opgelegd aan de luchtvaartmaatschappijen.

VI.6.2. WIJZIGINGEN VAN DE BENOEMINGSVOORWAARDEN VOOR DIRECTEUR EN ADJUNCT-DIRECTEUR

Het wetsvoorstel veranderde een van de voorwaarden om als directeur en adjunct-directeur van het OCAD aangewezen te worden, met name het bezit van de hoedanigheid van magistraat.

Het Vast Comité I onderschrijft dat het schrappen van de vereiste hoedanigheid van magistraat het aantal mogelijke kandidaten zal doen toenemen, maar formuleerde een aantal bedenkingen met in het achterhoofd de complexe juridische omgeving waarin het OCAD zich begeeft. De vraag rijst of de vervangende aanwijzingsvoorwaarde van 'bijkomende juridische expertise' in hoofde van de directeur en adjunct-directeur niet veeleer theoretisch van aard is, dan dat deze daadwerkelijk afdoende is om de schrapping van de hoedanigheid van magistraat te compenseren in het licht van het respecteren van een balans tussen de operationele behoeften van het OCAD en het belang van het respecteren en kennis hebben van de geldende regelgeving. Het Vast Comité I stelde vast dat in het licht van het schrappen van de benoemingsvoorwaarde van magistraat, het wetsontwerp geen bepalingen toevoegt aan de Wet van 10 juli 2006 ter bescherming van de onafhankelijkheid en onpartijdigheid van de leiding van het OCAD. Een dergelijk kader is evenwel noodzakelijk voor de onafhankelijkheid en onpartijdigheid van de werkzaamheden van het OCAD, o.m. binnen de uitvoering van de dreigingsevaluaties en het bepalen van het betrokken dreigingsniveau.

VI.6.3. UITBREIDING VAN DE OPDRACHTEN VAN HET OCAD

Het voorontwerp van wet beoogt nieuwe opdrachten voor het OCAD in te schrijven in artikel 8 van de wet van 10 juli 2006.

VI.6.3.1. Het coördineren van de globale aanpak tegen dreigingen

Deze bepaling voorziet in een coördinerende rol voor het OCAD in de globale aanpak tegen de dreigingen bedoeld in artikel 3 W.OCAD. De memorie van toelichting stelde dat dit een consolidatie betreft van een reeds bestaande praktijk.

De Vaste Comités P en I stellen echter vast dat de inhoud van deze coördinerende rol niet verder verduidelijkt wordt. De memorie van toelichting blijft vaag wat betreft de omschrijving ervan en beperkt zich tot een niet-limitatieve opsomming van voorbeelden zoals de interactie tussen de Lokale Task Forces (LTF's) en de Lokale lntegrale Veiligheidscellen inzake radicalisme, extremisme en terrorisme (LIVC's-R), de optimalisering van de Gemeenschappelijke gegevensbank. Volgens de Comités verdiende de aanbeveling om de opdracht van het OCAD inzake het coördineren van de globale aanpak tegen dreigingen te verduidelijken. Immers, het

OCAD heeft geen operationeel arsenaal ter beschikking om de dreigingen daadwerkelijk en globaal aan te pakken.

Het Vast Comité I stelde tevens vast dat het ontwerp verwarring creëerde met betrekking tot verschillende wettelijke kaders die de opdrachten van het OCAD vastleggen.[323] Volgens het Comité is er verduidelijking nodig in de verhouding tussen de voedingsplicht in hoofde van de 'basisdiensten' en de 'partnerdiensten'[324] en de meldingsplicht aan het OCAD voor de 'ondersteunende diensten van het OCAD'. De uitbreiding van de meldingsplicht naar alle nieuwe opdrachten van het OCAD creëert immers onduidelijkheid.

Daarenboven was volgens het Vast Comité I verduidelijking vereist over de gewijzigde meldingsplicht en de mate waarin de leden van de LIVC's-R verplicht zijn om informatie te verstrekken aan het OCAD, en bij uitbreiding, of de betrokken LIVC-R-leden persoonsgegevens mogen verstrekken aan het OCAD.

VI.6.3.2. Nieuwe opdrachten voor het OCAD van de Nationale Veiligheidsoverheid?

Verder voorziet het voorontwerp dat het OCAD, behalve de exhaustieve lijst van opdrachten die de dienst wettelijk zijn toebedeeld, desgevallend nieuwe opdrachten binnen zijn bevoegdheidsgebied kan krijgen van de Nationale Veiligheidsraad. Deze nieuwe opdrachten zouden dan verduidelijkt worden via een koninklijk besluit overlegd in de Ministerraad. Nu de uitbreiding van de lijst van de ondersteunende diensten bekrachtigd moet worden door een wet, is daarentegen geen dergelijke bekrachtiging vereist voor wat betreft de uitbreiding van de opdrachten van het OCAD en volstaat een KB dat in de Ministerraad overlegd werd. Het advies bracht dit verschil in benadering binnen dezelfde wet op de voorgrond.

Het Vast Comité I adviseerde verder om de term 'bevoegdheidsgebied van het OCAD' in betrokken bepaling nader te verduidelijken. Er bestaat in hoofde van het OCAD immers geen bevoegdheidsgebied dat uniform is voor al zijn opdrachten.[325]

---

323 In het bijzonder de W.OCAD, de regelgeving aangaande de gemeenschappelijke gegevensbanken en de Wet tot oprichting van de LIVC-R.

324 Artikelen 44/2, §2 en *44/11/3ter,* §4 WPA *i.o.* artikel 7, §1, eerste lid van het Koninklijk besluit van 21 juli 2016 KB Terrorist Fighters en artikel 7, §1, eerste lid KB Haatpropagandisten. Zie tevens de omzendbrief van 22 mei 2018 van de minister van Veiligheid en Binnenlandse Zaken en de minister van Justitie 'betreffende de informatie-uitwisseling rond en de opvolging van terrorist fighters en haatpropagandisten' (omzendbrief Terrorist fighters en haatpropagandisten). Ook het College van procureurs-generaal van het Openbaar Ministerie heeft enkele omzendbrieven uitgebracht tot regeling van deze aangelegenheid: COL 10/2015 'betreft: Gerechtelijke aanpak inzake de foreign terrorist fighters', COL 21/2016 'betreft: Gerechtelijke aanpak van haatpredikers' en COL 22/2016 'betreft: Gemeenschappelijke gegevensbank Foreign Terrorist Fighters'.

325 Bij wijze van voorbeeld, heeft de W.OCAD het over terrorisme, extremisme, inbegrepen het radicaliseringsproces terwijl de Wet op het politieambt (WPA) het dan weer heeft over terrorisme en extremisme dat tot terrorisme kan leiden.

Er wordt tevens voorgesteld de meldingsplicht van de steundiensten uit te breiden naar alle nieuwe opdrachten van het OCAD. In deze logica, zullen de steundiensten verplicht worden om alle inlichtingen waarover ze beschikken over te maken aan het OCAD wanneer deze relevant zijn voor OCADopdrachten. Hieronder vallen eveneens persoonsgegevens. In het licht van het grondrecht op bescherming van de persoonlijke levenssfeer, zoals vastgelegd in artikel 22 van de Grondwet, herinnerde het advies aan het feit dat overmaken van persoonsgegevens te allen tijde een regeling behoeft die wordt vastgelegd in een formele wet waarin minstens de basisregels en -doelstellingen vastgelegd worden.

VI.6.4. MEDEDELING EN CONSULTATIE VAN EVALUATIES

Het voorontwerp van wet houdt tevens een wijziging in voor wat betreft de voorwaarden en modaliteiten van de mededeling door het OCAD van strategische en punctuele evaluaties of evaluaties op verzoek van steundiensten. Wat dat betreft, wezen de Vaste Comités I en P op een aantal (voornamelijk taalkundige) incoherenties en suggereerden alternatieve formuleringen.

VI.6.5. MEDEDELING EN CONSULTATIE VAN INLICHTINGEN VAN GERECHTELIJKE AARD ONDER EMBARGO[326]

Het voorontwerp beoogde tevens wijzigingen aan te brengen in de W.OCAD door te voorzien dat de directeur van het OCAD niet de enige is binnen het OCAD die bestemmeling kan zijn van inlichtingen van gerechtelijke aard onder embargo, maar dat deze ook worden toegestuurd aan de bevoegde leden van het OCAD die door hem worden aangewezen om een *ad hoc* evaluatie te maken met de inlichtingen onder embargo.

De Vaste Comités P en I adviseerden de ontwerpers om in het voorontwerp van wet uitdrukkelijk te voorzien dat de kennisname van deze inlichtingen onder embargo door de aangewezen personeelsleden van het OCAD strikt noodzakelijk is voor de uitoefening van hun functie in het kader van de opdrachten van het OCAD.[327] De Comités raadden ook aan om uitdrukkelijk op te nemen dat de directeur van het OCAD ertoe gehouden is een lijst op te stellen van de aangewezen personeelsleden die toegang krijgen tot deze inlichtingen en deze lijst ter beschikking te houden van de Vaste Comités P en I.

---

326 Zie hierover: VAST COMITÉ I, *Activiteitenrapport 2008*, 110.

327 En dus zoals in de Franse versie van de memorie van toelichting werd opgenomen, ze een strikte *'need to know'* hebben.

VI.6.6. MEDEDELING EN CONSULTATIE VAN INLICHTINGEN BEDOELD IN ARTIKEL 12, 1STE LID W.OCAD

Het voorontwerp van wet beoogt dezelfde aanpassingen in te voegen voor wat betreft de inlichtingen onder embargo aangeleverd door de inlichtingen- en veiligheidsdiensten, de Administratie Douane en Accijnzen van de FOD Financiën en de FOD Buitenlandse zaken, die afkomstig zijn van een gelijkaardige buitenlandse dienst die uitdrukkelijk gevraagd heeft deze niet aan andere diensten tot te zenden, of waarvan de toezending de veiligheid van een menselijke bron in gevaar kan brengen.

De Comités adviseerden dan ook hier uitdrukkelijk te voorzien dat de kennisname van deze inlichtingen onder embargo door de aangewezen personeelsleden van het OCAD strikt noodzakelijk is voor de uitoefening van hun functie alsook dat de directeur van het OCAD ertoe gehouden is een lijst op te stellen van de aangewezen personeelsleden die toegang krijgen tot deze inlichtingen en deze lijst ter beschikking te houden van de Vaste Comités P en 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)[328] 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 de directeur van de Dienst Enquêtes I onder het toezicht van de procureur-generaal bij het hof van beroep of van de federaal procureur (art. 39 W.Toezicht) en heeft het Vast Comité I geen zeggenschap over hen. De voorzitter van het Vast Comité I moet er echter zorg voor dragen dat de uitvoering van de opdrachten van gerechtelijke politie de uitvoering van de toezichtonderzoeken niet hindert. De reden daarvoor ligt voor de hand: het controleorgaan heeft vele andere wettelijke opdrachten. Deze opdrachten zouden in het gedrang kunnen komen indien een te aanzienlijk deel van de tijd zou besteed worden aan gerechtelijke dossiers. De voorzitter kan in dat geval overleg plegen met de gerechtelijke autoriteiten over de inzet van de leden van de Dienst Enquêtes I in strafonderzoeken (art. 61*bis* W.Toezicht).

In de gevallen waarin de Dienst Enquêtes I strafonderzoeken voert, moet de directeur na het afronden van dit onderzoek verslag uitbrengen bij het Vast Comité I. In dat geval '*beperkt het verslag zich evenwel tot de informatie die nuttig is voor de uitoefening door het Vast Comité I van zijn opdrachten*' (art. 43, derde lid, W.Toezicht).

In 2021 voerde de Dienst Enquêtes I onderzoeksdaden uit in het kader zes opsporingsonderzoeken: vier onder leiding van het Federaal Parket, één onder leiding van het Arbeidsauditoraat van Luik en een laatste bij de procureur des Konings van Brussel. Vijf van de dossiers betroffen mogelijks leden van de Algemene Dienst Inlichting en Veiligheid, één dossier had mogelijks betrekking op leden van de Veiligheid van de Staat. In het kader van deze dossiers kreeg de Dienst

328 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).

Enquêtes I zes apostilles, waarvan er vier konden worden afgesloten. In totaal werden 10 processen-verbaal en 11 vertrouwelijke rapporten opgesteld. De beoogde strafbare feiten betroffen de 'schending van het beroepsgeheim', 'valsheid in geschrifte' en 'onrechtmatige toegang tot gegevensbanken'.

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 2021 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 2021 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. De uiteenzetting gebeurde via teleconferentie;
- Er werd door medewerkers van het Comité verschillende artikelen gepleegd in wetenschappelijke tijdschriften[329];
- De voorzitter werd in mei 2021 gevraagd deel uit te maken van het selectiecomité voor de aanduiding van een plaatsvervangend lid voor de BIM-Commissie. Doelstelling van deze selectie en de selectiecommissie was het verzamelen van nuttige informatie omtrent de kandidaten zodat een gemotiveerd advies kon worden gegeven aan de minister van Justitie;
- In juni 2021 trad de voorzitter, op verzoek van de *Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, op als moderator voor de RightsCon, 's werelds toonaangevende conferentie over mensenrechten in het digitale tijdperk. Het thema betrof '*When States of Emergency Collide: COVID-19, Counter-Terrorism and Transnational Data Flows*' en werd in samenspraak met het AWO Agency georganiseerd;
- Er vonden videoconferenties plaats tussen juristen van het Vast Comité I en vertegenwoordigers van het Federaal Instituut Mensenrechten (infra) over de actieve kennisgevingsplicht naar aanleiding van de toepassing van bijzondere inlichtingenmethoden;

---

329 F. GIVRON, en S. LIPSZYC, 'Le contentieux en matière de sécurité et son instance spécifique : l'Organe de recours en matière d'habilitations, attestations et avis de sécurité. La recherche de l'équilibre entre la protection des droits de la défense et la préservation des intérêts majeurs de l'État', *J.T.*, 2021/3, 45-53; W. VAN LAETHEM, 'Problemen met veiligheidsadvies van beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen', *Juristenkrant*, 2021, 439, 8-9 ; B. VERSCHAEVE, 'Het Incident Respons Team van de Staatveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht', *Politie en Recht*, nr 1, 2022, 3-20.

- Er vonden gedachtenuitwisselingen plaats met academici (Universiteit Antwerpen) over het stijgend belang van informatie van inlichtingen- en veiligheidsdiensten binnen de motivering van allerhande soorten bestuursbeslissingen;
- In september 2021 werd de dienstdoend griffier uitgenodigd om een uiteenzetting te geven over het theoretisch kader van veiligheidsscreenings in België tijdens een besloten studiedag. Deze werd georganiseerd voor academici en vertegenwoordigers vanuit de inlichtingenwereld en de kritieke infrastructuren. Het geheel paste in een doctoraatsthesis over *insider threat* (Universiteit Antwerpen);
- Nog in september nam het Comité, op verzoek van de minister van de regering van de Federatie Wallonië-Brussel bevoegd voor justitiehuizen, deel aan een meeting over de uitwisseling van informatie tussen de justitiehuizen, het Coördinatieorgaan voor de dreigingsanalyse (OCAD) en de Veiligheid van de Staat (VSSE).
- De Directeur van de Dienst Enquêtes werd ingeschakeld in een opleidingsmoment voor de rekruten bij de ADIV;
- In oktober 2021 sprak de voorzitter van het Vast Comité I op de derde *European Intelligence Oversight Conference* in Rome.[330]
- Een medewerkster van het Vast Comité I finaliseerde haar doctoraat en behaalde in december 2021 de titel van Doctor in de politieke en sociale wetenschappen (UCLouvain, Saint-Louis-Bruxelles).[331]

VIII.2. SAMENWERKINGSPROTOCOL MET DE FEDERALE OMBUDSMANNEN

De Wet van 15 september 2013[332] duidt de Federale Ombudsmannen[333] 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

330 De titel van zijn uiteenzetting luidde: *'European case law on the notification of secret measures and the Belgian response with particular attention to the future rol of the Standing Committee R'.*

331 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.

332 Wet van 15 september 2013 betreffende de melding van een veronderstelde integriteitsschending in de federale administratieve overheden door haar personeelsleden, *BS* 14 oktober 2013.

333 Wet van 22 maart 1995 tot instelling van de federale ombudsmannen, *BS* 7 april 1995.

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 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. In het protocol werden verder afspraken gemaakt over de onderzoeksmiddelen, het beroepsgeheim, de vertrouwelijkheid en de uitwisseling van *best practices*.

VIII.3. PARTNERSHIP MET HET FEDERAAL INSTITUUT MENSENRECHTEN

Met de Wet van 12 mei 2019 werd het Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens (FIRM) opgericht.[334] Middels een samenwerkingsprotocol kwamen alle deelnemende instanties overeen om praktijken en methoden uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen. In het kader van het uitwerken van een eerste strategisch plan, werden de partner-mensenrechtenactoren om hun inbreng verzocht. Het Comité werd eveneens om een gedachtewisseling verzocht door vertegenwoordigers van het FIRM in het kader van de realisatie van een alternatief rapport voor het VN-Antifoltercomité (CAT). Dit had onder meer betrekking op '*extraordinary renditions*'[335], en viel dus binnen het mandaat van het Vast Comité I.

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. Na verloop van tijd werd een nieuwe partner betrokken in dit project, namelijk het *Investigatory Powers Commissioner's Office (IPCO)* uit het Verenigd Koninkrijk. De groep werd herdoopt tot *Intelligence Oversight Working Group (IOWG)* en in 2019 uitgebreid met drie waarnemers, te weten de *Swedisch Foreign Intelligence Inspectorate (Statens inspektion av försvar-*

334 Wet van 12 mei 2019 tot oprichting van een Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens, B.S. 21 juni 2019.

335 Hierover in extenso: VAST COMITÉ I, *Activiteitenverslag 2006*, 34-41 ('II.2. De CIA-vluchten').

underättelse-verksamhet (SIUN)), de *Swedish Board of Inventions (Statens uppfinnarnämnd, (SUN))* en de Duitse *G10 Commission*.

Tengevolge de beperkingen omwille van COVID-19, bleven de internationale activiteiten in 2021 beperkt. In september 2021 vond een door het Zwitserse toezichtorgaan *Autorité de surveillance indépendante des activités de renseignement* (AS-Rens) georganiseerde virtuele vergadering plaats waarop de toekomst van de IOWG stond geagendeerd. Ook werd overleg gepleegd over de wijze waarop de toezichthouders omgingen met de pandemie en de nieuwe technologische ontwikkelingen op het vlak van *intelligence*. In 2022 wordt deze samenwerking geïntensiveerd.

VIII.5. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

In oktober 2021 vond de derde *European Intelligence Oversight Conference* in Rome plaats bij de Italiaanse toezichthouder, de *Procura Generale della Corte di Cassazione*. De conferentie agendeerde thema's als '*The developments in the light of European Case Law*', *'Bulk data collection and targeted interceptions'* en *'International cooperation and other oversight developments in the light of the revised Convention 108+'*.

In het verlengde van een vragenlijst over '*ex ante oversight*', lanceerde de Nederlandse toezichthouder CTIVD (Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten) in juli 2020 een gelijkaardig initiatief. Het betrof een vragenlijst over *complaint handling* (klachtenbehandeling). Het doel van dit initiatief was de beste praktijken in Europa op het gebied van klachtenbehandeling te verzamelen en te analyseren met de betrachting deze vervolgens te kunnen verbeteren. Ook het Vast Comité I leverde hiertoe zijn inhoudelijke bijdrage.

Het Vast Comité I behield zijn voornemen om, samen met de Zwitserse *Autorité de surveillance indépendante des activités de renseignement* (AS-Rens), over te gaan tot de – zij het kortstondige – uitwisseling van personeelsleden in het kader van een stage. Na een opschorting als gevolg van de coronacrisis is deze uitwisseling gepland in de loop van 2022.

De *Danish Intelligence Oversight Board* deelde met de Belgische en andere Europese toezichthouders zijn '*Standards for Danish intelligence oversight activities*'.

Met de Luxemburgse *Cour administrative* ten slotte, werd informatie uitgewisseld over de wetgeving aangaande het gebruik van geclassificeerde stukken in het kader van veiligheidsmachtigingen.

HOOFDSTUK IX.

HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN[336]

Dit hoofdstuk omvat het op 20 mei 2020 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[337] 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, veiligheidsadviezen.

Daarnaast kan het Beroepsorgaan ook optreden als 'annulatierechter' tegen beslissingen van publieke of administratieve overheden om in een bepaalde sector, voor een bepaalde plaats of voor een bepaald evenement veiligheidsattesten of -adviezen aan te vragen.[338]

Het Beroepsorgaan is samengesteld uit de voorzitters van het Vast Comité I, het Vast Comité P en de Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA). Als ze verhinderd zijn, kunnen de drie voorzitters worden vervangen

---

336 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 jaarverslag moet opstellen.

337 GIVRON, F. en LIPSZYC, S., 'Le contentieux en matière de sécurité et son instance spécifique : l'Organe de recours en matière d'habilitations, attestations et avis de sécurité. La recherche de l'équilibre entre la protection des droits de la défense et la préservation des intérêts majeurs de l'État', *J.T.*, 2021/3, 45-53.

338 Voor meer informatie, zie VAST COMITÉ I, *Activiteitenverslag 2006*, 87-120 en VAST COMITÉ I, *Activiteitenverslag 2018*, 111-124.

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 personeel. De activiteiten van het Beroepsorgaan vormen al meer dan twintig jaar een perfect voorbeeld van synergie binnen bepaalde satellietinstellingen van het parlement. De samenstelling van het Beroepsorgaan levert bovendien 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.

Het Beroepsorgaan heeft alle maatregelen getroffen die nodig zijn om zijn werking te garanderen en dit ondanks de COVID-19-pandemie. Zo bleef het Beroepsorgaan zijn hoorzittingen houden à rato van minimaal twee per maand. In 2021 vonden er dertighoorzittingen plaats.[339]

IX.1.2. GEDETAILLEERDE CIJFERS

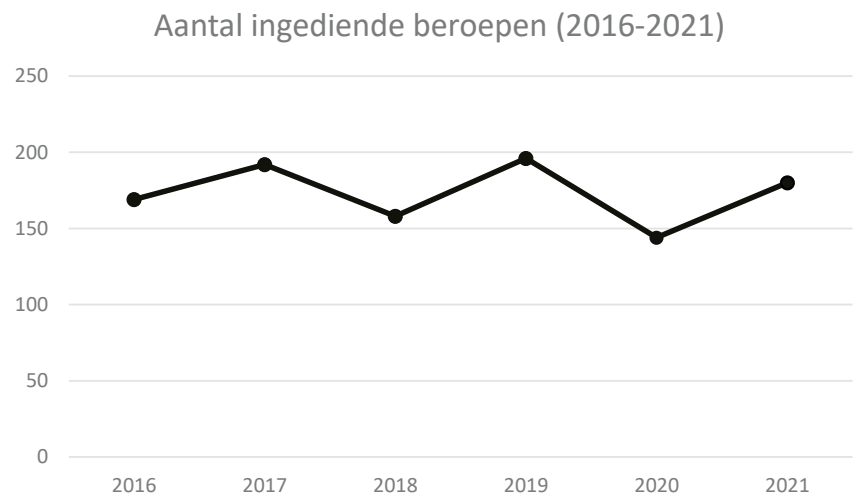
In dit onderdeel worden de aard van de bestreden beslissingen, de hoedanigheid van de bevoegde overheden en de verzoekers, en de aard van de beslissingen van het Beroepsorgaan binnen de verschillende beroepsprocedures cijfermatig weergegeven. Om enige vergelijking mogelijk te maken, werden de cijfers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

In 2021 werden 180 beroepen ingesteld tegenover 144 in 2020 en 196 in 2019 (*infra*). Deze cijfers sluiten aan bij het economisch herstel en de vraag naar veiligheidsadviezen, in het bijzonder in de luchtvaartsector en voor de kandidaten voor Defensie.

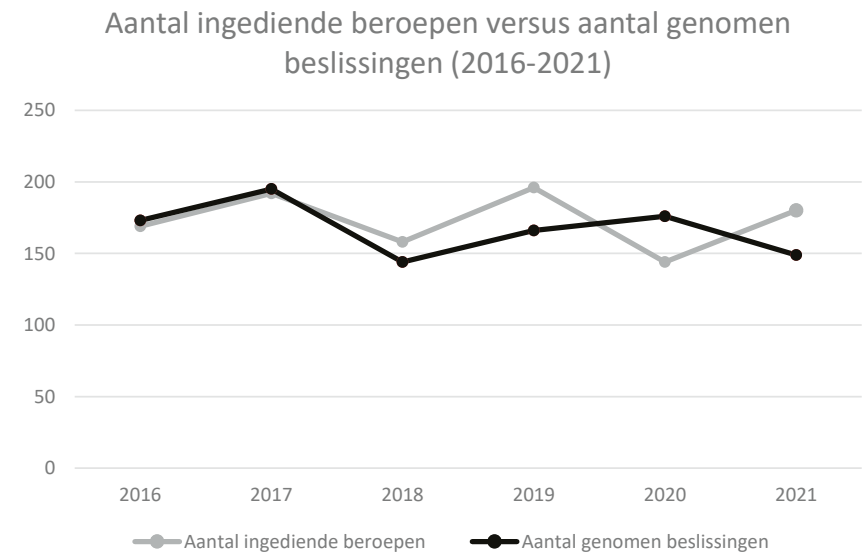
Er zijn 149 definitieve beslissingen genomen.

339 13 in het Nederlands en 17 in het Frans.

Tabel 1. Aantal ingediende beroepen (2016-2021)



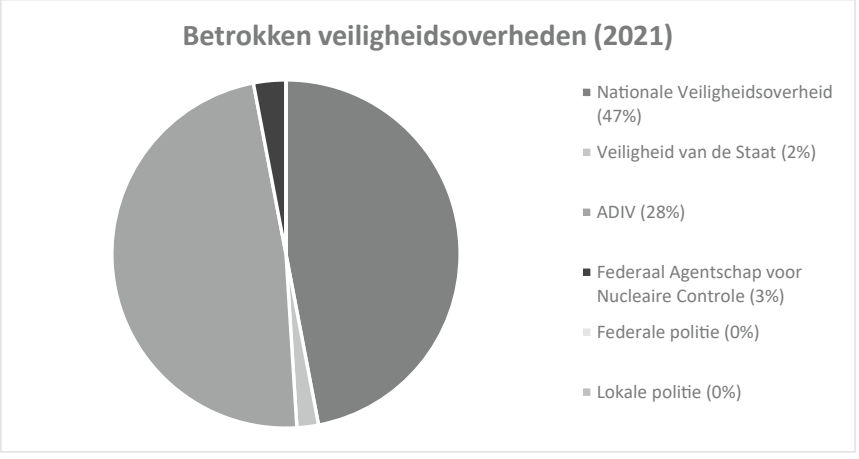
Tabel 2. Aantal ingediende beroepen versus aantal verleende beslissingen (2016-2021)



Tabel 3. Betrokken veiligheidsoverheden (2016-2021)

	2016	2017	2018	2019	2020	2021
Nationale Veiligheidsoverheid	92	129	113	114	91	86
Staatsveiligheid	0	0	0	0	0	4
Algemene Dienst Inlichting en Veiligheid	68	53	32	61	41	84
Federaal Agentschap voor Nucleaire Controle	8	7	10	17	7	6
Federale politie	1	3	3	3	4	0
Lokale politie	0	0	0	1	1	0
TOTAAL	**169**	**192**	**158**	**196**	**144**	**180**

Onderstaande grafiek toont de verdeling van de betrokken veiligheidsoverheden in 2021.



Tabel 4. Aard van de bestreden beslissingen

	2016	2017	2018	2019	2020	2021
Veiligheidsmachtigingen (Art. 12 e.v. W.C&VM)						
Vertrouwelijk	5	1	2	5	0	2
Geheim	38	33	31	39	27	50
Zeer geheim	7	6	3	7	5	8
Weigering	28	30	26	39	23	37
Intrekking	9	7	4	16	8	17
Weigering en intrekking	0	0	0	0	0	4
Machtiging voor beperkte duur	4	1	1	3	0	1
Machtiging voor een lager niveau	1	0	0	0	0	
Geen beslissing binnen de termijn	7	2	5	0	0	1
Geen beslissing binnen de verlengde termijn	1	0	0	0	0	0
Andere					1[340]	
SUBTOTAAL VEILIGHEIDSMACHTIGINGEN	**50**	**40**	**36**	**51**	**32**	**60**
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)						
Weigering	1	3	3	1	0	3
Intrekking	0	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	0	0	0	

340 '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
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)						
Weigering	9	20	15	12	6	2
Intrekking	0	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	0	0	0	1
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)						
Weigering	7	7	11	17	7	6
Intrekking	1	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	1	0	0	0
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)						
Negatief advies	101	122	92	115	99	108
Geen advies	0	0	0	0	0	0
Herroeping van positief advies	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
Weigering van de NVO om verificaties voor veiligheidsattesten te verrichten	0	0	0	0	0	0

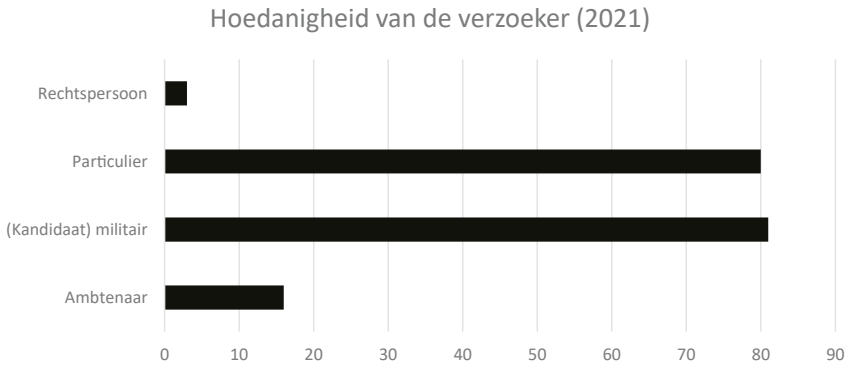
	2016	2017	2018	2019	2020	2021
Beslissing van een administratieve overheid om veiligheidsadviezen te eisen	0	0	0	0	0	0
Weigering van de NVO om verificaties voor veiligheidsadviezen te verrichten	0	0	0	0	0	0
SUBTOTAAL ATTESTEN EN ADVIEZEN	119	152	122	145	112	120
TOTAAL BESTREDEN BESLISSINGEN	**169**	**192**	**158**	**196**	**144**	**180**

Tabel 5. Hoedanigheid van de verzoeker

	2016	2017	2018	2019	2020	2021
Ambtenaar	2	4	5	4	8	16
(kandidaat) Militair	23	20	8	27	39	81
Particulier	139	164	140	163	95	80
Rechtspersoon	5	4	5	2	2	3

Onderstaande grafiek toont de verdeling volgens de 'hoedanigheid van de verzoeker' in 2021.

Tabel 6. Taal van de verzoeker



	2016	2017	2018	2019	2020	2021
Franstalig	99	115	83	101	83	86 (1)
Nederlandstalig	70	77	75	95	61	94 (2)
Duitstalig	0	0	0	0	0	0
Anderstalig	0	0	0	0	0	0

(1) 86 Franstalige dossiers in 2021 + 29 Franstalige dossiers van de vorige jaren maar behandeld in 2021 = 115 Franstalige verzoekers

(2) 94 Nederlandstalige dossiers in 2021 + 18 Nederlandstalige dossiers van de vorige jaren maar behandeld in 2021 = 112 Nederlandstalige verzoekers

Tabel 7. Handelingen van de griffie

	2016	2017	2018	2019	2020	2021
Volledig dossier opvragen (1)	167	191	154	191	141	180
Vraag om bijkomende informatie (2) en herinneringen verstuurd naar de veiligheidsoverheden (3) *	23	36	12	39	41	45

(1) Het Beroepsorgaan kan het gehele dossier opvragen bij de veiligheidsoverheden. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan door de griffie.

(2) Het Beroepsorgaan beschikt over de mogelijkheid om tijdens de procedure aanvullende informatie die het nuttig acht, op te vragen. In de praktijk neemt de griffie de taak op zich om de overheden te vragen de dossiers te vervolledigen.

(3) Art. 6 van het KB Beroepsorgaan bepaalt de termijnen voor de aanlevering van de dossiers door de veiligheidsoverheden. Die termijnen vangen aan wanneer de griffier een kopie van het beroep naar de betrokken veiligheidsoverheid stuurt. Ze variëren naargelang de aard van de betwiste handeling. Zo moet de veiligheidsoverheid haar dossier aanleveren binnen de 15 dagen 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.

Tabel 8. Voorbereidende gerechtelijke handelingen van het Beroepsorgaan [341]

	2016	2017	2018	2019	2020	2021
Horen van een lid van een overheidsinstantie (1)	10	0	1	6	1	4
Beslissing van de voorzitter (2)	0	0	0	0	0	0

341 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.

	2016	2017	2018	2019	2020	2021
Verwijderen van informatie uit het dossier door het Beroepsorgaan (3)	54	80	72	77	50	77
Beslissingen alvorens recht te doen (4)	/	/	/	9	9	19

(1) Het Beroepsorgaan kan beslissen om de leden van de inlichtingen- en politiediensten of van de veiligheidsoverheden die aan het veiligheidsonderzoek of de veiligheidsverificatie hebben meegewerkt, te horen.

(2) De voorzitter van het Beroepsorgaan kan beslissen dat het lid van de inlichtingendienst bepaalde gegevens geheim houdt tijdens zijn verhoor.

(3) Indien de betrokken inlichtingen- of politiedienst hierom verzoekt, kan de voorzitter van het Beroepsorgaan beslissen dat bepaalde informatie wordt verwijderd uit het dossier dat ter inzage aan de verzoeker zal worden voorgelegd.

(4) Het kan bijvoorbeeld gaan om een beslissing om twee dossiers samen te voegen of om nadere informatie te vragen over de context van een gerechtelijk dossier. Deze gegevens worden geregistreerd vanaf 2019.

Tabel 9. Wijze waarop de verzoeker zijn rechten van verdediging uitoefent

	2016	2017	2018	2019	2020	2021
Inzage van het dossier door de verzoeker en/of zijn advocaat	87	105	69	96	96	97
Horen van de verzoeker (al dan niet bijgestaan door zijn advocaat)[342]	127	158	111	143	135	151

Tabel 10. Aard van de beslissingen van het Beroepsorgaan

	2016	2017	2018	2019	2020	2021
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)						
Beroep onontvankelijk	0	3	0	1	1	0
Beroep zonder voorwerp	7	0	4	3	3	3

342 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
Beroep ongegrond	18	13	12	12	16	11
Beroep gegrond (volledige of gedeeltelijke toekenning)	24	24	12	25	14	17
Bijkomende onderzoeksdaden door de overheidsinstantie	2	0	1	1	2	1
Bijkomende termijn voor de overheidsinstantie	2	1	1	0	3	0
Verleent akte van afstand van beroep	0	0	3	2	2	11
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)						
Beroep onontvankelijk	0	1	0	0	0	0
Beroep zonder voorwerp	0	1	0	0	0	0
Beroep ongegrond	1	0	1	1	0	2
Beroep gegrond (toekenning)	1	1	0	3	0	2
Verleent akte van afstand van beroep	-	-	-	1	0	0
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)						
Beroep onontvankelijk	0	1	2	4	2	0
Beroep zonder voorwerp	0	1	0	0	0	0
Beroep ongegrond	2	12	2	4	4	1
Beroep gegrond (toekenning)	4	7	3	4	1	0
Verleent akte van afstand van beroep	0	1	2	0	0	0
Veiligheidsattesten voor nucleaire sector (art. 8*bis*, §2 W.C&VM)						
Beroep onontvankelijk	1	1	0	1	0	0
Beroep zonder voorwerp	1	0	1	0	0	0
Beroep ongegrond	0	1	1	5	2	2

	2016	2017	2018	2019	2020	2021
Beroep gegrond (toekenning)	7	5	6	7	4	6
Verleent akte van afstand van beroep	-	-	2	0	0	0
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)						
Beroepsorgaan onbevoegd	0	20[343]	12	0	0	0
Beroep onontvankelijk	15	10	3	7	8	3
Beroep zonder voorwerp	0	1	3	1	6	4
Bevestiging van negatief advies	42	49	46	40	51	47
Omzetting in positief advies	46	41	27	43	52	34
Verleent akte van afstand van beroep	0	1	0	1	5	5
Beroep tegen normatieve rechtshandelingen van een administratieve overheid (art. 12 W.Beroepsorgaan)	0	0	0	0	0	0
TOTAAL	**173**	**195**	**144**	**166**	**176**	**149**

IX.2. OPMERKINGEN EN SUGGESTIES VAN DE VOORZITTER VAN HET BEROEPSORGAAN

IX.2.1. EEN BIJZONDERE EN COMPLEXE PROCEDURE

Als administratief rechtscollege onderscheidt het Beroepsorgaan zich door een administratief beheer van dossiers dewelke bijzonder van aard zijn en meer complex in vergelijking met andere rechtscolleges van de gerechtelijke en administratieve orde.

[343] 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.

Een eerste bijzonderheid is de wettelijke vereiste van artikel 4 Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veilig-heidsattesten en veiligheidsadviezen (W.Beroepsorgaan), dewelke vandaag buitensporig blijkt. De rechtsonderhorige moet zijn beroep inzake veiligheidsattesten en -adviezen immers instellen binnen de strikte termijn van acht dagen en dit per aangetekend schrijven. De rechtspractici zijn van mening dat een dergelijke termijn onbetwistbaar te kort is voor de burger.

Een tweede bijzonderheid houdt in dat de eiser, in het licht van de wet, in zijn beroep een uiteenzetting moet opnemen van de omstandigheden van de zaak en van de aangevoerde redenen. De voorzitter van het Beroepsorgaan is er zich ervan bewust dat dit wettelijk voorschrift geen rekening houdt met de moeilijkheid voor de burger om in rechte te handelen.

Een derde bijzonderheid heeft te maken met de vraag vanwege de veiligheidsoverheden, in bijna één dossier op twee (77/180), tot beperking van het recht van de rechtsonderhorige om kennis te nemen van het geheel van zijn dossier. Aan het Beroepsorgaan wordt immers gevraagd om artikel 5 §3 W.Beroepsorgaan toe te passen. Dit artikel luidt als volgt: "*Op verzoek van de politie- of inlichtingendienst kan het beroepsorgaan beslissen dat sommige inlichtingen uit de verklaring van een lid van de in § 2 bedoelde politie- of inlichtingendienst, uit het onderzoeksverslag of het onderzoeksdossier of het verificatiedossier, om een van de in § 2, vierde lid, genoemde redenen, of als deze onder het geheim van een lopend opsporings- of gerechtelijk onderzoek vallen, geheim zijn en dat de eiser noch zijn advocaat er inzage van krijgen. Als deze geheimen betrekking hebben op een lopend opsporingsonderzoek of gerechtelijk onderzoek, overlegt het beroepsorgaan hierover voorafgaandelijk met de bevoegde magistraat. Wanneer die inlichtingen afkomstig zijn van een buitenlandse inlichtingendienst, wordt de beslissing tot niet-inzage genomen door de inlichtingen- en veiligheidsdienst. Tegen die beslissingen is geen beroep mogelijk.*" Daaruit volgt dat de voorbereiding van de dossiers van het Beroepsorgaan vereist dat ze worden gescand en vervolgens dat de gevoelige informatie eruit wordt verwijderd. Dit werk wordt pagina per pagina, paragraaf per paragraaf of zelfs woord per woord uitgevoerd door de griffie. *In concreto* gaat het om een juridische analyse die wordt goedgekeurd door de voorzitter van het rechtscollege, en daarna wordt uitgevoerd door de leden van de griffie. Voor het rechtscollege gaat het erom garanties te bieden voor het recht van de rechtsonderhorige om in bezit te worden gesteld van zoveel mogelijk informatie tegenover een wettelijke eis tot beperking van de toegang.

Een vierde bijzonderheid betreft de termijnen voor het toesturen van de administratieve dossiers door de veiligheidsoverheden, in weerwil van de wettelijke voorschriften. Voor 45 van de 180 ingediende dossiers zag de griffie van het Beroepsorgaan zich genoodzaakt een of meerdere herinneringen te versturen naar de veiligheidsoverheden om hen ertoe te bewegen het administratieve dossier toe te sturen. Dergelijke vertragingen doen zich steeds vaker voor en hebben nu betrekking op één dossier op vier, tegenover één dossier op tien vijf jaar geleden.

Daardoor kan het Beroepsorgaan geen beslissingen nemen binnen de opgelegde termijnen. Daarnaast is er vooral sprake van nadeel voor de rechtsonderhorige voor wie het verkrijgen van een veiligheidsmachtiging of -advies vaak de *conditio sine qua non* is voor de uitoefening van een functie.

Een vijfde bijzonderheid tot slot heeft te maken met de vermeerdering van de beroepen die worden ingesteld door buitenlandse aanvragers of aanvragers die in het buitenland hebben verbleven en het feit dat de wettelijke instrumenten waarover de veiligheidsoverheden beschikken, ongeschikt zijn om aan deze maatschappelijke realiteit te beantwoorden. Als gevolg daarvan moeten de veiligheidsoverheden soms verdragen sluiten die de uitwisseling van informatie en inlichtingen met buitenlandse veiligheidsoverheden mogelijk maken. Bij gebrek aan dergelijke akkoorden, volgen de veiligheidsoverheden de rechtspraak van het Beroepsorgaan inzake de problematiek van onderzoeken of verificaties naar personen die niet beschikken over de Belgische nationaliteit niet, en zonder dit op een omstandige wijze te motiveren. De voorzitter van het Beroepsorgaan is van mening dat de Belgische veiligheidsoverheden zouden moeten trachten om informatie in te winnen bij de homologe diensten in het buitenland.[344]

Volgens de voorzitter van het Beroepsorgaan zijn de wet en zijn koninklijke besluiten niet aangepast aan de moderne eisen van toegang tot justitie. De artikelen 2 en 3 van het KB Beroepsorgaan bepalen immers dat "*alle processtukken aan het beroepsorgaan worden toegezonden bij ter post aangetekende brief*" en dat "*de beroepsakte wordt ondertekend en gedagtekend door de eiser of door een advocaat*". Heel wat rechtsonderhorigen nemen deze regels niet in acht en meestal is dit het gevolg van een onvoldoende beheersing van de procedureregels (begrijpelijk gezien de complexiteit van deze regels).

Het wetsvoorstel dat door de voorzitter van het Beroepsorgaan werd opgesteld in samenwerking met voormalig voorzitter van het Hof van Cassatie, Ivan Verougstraete, tracht daaraan te verhelpen. Er moet immers meer rekening worden gehouden met de hoedanigheid en zelfs de kwetsbaarheid van heel wat verzoekers. Daarenboven moet worden voorzien in wettelijke bepalingen die geen nietigheid van rechtswege noch de onontvankelijkheid van het verzoek met zich meebrengen.

De tekst voor hervorming werd op 24 november 2020 toegezonden aan de Kamer van volksvertegenwoordigers. Rekening gehouden met de verschillende wetsvoorstellen in voorbereiding tot wijziging van onder meer de Classificatiewet, is het Beroepsorgaan van mening dat er met deze voorstellen rekening dient te worden gehouden. Per slot van rekening moet de regelgeving betreffende de veilig-

344 Met de Wet van 23 februari 2018 (*B.S.* 1 juni 2018) heeft de wetgever aan de politie- en de inlichtingendiensten uitdrukkelijk de bevoegdheid verleend om relevante informatie op te vragen bij buitenlandse partnerdiensten in het kader van een veiligheidsverificatie (zie artikel 22*sexies*, 3de W.C&VM en *Parl. st*. Kamer, 2017-2018, 54 2767/001, 13). Via deze bepaling heeft de wetgever beslist dat, naast het feit dat een veiligheidsverificatie zich niet altijd beperkt tot een eenvoudige verificatie van sommige databanken, ook buitenlandse informatie relevant kan zijn voor een veiligheidsverificatie.

heidsmachtigingen, - attesten en -adviezen op harmonieuze wijze kunnen worden samen gelezen met de regelgeving aangaande het eventuele beroep tegen deze administratieve beslissingen.

Op 14 februari 2022 stuurde de voorzitster van de Kamer haar antwoord naar de voorzitter van het administratieve rechtscollege, waarin ze aandrong op nieuw overleg met het Vast Comité P en de Geschillenkamer van de Gegevensbeschermingsautoriteit.

De toegankelijkheid van het administratieve rechtscollege blijft prioritair voor het Beroepsorgaan. De tekst, zoals opgesteld, had tot doel het Beroepsorgaan te bevestigen in zijn rol van natuurlijke rechter inzake veiligheidsaangelegenheden, de beroepstermijnen te harmoniseren, de procedure minder ingewikkeld te maken en de digitalisering ervan mogelijk te maken.

IX.2.2. BESLISSING VAN DE RAAD VAN STATE

In een specifiek dossier ging de verzoeker voor de Raad van State in cassatie tegen een beslissing van het Beroepsorgaan. Dit gebeurde sinds de oprichting van het Beroepsorgaan in 1998 nooit eerder. De Raad van State verklaarde het beroep ontvankelijk[345], maar ongegrond.[346]

IX.2.3. AANSPRAKELIJKHEID VAN HET BEROEPSORGAAN

Niettegenstaande het ontbreken van een rechtspersoonlijkheid van het Beroepsorgaan stelde een rechtsonderhorige, volgend op een beslissing van het administratieve rechtscollege en een arrest van onbevoegdheid van de Raad van State, een aansprakelijkheidsvordering in. Er werd een dagvaarding ingeleid voor de Franstalige rechtbank van eerste aanleg van Brussel. Daarbij werd niet enkel de Belgische Staat, maar ook het Beroepsorgaan zelf gedagvaard. Deze zaak is hangende voor het hof van beroep van Brussel volgend op het vonnis van 7 september 2018 waarbij het Beroepsorgaan werd veroordeeld tot de betaling van een schadevergoeding.

345 *In extenso*: W. VAN LAETHEM, 'Problemen met veiligheidsadvies van beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen', *Juristenkrant* 2021, 439, 8-9.

346 Raad van State, arrest nr. 251.927, 26 oktober 2021 (www.raadvst-consetat.be).

IX.2.4. TWEE KWESTIES MET BETREKKING TOT ARTIKEL 6 VAN HET EUROPEES VERDRAG VOOR DE RECHTEN VAN DE MENS (EVRM)

De voorzitter van het Beroepsorgaan acht het aangewezen om de Kamer van volksvertegenwoordigers attent te maken op twee kwesties die worden opgeworpen ten gevolge de Europese rechtspraak en waarmee de Wet op het Beroepsorgaan voorals nog geen rekening hield.

Artikel 6 van het Verdrag voor de Rechten van de Mens (EVRM) bekrachtigt het recht op een eerlijk proces, en dit zowel op gerechtelijk als bestuurlijk vlak. Het eerste lid van het artikel betreft in het bijzonder de kwestie van de openbaarheid van de zittingen en van de publicatie van de beslissingen:

"Bij het vaststellen van zijn burgerlijke rechten en verplichtingen of bij het bepalen van de gegrondheid van een tegen hem ingestelde vervolging heeft een ieder recht op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn, door een onafhankelijk en onpartijdig gerecht dat bij de wet is ingesteld. De uitspraak moet in het openbaar worden gewezen maar de toegang tot de rechtszaal kan aan de pers en het publiek worden ontzegd, gedurende de gehele terechtzitting of een deel daarvan, in het belang van de goede zeden, van de openbare orde of nationale veiligheid in een democratische samenleving, wanneer de belangen van minderjarigen of de bescherming van het privé leven van procespartijen dit eisen of, in die mate als door de rechter onder bijzondere omstandigheden strikt noodzakelijk wordt geoordeeld, wanneer de openbaarheid de belangen van een behoorlijke rechtspleging zou schaden."

De situatie ten aanzien van het huidige recht en de Europese rechtspraak vereist op dat vlak een denkoefening in het belang van de rechtsonderhorige. Het gaat enerzijds om de publicatie van de beslissingen en anderzijds om de openbaarheid van de zittingen.

IX.2.4.1. De publicatie

Eind juni 2014 bracht de Commissie voor de Modernisering van de Rechterlijke Orde (CMRO) deze kwestie ter sprake.[347] In België bestaan drie zogenaamde 'hooggerechtshoven': het Hof van Cassatie, de Raad van State en het Grondwettelijk Hof. Voor elk van deze colleges geldt een verschillende regeling inzake de publicatie van zijn beslissingen; elk college staat autonoom in voor de bekendmaking ervan. De toegankelijkheid van de rechtspraak in België wordt in het algemeen voorzien door middel van openbare (Juridat…) of private gegevensbanken (Jura, Stradalex, Jurisquare…) en via tijdschriften.

347 Commissie voor de Modernisering van de Rechterlijke Orde, *Verslag gewijd aan de bekendmaking van rechterlijke beslissingen. De veer, de Pelikan en de cloud*, 30 juni 2014.

Voor wat betreft de Raad van State, wordt deze kwestie geregeld door een koninklijk besluit en een ministerieel besluit.[348] In de regel geldt de publicatie van alle arresten, met als enig voorbehoud deze in verband met de zeer specifieke materie van de wetgeving betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen. In tegenstelling tot het Hof van Cassatie, bestaat er geen filter die de toegang tot een deel van de rechtspraak verhindert. De Raad van State hanteert immers een tweeledige aanpak wat betreft de publicatie van zijn beslissingen: enerzijds wordt de volledige rechtspraak zeer snel *online* geplaatst, anderzijds wordt in een afzonderlijke databank een beredeneerde en gestructureerde selectie gemaakt van de interessante arresten. De databank is openbaar en kosteloos. Het aan het koninklijk besluit voorafgaand verslag aan de Koning is bijzonder verhelderend in verband met het belang om zekerheden te bieden voor wat betreft de toegankelijkheid van de rechtspraak van dit college. In het koninklijk besluit zelf komt ook de kwestie van de anonimisering aan bod.

Meer in het bijzonder stelde de CMRO vast dat de niet-beschikbaarheid van de rechtspraak van de hoven en rechtbanken een '*democratisch deficit*' doet ontstaan: hoe kan de toegang voor iedereen tot de rechter worden gegarandeerd indien de rechtspraak niet toegankelijk is? Hoe kan het recht worden onderwezen en beoefend wanneer niemand weet hoe er recht wordt gesproken en gedaan?

Wat betreft het Beroepsorgaan, bevat de Wet van 11 december 1998 hierover geen enkele bepaling. De verschillende veiligheidsoverheden hebben ondertussen al wel hun bezorgdheid uitgesproken wat betreft de publicatie van de beslissingen.

De voorzitter van het Beroepsorgaan is zich ervan bewust dat zijn rechtspraak betrekking heeft op specifieke kwesties, waarvan sommige verband kunnen houden met de veiligheid van de Staatsbelangen. Het lijdt geen twijfel dat anonimisering in dit opzicht stelselmatig en op zeer voorzichtige wijze moet gebeuren. De problematiek van de anonimisering hangt in België nauw samen met die van de bescherming van de persoonlijke levenssfeer in het domein van de gegevensbanken. In het licht van zijn bevoegdheid – beperkt tot natuurlijke personen – stelde

348 Koninklijk besluit van 7 juli 1997 betreffende de publicatie van de arresten en de beschikkingen van niet-toelaatbaarheid van de Raad van State en ministerieel besluit van 3 februari 1998 tot bepaling van het informatienetwerk dat toegankelijk is voor het publiek en van de magnetische drager met het oog op de raadpleging en de registratie van de arresten van de Raad van State.

de gewezen Commissie voor de bescherming van de persoonlijke levenssfeer eerder al een doorgedreven anonimisering voor.[349]

Een debat over de publicatie van de beslissingen van het Beroepsorgaan door de Kamer van volksvertegenwoordigers in het kader van de democratische versterking van de instellingen lijkt dan ook aangewezen.

IX.2.4.2. De openbaarheid van de zittingen

Artikel 6 van het EVRM voorziet in het recht op een eerlijk proces en behandelt in het bijzonder in zijn eerste lid de kwestie van de openbaarheid van de zittingen en van de uitspraak van de genomen beslissingen. De Belgische wetgever heeft in 1998 geen bepalingen aangaande de openbaarheid van de zittingen opgenomen in de organieke wet op het Beroepsorgaan.

Uit een analyse van het Europees Hof komen de volgende algemene principes naar voren inzake zittingen[350]:

"In principe heeft de rechtsonderhorige recht op een openbare zitting, daar hij op deze manier beschermd is tegen een geheime justitie die aan de controle van het publiek ontsnapt. Door de transparantie die ze aan de rechtsbedeling verleent, helpt de openbare zitting het doel van artikel 6 § 1, i.e. een eerlijk proces, verwezenlijken. Hoewel het houden van een openbare zitting een fundamenteel beginsel is dat wordt bekrachtigd door artikel 6 § 1, gaat het niet om een absolute verplichting (De Tommaso t. Italië [GC], 2017, § 163). Om te bepalen of een proces voldoet aan de vereiste van openbaarheid, dient men de hele procedure te bekijken (Axen t. Duitsland, 1983, § 28).

In een procedure die voor een enkele rechtbank wordt gehouden, houdt het recht van eender wie op het feit dat zijn zaak 'in het openbaar zou worden gehoord', in de betekenis van artikel 6 § 1, het recht op een 'zitting' in (Göç t. Turkije [GC], 2002, § 47; Fredin t. Zweden (nr. 2), 1994, §§ 21-22; Allan Jacobsson t. Zweden (nr. 2), 1998, § 46; Selmani e.a. t. de Voormalige Joegoslavische Republiek Macedonië, 2017, §§ 37-39).

---

349 Advies nr. 42/97 van 23 december 1997 en aanbeveling nr. 03/2012 van 8 februari 2012. In 1997 schreef de Commissie voor de bescherming van de persoonlijke levenssfeer: *"De bescherming is des te noodzakelijker daar de navigatieprogrammatuur en het vermogen van de informatiesystemen wat de onderlinge verbindingen tussen gegevens betreft, steeds krachtiger worden en er zo goed als geen controle bestaat op het gebruik dat van de systemen wordt gemaakt via deze opvragingen op afstand. Men kan zich aldus indenken hoe makkelijk het voor een goed geïnformeerd internaut is om de ganse rechtspraak te verzamelen over ontslagen wegens ernstige redenen, om er naam en adres van de betrokken werknemers uit te halen, of de geneesheren te identificeren wier aansprakelijkheid voor de rechtbank zou zijn gebracht. Het gedrag van een rechter tegenover een bepaald type conflict zal statistisch kunnen worden geëvalueerd en de naam van een advocaat zal kunnen worden geassocieerd met een percentage van processen die een gunstige afloop kennen."* (Advies CBPL nr. 42/97 van 23 december 1997).

350 RAAD VAN EUROPA, EUROPEES HOF VOOR DE RECHTEN VAN DE MENS, *Guide sur l'article 6 de la Convention européenne des droits de l'homme*, 31 december 2021 (vrije vertaling) https://www.echr.coe.int/documents/guide_art_6_fra.pdf

De openbaarheid van de debatten moet ook worden gelezen vanuit de invalshoek van de aanwezigheid van publiek en pers: De openbaarheid van de gerechtelijke debatten beschermt de rechtsonderhorigen tegen een geheime justitie die ontsnapt aan de controle van het publiek en vormt aldus een van de middelen die bijdragen tot het behoud van het vertrouwen in de rechtbanken. Ze helpt het doel van een eerlijk proces bereiken (Martinie t. Frankrijk [GC], 2006, § 39; Diennet t. Frankrijk, 1995, § 33; Gautrin e.a. t. Frankrijk, 1998, § 42; Hurter t. Zwitserland, 2005, § 26; Lorenzetti t. Italië, 2012, § 30). Artikel 6 § 1 belet echter niet dat rechtscolleges kunnen beslissen, rekening houdend met de bijzonderheden van een zaak, om af te wijken van dit beginsel (Martinie t. Frankrijk [GC], 2006, §§ 40-44). Een zaak achter gesloten deuren, volledig of gedeeltelijk, moet dan strikt worden geregeld door de omstandigheden van de zaak (Lorenzetti t. Italië, 2012, § 30). De tekst van artikel 6 § 1 voorziet in meerdere uitzonderingen. Dit artikel bepaalt: "[...] de toegang tot de rechtszaal kan aan de pers en het publiek worden ontzegd, gedurende de gehele terechtzitting of een deel daarvan":

– "in het belang van de goede zeden, van de openbare orde of nationale veiligheid in een democratische samenleving" (B. en P. t. Verenigd Koninkrijk, 2001, § 39; Zagorodnikov t. Rusland, 2007, § 26);

– "wanneer de belangen van minderjarigen of de bescherming van het privé leven van de procespartijen dit eisen": de belangen van minderjarigen of de bescherming van het privéleven van de partijen bij het proces staan bijvoorbeeld op het spel in het kader van procedures betreffende de hoede over minderjarige kinderen als gevolg van de echtscheiding of de feitelijke scheiding van de ouders, of bij geschillen tussen leden van eenzelfde familie (ibidem, § 38). In zaken die echter betrekking hebben op de plaatsing van een kind in een openbare instelling, moeten de redenen om de zaak aan het onderzoek van het publiek te onttrekken aandachtig worden onderzocht (Moser t. Oostenrijk, 2006, § 97). In het geval van een tuchtrechtelijke procedure tegen een arts, waarbij de noodzaak om het beroepsgeheim of de persoonlijke levenssfeer van de patiënten te beschermen een reden kan zijn om de zaak achter gesloten deuren te houden, moet deze laatste strikt worden geregeld door de omstandigheden (Diennet t. Frankrijk, 1995, § 34). Voor een voorbeeld van een procedure tegen een advocaat, zie Hurter t. Zwitserland, 2005, §§ 30-32;

– " in die mate als door de rechter onder bijzondere omstandigheden strikt noodzakelijk wordt geoordeeld, wanneer de openbaarheid de belangen van een behoorlijke rechtspleging zou schaden": het is mogelijk om af te wijken van het principe van de openbaarheid van de debatten om de veiligheid en de intimiteit van de getuigen te beschermen of ter bevordering van de vrije uitwisseling van informatie en meningen in de voortzetting van de zaak (B. en P. t. Verenigd Koninkrijk, 2001, § 38; Osinger t. Oostenrijk, 2005, § 45).

Het Hof heeft toegevoegd dat de rechtspraak betreffende het houden van een zitting als zodanig – vooral met betrekking tot het recht zich uit te drukken voor de rechtbank zoals bedoeld in artikel 6 § 1 – van toepassing kon zijn naar analogie met het

houden van debatten die voor het publiek toegankelijk zijn. Aldus moet een zitting die plaatsvindt krachtens het nationaal recht in principe openbaar zijn. Het houden van een openbare zitting is echter niet absoluut, waarbij de omstandigheden die toelaten ervan af te wijken voornamelijk afhankelijk zijn van de aard van de vragen die bij interne rechtbanken aanhangig worden gemaakt (De Tommaso t. Italië [GC], 2017, §§ 163-167). "Uitzonderlijke omstandigheden – meer bepaald het uiterst technische karakter van de vragen waarover een uitspraak moet worden gedaan – kunnen het ontbreken van openbaarheid rechtvaardigen, op voorwaarde dat de specificiteit van de materie geen controle van het publiek vereist" (Lorenzetti t. Italië, 2012, § 32).

De loutere aanwezigheid van geclassificeerde documenten in een gerechtelijk dossier leidt er niet automatisch toe dat het publiek wordt uitgesloten van de debatten. Alvorens het publiek uit te sluiten van een bijzondere zaak, zou de rechtbank op specifieke wijze moeten nagaan of een dergelijke uitsluiting noodzakelijk is om een openbaar belang te beschermen en die uitsluiting beperken tot wat strikt noodzakelijk is om het beoogde doel te bereiken (Nikolova en Vandova t. Bulgarije, 2013, §§ 74-77 in verband met een zaak achter gesloten deuren wegens documenten die als staatsgeheim zijn geklasseerd; zie ook over de principes, Vasil Vasilev t. Bulgarije, 2021,§§ 105-106)." [vrije vertaling]*

De kwestie van de openbaarheid van de zittingen vereist een bijzondere aandacht van en een grondig debat in de Kamer van volksvertegenwoordigers. De voorzitter van het Beroepsorgaan is bereid om op actieve wijze mee te werken aan dit proces.

IX.2.5. DE DOELTREFFENDHEID VAN DE BESLISSINGEN VAN HET BEROEPSORGAAN

Een kwestie van de doeltreffendheid van de beslissingen van het Beroepsorgaan doet zich voor ten aanzien van de Nationale Veiligheidsoverheid (NVO). Naast de weigering om administratieve dossiers toe te sturen in het kader van bepaalde beroepen, wijst de voorzitter van het Beroepsorgaan op wat wordt bepaald in artikel 12 § 6 van de organieke wet: "*De beslissingen van het beroepsorgaan zijn vanaf hun kennisgeving rechtstreeks uitvoerbaar.*"

Het Beroepsorgaan had in een zaak aan de betrokkene een veiligheidsmachtiging (niveau 'GEHEIM EU') verleend die hem was geweigerd door de NVO. Op 19 juli 2021 gaf de Franstalige rechtbank van eerste aanleg van Brussel (A.R. 2021/51/C) bij een op tegenspraak verleende beschikking in kort geding aan de Belgische Staat het bevel, via de NVO, om aan de verzoeker zijn veiligheidsmachtiging te verlenen binnen de maand volgend op de betekening van de beschikking. Dit op straffe van een dwangsom die werd vastgesteld op € 500 per dag vertraging, met een maximum van € 10.000.

In hetzelfde dossier waren de Federale Ombudsmannen, tot wie de betrokkene zich had gewend wegens de niet-uitvoering van de beslissing van het Beroepsorgaan, tussengekomen, doch zonder succes. Ze beschouwden de klacht als gegrond, en gaven volgende motivering: *"[...] In een rechtsstaat doet de niet-uitvoering van een beslissing die is genomen in het kader van een administratief beroep op ernstige wijze afbreuk aan de rechtszekerheid."*

IX.2.6. VOORUITZICHTEN

In uitvoering van de aanbevelingen van het Vast Comité I, neemt de minister van Defensie zich voor om wetsontwerpen in te dienen met als doel het principe van een veiligheidsverificatie voor zowel het burger- als het militair personeel van Landsverdediging te systematiseren. Dit veiligheidsadvies zou niet langer enkel bij de kandidaatstelling vereist zijn, maar voor de volledige duur van de loopbaan van de verschillende medewerkers van Landsverdediging. We kunnen aannemen dat een dergelijk veiligheidsadvies om de vijf jaar zal worden vernieuwd. Eventuele beroepen zullen in principe tot de bevoegdheid van het Beroepsorgaan behoren.

Naar aanleiding van het toezichtonderzoek van september 2021 van het Vast Comité I naar de wijze waarop de Veiligheid van de Staat de regeringscommissaris Ihsane Haouach opvolgde, beval dit Comité aan dat de uitoefening van bepaalde 'openbare functies' de voorafgaande controle vereist van de integriteit, de loyaliteit en de discretie, zoals reeds vereist in sommige Europese landen. De uitvoering van deze aanbeveling zou moeten leiden tot een uitbreiding van de veiligheidsadviezen dewelke eveneens het voorwerp zullen uitmaken van een jurisdictionele controle door het Beroepsorgaan.

Ten slotte moet er worden tegemoetgekomen aan de vrijstelling van de portkosten, alsook met de mogelijkheid een beroep op digitale wijze in te dienen en toe te staan dat de akten van betekening, volgens de voorkeur van de rechtsonderhorige, via de post of op digitale wijze worden toegestuurd in het kader van de procedure hangende voor het Beroepsorgaan.

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 2021 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.[351], [352]

In afwachting van de benoeming van een griffier, werd Wauter Van Laethem (N) aangesteld als plaatsvervangend griffier.[353]

Bij de Dienst Enquêtes I, sinds 1 januari 2021 onder leiding van Fabian Poncelet (F), werden enkele wijzigingen opgetekend. In juni 2021 trad een nieuwe Franstalige commissaris-auditor aan; hij wordt gedetacheerd vanuit de Federale Politie. Een commissaris-auditor nam ontslag en zal in de loop van 2022 worden vervangen.

Ten slotte bleef ook de administratieve staf van het Vast Comité I niet ongewijzigd. De in december 2020 aangeworven Franstalige statutaire jurist van de Afdeling documentatie en juridische analyse keerde in augustus 2021 terug naar zijn dienst van oorsprong. Aan dezelfde afdeling werden in oktober 2021 twee

---

351 Thibaut Vandamme legde op 11 januari 2021 de eed af. Met toepassing van art. 157, nr. 6 van het Kamerreglement, werd in de plenaire vergadering van 20 mei 2021 Thierry Werts verkozen verklaard voor het mandaat van eerste plaatsvervanger van Thibaut Vandamme (CRABV55PLEN105, 20 mei 2021, 46).

352 Wauter Van Laethem nam eind 2021 ontslag als tweede plaatsvervangend lid van het Nederlandstalige lid (*Hand*. Kamer 2021-22, 10 november 2021, CRIV55PLEN139, 68). Hij werd in maart 2022 vervangen door Filip Vanneste, substituut-procureur-generaal bij het Hof van Beroep te Antwerpen (*Hand.* Kamer 2021-22, 24 maart 2022, CRIV55PLEN171, 67).

353 Een oproep tot benoeming van griffier van het Vast Comité I verscheen halfweg mei 2020 in het Belgisch Staatsblad. Op 21 juni 2021 werd een wetsvoorstel ingediend tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van de Vaste Comités I en P (*Parl. St.* Kamer 2020-21, 55K2064/001). De aangelegenheid werd eerst besproken in de Conferentie van voorzitters (24 februari en 3 maart 2021) (*Hand*. Kamer 2020-21, 55K1924/001). De 'Wet van 14 augustus 2021 tot wijziging van de wet van 18 juli 1991 […], alsook tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van het Vast Comité I en het Vast Comité P' verscheen in het Belgisch Staatsblad op 8 december 2021. Een nieuwe vacature verscheen in het Staatsblad 19 juli 2021. Op 26 april 2022 legde Frédéric Givron (F) in handen van de Kamervoorzitster de eed af als nieuwe griffier van het Vast Comité I.

Franstalige medewerkers toegevoegd. Ook werd in april 2021 een Nederlandstalige statutaire secretaresse aangeworven. Eind 2021 telde de administratieve staf 18 personeelsleden.

Halfweg juni 2021 werd door de voorzitter van het Vast Comité I bij de voorzitster van de Kamer van Volksvertegenwoordigers het personeelsgebrek en de sterk toegenomen takenpakket opnieuw aangekaart.[354] Niettegenstaande de dynamiek die de Kamer aan de dag legt in het kader van de synergiedoelstellingen, die onderschreven worden door het Comité, zag het Comité zich genoodzaakt om een dringende versterking te bepleiten. 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.

X.2. EEN WELZIJNSAUDIT OP HET COMITE

Naar aanleiding van signalen van onwelzijn op het Vast Comité I, werd IDEWE, een externe dienst voor preventie en bescherming op het werk, de opdracht gegeven om een analyse van de psychosociale risico's uit te voeren. De audit analyseerde thema's die overeenstemmen met de vijf domeinen van psychosociale risico's op het werk (arbeidsinhoud, arbeidsorganisatie, arbeidsomstandigheden, arbeidsvoorwaarden en interpersoonlijke relaties op het werk). Dit resulteerde in een omstandig rapport[355], met daarin de resultaten van de analyse en een advies aan de werkgever.[356]

Op basis daarvan werd een veranderingstraject opgestart. Het Vast Comité I zal daarin begeleid worden door de FOD Beleid en Ondersteuning. Er wordt onder meer voorzien in een stakeholdersbevraging en een grondige SWOT- en PESTEL-analyse[357]. De afronding van het project wordt voorzien eind juni 2022.

Naar aanleiding van de resultaten van de welzijnsaudit, werd half december 2021 alvast een nieuwe Nederlandstalige vertrouwenspersoon aangesteld. De benoeming van een Franstalige vertrouwenspersoon volgde eind januari 2022.[358]

---

354 Brief van de Voorzitter van het Vast Comité I aan de Voorzitster van de Kamer van Volksvertegenwoordigers d.d. 16 juni 2021.

355 IDEWE, Analyse van de psychosociale risico's, 23 november 2021, 31 p.

356 Er werd voorgesteld het 'teamdoelmatigheidsmodel' (SDRPI) te hanteren om de vastgestelde probleemsituaties te verhelpen. Daarbij wordt ingezet op de **S**ituatie (context waarbinnen wordt gewerkt), de **D**oelen (creëren van heldere en gedeelde doelen), de **R**ollen (wat mag van wie verwacht worden), de **P**rocedures (ontwikkeling van gepaste werkwijzen) en de **I**nterpersoonlijke relaties.

357 De PESTEL-analyse is een bedrijfskundig model dat wordt gebruikt voor het identificeren van de invloed van externe factoren op een organisatie. PESTEL staat voor politiek, economisch, sociologisch, technologisch, ecologisch en legal (juridisch).

358 De wetgeving (2014) rond psychosociale risico's op het werk verplicht vertrouwenspersonen een basisopleiding van 30 lesuren te volgen. Een werknemer die aangesteld is als vertrouwenspersoon moet binnen de twee jaar na zijn aanstelling een opleiding volgen.

X.3. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE

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 kende in 2021 een andere samenstelling. Maakten als stemgerechtigde leden deel uit van de commissie: Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen)[359], 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 Boukli (PVDA-PTB), Patrick Dewael[360] (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 2021 vonden, ondanks de sanitaire crisis, meerdere (negen in totaal) vergaderingen plaats. Tijdens deze commissievergaderingen werden – achter gesloten deuren – diverse door het Vast Comité I afgesloten toezichtonderzoeken besproken.[361] Eind april en begin juli 2021 werd in vergaderingen samen met het Vast Comité P voorzien voor de bespreking van respectievelijk de gemeenschappelijke toezichtonderzoeken over het Coördinatieorgaan voor de dreigingsanalyse (OCAD) en de steundiensten enerzijds en naar de rol van het OCAD in de opvolging van Jürgen Conings anderzijds. Verder werd tijd uitgetrokken voor de bespreking van het verslag opgesteld in het kader van zijn controlebevoegdheid – samen met het Controleorgaan op de politionele informatie (COC) – aangaande de gemeenschappelijke gegevensbanken (art. 44/6 WPA). Tijdens haar vergadering van 22 september 2021 werd het algemeen *Activiteitenverslag 2020* besproken.[362] De Commissie benadrukte onder meer "*dat het jaarverslag niet alleen belangrijk is om rekenschap aangaande de activiteiten van het Vast Comité I ten aanzien van het Parlement af te leggen, maar ook om buitenstaanders (academici, journalisten, medewerkers van de inlichtingendiensten enzovoort op volstrekt transparante wijze te informeren*". Een aantal thema's weerhielden de bijzondere aandacht van de Kamerleden, zoals de *follow-up* van klachten, het Memorandum of Understanding (MoU) tussen de ADIV en de inlichtingendiensten van Rwanda, COVID-19 en de rol van de inlichtingendiensten of nog, de buitenlandse intercepties. De Commis-

359 Ondertussen vervangen door Julie Chanson (Ecolo-Groen).
360 Ondertussen vervangen door Tim Vandenput (Open Vld).
361 Eenmaal werd een vergadering belegd waarin de tussentijdse rapportage (stand van zaken) van het toezichtonderzoek m.b.t. Jürgen Conings werd geagendeerd.
362 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).

sie nam als eindconclusie "*akte van het activiteitenverslag 2020 van het Vast Comité I en verleent haar goedkeuring aan de aanbevelingen van het Vast Comité I*".[363]

De Commissie boog zich ten slotte ook over de interne problematiek[364] aan de top van het Vast Comité I; daartoe werden in het najaar van 2021 drie commissievergaderingen achter gesloten deuren georganiseerd.

X.4. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITE P

In 2021 vonden, behoudens enkele (informele) contacten op de werkvloer, geen gemeenschappelijke vergaderingen plaats.[365]

In 2021 waren drie gemeenschappelijke toezichtonderzoeken aan de orde: het opvolgonderzoek naar de implementatie van de door de Vaste Comités I en P geformuleerde aanbevelingen in het kader van het onderzoek naar de ondersteunende diensten van het OCAD (cf. I.1) en het toezichtonderzoek naar de vier 'bijkomende' ondersteunende diensten van het OCAD (cf. I.2). Het derde gemeenschappelijk onderzoek betrof dit naar de 'rol van het OCAD in de opvolging van de militair Jürgen Conings' (cf. I.10). Daartoe werd actief samengewerkt door de ondersteunende diensten van beide Comités.

Wel werden door beide Comités aan hun enquêtediensten de opdracht gegeven om werkprocessen voor te bereiden voor de afhandeling van gemeenschappelijke klachten en toezichtonderzoeken. Ook werd door het Vast Comité P ingestemd met het verzoek van het Vast Comité I, meer in het bijzonder van zijn Dienst Enquêtes, tot het verkrijgen van een opleiding in het kader van de raadpleging van de Algemene Nationale Gegevensbank (ANG).[366] Ten slotte werden, conform art. 52 W.Toezicht, ook activiteitenverslagen en toezichtrapporten onderling uitgewisseld.

---

363 *Parl. St.* Kamer 2020-21, nr. 55K2209/001, 20 oktober 2021 (Activiteitenverslag 2020 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).

364 De Commissie vergaderde onder meer na het verschijnen van een artikel in de nasleep van het rapport in de zaak-Jürgen Conings (Q. JARDON, 'Serge Lipszyc. Gendarme des services secrets', *Wilfried*, Automne 2021, Nr. 17, 1-7) en een verzoek dat bij de Kamervoorzitster werd neergelegd door twee raadsheren.

365 Art. 52 W.Toezicht stelt dat minstens twee maal per jaar gemeenschappelijke vergaderingen dienen plaats te vinden.

366 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).

X.5. EEN AANZIENLIJKE AANDACHT VANUIT DE MEDIA

Anders dan voorgaande jaren, was het Vast Comité I in 2021 voorwerp van een aanzienlijke media-aandacht. Vier gebeurtenissen (opgenomen in chronologische volgorde) lagen hieraan ten grondslag.

Vooreerst was er de publicatie van het toezichtsonderzoek naar de opvolging van extreemrechts door de Belgische inlichtingendiensten.[367] De voornaamste bevindingen van dit onderzoek werden overgenomen door meerdere Belgische media.

Vervolgens werd de zaak-Jürgen Conings, en de rol daarin toegemeten aan het Vast Comité I, sterk gemediatiseerd. Ter herinnering, het Vast Comité I werd door de minister van Defensie verzocht een toezichtonderzoek te openen om de betrouwbaarheid van informatie over vermoedelijke geradicaliseerden binnen Defensie na te gaan, en aanbevelingen te doen om de goede werking van de ADIV, maar ook van Defensie als geheel, te waarborgen.[368] De (sterk ingewachte) conclusies van dit rapport werden breed uitgemeten in de media.

Daarnaast werd het Vast Comité I gevat in de zaak-Ishane Haouach, voormalig regeringscommissaris bij het Instituut voor de gelijkheid van mannen en vrouwen (IGMV).[369] De aandacht voor deze zaak was groot en begon toen in de media het bestaan van een nota van de Veiligheid van de Staat werd bekendgemaakt waarin sprake was van 'nauwe contacten' tussen de Moslimbroederschap en de regeringscommissaris, al dan niet bewust wat deze laatste betrof.

Tot slot was er het interview dat de voorzitter van het Comité gaf aan het tijdschrift *Wilfried* en dat in oktober 2021 werd gepubliceerd *(supra)*. Hierin gaf de voorzitter uiting aan enkele van zijn persoonlijke zorgen naar aanleiding van verschillende belangrijke gebeurtenissen en dossiers, zoals bijv. over de zaak-Jürgen Conings. Dit interview, en de reacties die erop volgden alsook de daaropvolgende deining binnen de directie van het Comité, kreeg veel de aandacht in de pers.

Vermist het Comité er zich van bewust is dat communicatie omtrent zijn opdrachten een complexe maar essentiële aangelegenheid is, nam het Comité zich voor om in de toekomst meer aandacht aan deze kwestie te besteden, met name door de informatieverstrekking te verbeteren. De toekomstige herziening van zijn website is volledig in overeenstemming met deze aanpak.

---

367 VAST COMITÉ I, *Activiteitenverslag 2020,* 38 e.v. ('I.7. De opvolging van extreemrechts door de Belgische inlichtingendiensten').

368 Hierover 'I.9. Het opsporen en opvolging van de radicalisering van een militair: de zaak-Jürgen Conings'.

369 Hierover 'I.11. De opvolging van een regeringscommissaris door de VSSE'.

X.6. DE *DATA PROTECTION OFFICER* OP HET COMITÉ

Binnen het Comité is al enkele jaren een *Data Protection Officer* (DPO) aangesteld voor alle verwerkingen van persoonsgegevens die buiten de 'nationale veiligheid' vallen. In het kader van de synergie-oefening vanuit de Kamer van volksvertegenwoordigers vervult de functionaris voor gegevensbescherming deze rol ook voor andere dotatiegerechtigde instellingen die in het Forumgebouw resideren. De functionaris voor gegevensbescherming verleende advies inzake camerabewaking waarbij een register werd opgesteld en de aangifte werd geformaliseerd naar aanleiding van de zgn. 'nieuwe Camerawet'.[370] Daarnaast gaf de DPO ook advies- en informatieverlening inzake het intern beheer van de persoonsgegevens van de personeelsleden, onder andere in het kader van de COVID-19-pandemie.

X.7. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Het 'budget 2020' van het Vast Comité I werd vastgelegd op 5,215 miljoen euro, wat een vermeerdering inhield van 13% ten aanzien van het budget 2020.[371]

De voornaamste reden voor deze stijging was de indiening van een operationeel project voor de digitalisering van de werkprocessen. Dit project werd voorgesteld in partnerschap met een industriële operator dewelke vertrouwd is met overheidsdiensten en hun administratieve procedures. Hoewel de Commissie voor de Comptabiliteit het door het Comité voorgestelde initiatief steunde, werd vooralsnog besloten het geautomatiseerd documentenbeheer te bevriezen in afwachting van de bevindingen van het lopende overleg tussen de diensten van de Quaestuur en het Comité, opdat het project zou kunnen worden geïntegreerd in eventuele synergiën.

De financieringsbronnen van het budget werden door de Kamer van Volksvertegenwoordigers[372] als volgt toegewezen: 74,44 % dotatiebudget en 25,56 % boni van 2019.

De uitvoering van het budget 2020 leverde een budgettaire bonus op van 1,87 miljoen euro's (niet geaudite cijfers) 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

370 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.

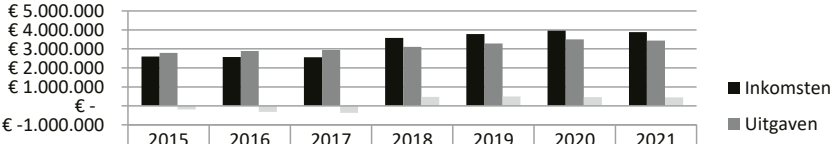
371 *Hand.* Kamer 2020-21, CRIV55PLEN081, 63.

372 *Parl. St.* Kamer 2020-21, 55K01676/001, 30-34.

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. Deze tendens was bijzonder uitgesproken in 2021 aangezien het Comité geconfronteerd werd met een aantal samenlopende omstandigheden, zoals de oprusttstelling van diverse personeelsleden en vertragingen bij de vervanging daarvan. Er kan worden gesteld dat er in 2021 een aanzienlijk personeelsverloop was in zowat elke personeelscategorie, zowel op leidinggevend als op uitvoerend niveau: de post van griffier bleef bijvoorbeeld het hele jaar vacant totdat de Kamer van volksvertegenwoordigers recent een opvolger benoemde. Verschillende medewerkers opteerden dan weer voor een andere carrièrekeuze. Samen met de bevriezing van het budget voor het digitaliseringsproject (zie hierboven), waartoe de Kamer heeft besloten, leverde dit alles een aanzienlijke boni op, dewelke waarschijnlijk zal worden toegewezen aan de operationele begroting voor 2023 wanneer de begrotingsvoorstellen door de Kamer van volksvertegenwoordigers worden besproken.

Vast Comité I: Evolutie van de balans



	2015	2016	2017	2018	2019	2020	2021
Inkomsten	€ 2.597	€ 2.570	€ 2.565	€ 3.582	€ 3.780	€ 3.963	€ 3.882
Uitgaven	€ 2.792	€ 2.889	€ 2.937	€ 3.106	€ 3.284	€ 3.500	€ 3.437
Resultaat	€ -194.	€ -318.	€ -372.	€ 475.4	€ 496.0	€ 463.0	€ 444.8

Vanaf het begrotingsjaar 2023 zal het Comité volledig worden geïntegreerd in het door de Kamer geïnitieerde synergie-project[373], hetgeen onmiskenbare gevolgen zal hebben voor de werking van de dotatiegerechtigde instellingen in het algemeen en van het Vast Comité I in het bijzonder. Deze veranderingen zullen gevolgen hebben voor zowel het personeelskader als voor de werkingskredieten, die zoveel mogelijk zullen worden samengevoegd. De spildatum voor de invoegetreding van deze veranderingen werd vastgesteld op 1 januari 2023.

373 *Parl. St.* Kamer 2020-21, 55K01924/001.

X.8. 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.[374] 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.[375]

Tussen januari en begin februari 2021 werden alle betrokken instellingen, waaronder ook het Vast Comité I, door de diensten van de Quaestuur en het secretariaat van de Commissie voor de Comptabiliteit bevraagd.

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 (Incentris) en een burgerportaal. 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. Ook werd beslist om een deel van de kantoren van het Vast Comité I toe te wijzen aan de BIM-Commissie. Om deze beleidslijnen te concretiseren, werden thematische werkgroepen opgericht waaraan leden van de Kamer en bepaalde instellingen deelnemen, met als logica een vertegenwoordiging per 'familie' van instellingen (een familie wordt gevormd door instellingen met verwante opdrachten).[376] [377]

In september 2021 werd door de Kamer een bijeenkomst georganiseerd voor de personeelsleden van de betrokken instellingen, om hen te informeren over de beleidslijnen waartoe werd besloten alsook over de stand van zaken van de projecten.

Voor het toewijzen van bepaalde kantoren van het Vast Comité I aan de BIM-Commissie, werden vanaf oktober 2021 verscheidene bezoeken georganiseerd, in aanwezigheid van de architect van de Kamer. Er werden ook vergaderingen gehouden met de BIM-Commissie, het Vast Comité I en de architect om

---

374 Het Rekenhof richtte zich vooral op de budgettaire aspecten (een analyse van de inkomsten en uitgaven) en op de afbakening van de taken van de diverse instellingen. Ernst and Young op zijn beurt analyseerde de processen, de systemen en de organisatie die in elk van deze instellingen aanwezig zijn.

375 *Dotatiegerechtigde instellingen. Opdrachten – Ontvangsten – Uitgaven.* Audit op vraag van de Commissie voor de Comptabiliteit van de Kamer van Volksvertegenwoordigers, Verslag goedgekeurd op 28 maart 2018 door de algemene vergadering van het Rekenhof.

376 Het Vast Comité I behoort tot de familie 'Veiligheid en bescherming', en dit samen met het Vast Comité P, de Gegevensbeschermingsautoriteit, het Controleorgaan op de politionele informatie en de BIM-Commissie.

377 Halfweg oktober 2021 werd door de Kamervoorzitster aangedrongen op een meer actieve participatie en een performante informatiedoorstroming vanuit het Vast Comité I opdat de in het kader van het synergieproject tussen de dotatiegerechtigde instellingen opgerichte werkgroepen, in staat zouden worden gesteld hun taken naar behoren uit te voeren. De Voorzitster was er zich van bewust dat het ontbreken van een griffier deze opdracht kon bemoeilijken.

de implicaties en de kosten van een dergelijk project in te kunnen schatten. In de loop van 2022 zal, met het oog op de verhuis van de BIM-Commissie, een dossier worden voorgelegd aan Commissie voor de Comptabiliteit.

X.9. 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.[378] Door de strikte coronamaatregelen konden geen interne of externe opleidingen worden bijgewoond in de loop van 2021.

[378] Er vonden wel de door de medewerkers verplicht bij te wonen veiligheidsbriefings plaats.

HOOFDSTUK XI.
AANBEVELINGEN

Op basis van de in 2021 afgesloten toezichtonderzoeken, controles en inspecties formuleert het Vast Comité I onderstaande aanbevelingen. Zij hebben zowel betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen, op de coördinatie en de efficiëntie van de inlichtingendiensten, het Coördinatieorgaan voor de dreigingsanalyse (OCAD) en de ondersteunende diensten als op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I.

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

XI.1.1. UITWERKEN VAN EEN VOORSTEL VAN RICHTLIJN I.V.M. MEDELING VAN INFORMATIE DOOR DE VSSE OF DE ADIV AAN WERKGEVERS EN AANPASSING VAN BESTAANDE RICHTLIJNEN[379]

Het Comité beveelde aan dat de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) binnen zes maanden na het afsluiten van zijn toezichtonderzoek naar '*De uitwisseling van informatie over een werknemer tussen de inlichtingendiesnten en een private- of publieke werkgever*' een voorstel tot richtlijn ter uitvoering van de laatste zinsnede van artikel 19, eerste lid, van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (W.I&V) zou opstellen ten behoeve van respectievelijk de minister van Justitie en van Defensie met het verzoek het voorstel ter goedkeuring voor te leggen aan de Nationale Veiligheidsraad (NVR).

Tevens dient de VSSE zijn richtlijnen ter zake te evalueren en aan te passen aan het wettelijke kader. Gelet op het belang van deze materie, dient deze aanpassing ook te gebeuren binnen een termijn van zes maanden.

---

379 Zie Hoofdstuk 'I.3. De uitwisseling van informatie over een werknemer tussen de inlichtingendiensetn en een private- of publieke werkgever'

Verder beveelt het Comité aan dat de wetgever zou verduidelijken of artikel 19, eerste lid, laatste zin W.I&V ook een verplichting inhoudt om onder bepaalde gevallen *verplicht* te antwoorden op een vraag of om *op eigen initiatief* gegevens te verstrekken. In afwachting van een wetgevend initiatief moet deze kwestie geregeld worden in de richtlijn van de Nationale Veiligheidsraad.

XI.1.2. RICHTLIJNEN INZAKE DE OPVOLGING VAN POLITIEKE MANDATARISSEN[380]

Het Vast Comité I herhaalt met klem zijn eerdere aanbeveling uit 2013 dat de ADIV eenduidige richtlijnen moet opstellen met betrekking tot de inwinning, de verwerking, de raadpleging, de opslag en de archivering van gegevens van politieke mandatarissen.

Het Vast Comité I beveelt ook aan dat de inlichtingendiensten in hun rapportage de nodige aandacht moeten besteden aan de positie van een in een verslag vermeld persoon ten aanzien van de dreiging (slachtoffer, actor, passant, …).

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

XI.2.1. AANBEVELINGEN M.B.T. HET OCAD EN ZIJN (NIEUWE) ONDERSTEUNENDE DIENSTEN[381]

Informatieverstrekking of opleiding voor bij het OCAD gedetacheerde personeelsleden van het Directoraat-generaal Penitentiaire Inrichtingen

Er werd vastgesteld dat de personeelsleden gedetacheerd uit het directoraat-generaal Penitentiaire Inrichtingen (DG EPI) weinig of zelfs helemaal geen bezoeken brengen aan hun dienst van oorsprong en zeggen dat ze niet op de hoogte worden gebracht van eventuele wijzigingen die zijn doorgevoerd binnen hun vroegere dienst. Een regelmatige informatieverstrekking of opleiding die hen in staat stelt hun kennis van hun ondersteunende dienst van oorsprong bij te werken en op de hoogte te blijven van eventuele wijzigingen, zoals wetgevende of van inwendige orde bijvoorbeeld, zou een meerwaarde zijn.

380 Zie Hoofdstuk 'I.8. De opvolging van politieke mandatrissen'

381 Zie hoofdstukken 'I.1 De ondersteunende diensten van het OCAD' en 'I.2. Het OCAD en de 'bijkomende' ondersteunende diensten'.

BINII voor het DG EPI en de dienst Erediensten en Vrijzinnigheid

Het zou opportuun zijn dat de FOD Justitie snel beschikt over het BINII-systeem (*B*elgian Intelligence Network Information Infrastructure) om beide diensten toe te laten makkelijker geclassificeerde gegevens uit te wisselen.

Toegang Thesaurie tot GGB

Het zou opportuun zijn dat de Thesaurie zo snel mogelijk beschikt over haar toegangen tot de Gemeenschappelijke gegevensbanken (GGB).

Een functionele mailbox voor de dienst Erediensten en Vrijzinnigheid

Het zou opportuun zijn dat de dienst Erediensten en Vrijzinnigheid beschikt over een functionele mailbox want dergelijke mailbox zou een opvolging van elk verzoek of elk inkomend en uitgaand document garanderen door alle leden van de cel "terrorisme en radicalisme".

Een toegang tot de GGB voor de dienst Erediensten en Vrijzinnigheid in overeenstemming met het wettelijk kader

Er werd vastegesteld dat de dienst Erediensten en Vrijzinnigheid beschikte over een toegang tot de Gemeenschappelijke gegevensbank 'Haatpropagandisten' (GGB HP) die ruimer was dan de toegang waarin het Koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten (KB HP) voorziet. Het Controleorgaan voor politionele informatie (COC) en het Vast Comité I verzochten de verwerkingsverantwoordelijken een einde te stellen aan de gevallen van onregelmatige toegang en bevolen de Federale Politie aan om de technische oplossingen te ontwikkelen die nodig zijn om de toegang door deze dienst in overeenstemming te brengen met de geldende wetgeving (i.e. enkel onrechtstreekse toegang tot de GGB HP). Het COC en het Vast Comité I bevolen de verwerkingsverantwoordelijken ook aan om op juridisch en operationeel vlak na te gaan of de regelgeving betreffende de toegang van de dienst Erediensten en Vrijzinnigheid al dan niet moest worden herzien.

XI.2.2. CORRECTE TOEPASSING VAN DE MOGELIJKHEID OM VEILIGHEIDSSCREENINGS AAN TE VRAGEN[382]

Het Comité nodigt spelers uit de publieke en private sector uit om te onderzoeken voor welke functies, toelatingen of vergunningen bepaalde potentiële dreigingen preventief kunnen ondervangen worden door een beroep te doen op het systeem van de veiligheidsscreenings uit de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (W.C&VM). Het Comité benadrukt wel dat dit systeem oordeelkundig moet gebruikt worden en niet mag leiden tot een ongebreidelde toepassing.

XI.2.3. VERPLICHTE MELDING NAAR WERKGEVER IN GEVAL VAN OPNAME IN EEN GEMEENSCHAPPELIJKE GEGEVENSBANK[383]

Het Comité suggereert om te onderzoeken of het nuttig zou zijn om een verplichte melding naar de werkgever in het leven te roepen ten aanzien van iedere (kandidaat-)werknemer die is opgenomen in de Gemeenschappelijke gegevensbank Terrorist Fighters of Haatpredikers.

XI.2.4. EEN BREED DEBAT OVER DE TAKEN EN DE PRIORITEITEN VAN DE INLICHTINGENDIENSTEN[384]

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 wetenschappelijk of 'strategisch' onderbouwde discussie, want daarvoor bestaat momenteel geen wetenschappelijke methode, 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).

---

382 Zie Hoofdstuk 'I.3. De uitwisseling van informatie over een werknemer tussen inlichtingendiensten en een private- of publieke werkgever'

383 *Ibid.*

384 Zie Hoofstukken 'I.5. De opvolging van schadelijke sektarische organisaties en criminele organisaties' en 'I.9. Het opsporen en opvolgen van de radicalisering van een militair: de zaak Jürgen Conings'. Deze aanbeveling kreeg een zeer hoge prioriteit.

XI.2.5. MEER VEILIGHEIDSSCREENINGS VAN MILITAIREN EN BURGERPERSONEEL BIJ DEFENSIE[385]

Het Vast Comité I stelt vast dat de militairen van het departement Defensie, met uitzondering van degenen met een veiligheidsmachtiging, slechts aan één veiligheidsverificatie worden onderworpen, namelijk helemaal aan het begin van hun aanwerving, terwijl duidelijk blijkt dat de integriteit van sommige militairen in de loop van hun opeenvolgende activiteiten of in de loop van de tijd wel degelijk een probleem zou kunnen vormen. Dit betekent dat deze leden alleen als zodanig bekend zullen zijn wanneer zij een bedreiging vormen die door de ADIV werd opgespoord.

Het Vast Comité I merkt op dat burgers van het departement Defensie en reservisten, in tegenstelling tot militairen, op enkele uitzonderingen na, bij hun aanwerving niet worden onderworpen aan een veiligheidsverificatie. Dit verschil in behandeling kan slechts worden gerechtvaardigd indien het ongepaste gebruik van de functie die zij uitoefenen de fundamentele belangen van de Staat niet in gevaar kan brengen. Het Vast Comité I beveelt daarom aan dat de bevoegde administratieve overheid onderzoekt of de door de Wet van 23 februari 2018 gecreëerde mogelijkheid om veiligheidsverificaties te vragen, niet moet worden geactiveerd. Deze wet maakt het mogelijk om na een risico-, dreigings- en impactanalyse te bepalen voor welke functies een veiligheidsadvies is aangewezen.

De wet staat ook toe dat een dergelijke beoordeling om de vijf jaar wordt uitgevoerd en dat in de tussentijd een positief advies wordt omgezet in een negatief advies. In die zin biedt deze wet een interessante mogelijkheid die momenteel niet geldt voor militairen; zij kunnen slechts één keer worden gescreend (d.w.z. bij hun aanwerving). Er moet echter voor ogen worden gehouden dat het huidige 'negatieve advies' voor militairen een *de facto* 'negatieve beslissing' impliceert, terwijl de gevolgen van een 'negatief advies' onder de Wet van 2018 toekomt aan de overheid die het advies vraagt.

Het Vast Comité I merkt op dat leerlingen van de Koninklijke Militaire School (KMS) en van andere scholen die afhangen van het departement Defensie, in tegenstelling tot militairen, op enkele zeldzame uitzonderingen na, bij hun aanwerving niet worden onderworpen aan een veiligheidsverificatie. Dit verschil in behandeling valt niet te rechtvaardigen en deze situatie vormt noodzakelijkerwijs een risico voor departement Defensie dat medewerkers in dienst neemt zonder dat het idealiter degenen heeft kunnen opsporen die een bron van bedreiging zouden kunnen vormen of die niet over de morele kwaliteiten zouden beschikken die de uitoefening van hun taken onontbeerlijk zijn, waarbij de tijd ook voorbijgaat.

Het Vast Comité I merkt op dat buitenlandse studenten van de KMS bij hun toelating niet worden onderworpen aan een veiligheidsverificatie. Die zou in elk

[385] Zie Hoofdstuk 'I.7. Veiligheidsscreenings van militairen en burgerpersoneel bij Defensie'

geval moeten worden voorafgegaan door een risicoanalyse door de ADIV. Ze zou voorafgaand en systematisch zijn per geval van kandidaat-leerling.

Deze aanbevelingen zouden moeten worden toegepast voor alle scholen die afhangen van het departement Defensie.

XI.2.6. DE OPRICHTING VAN EEN COHERENT 'INTELLIGENCE' GEHEEL[386]

Het Vast Comité I beveelt de oprichting aan van een coherent 'intelligence' geheel bij Defensie die de volledige militaire inlichtingendienst omvat en de permanente opleiding en ontwikkeling van het betrokken personeel mogelijk maakt. Dit moet de beschikbaarheid van binnen de ADIV opgeleid militair personeel van hoge kwaliteit mogelijk maken. Deze eenheid moet over een maximale autonomie beschikken bij het beheer en de ontwikkeling van haar personeel. Deze aanbeveling is van fundamenteel belang en wordt al vele jaren door het Comité naar voren gebracht.

XI.2.7. STABILITEIT IN HET PERSONEELSBELEID BIJ DE ADIV

Het Vast Comité I beveelt ook aan om stabiliteit te brengen in de inzet van militair personeel en om frequent verloop, zoals dat elders bij Defensie voorkomt, te vermijden. Stabiliteit van vijf jaar moet het doel zijn voor sleutelposities.

XI.2.8. BEKRACHTIGING INLICHTINGEN- (EN VEILIGHEIDS-) STUURPLAN

Het Vast Comité I beveelt aan om het Inlichtingen- (en Veiligheids-) stuurplan onverwijld te bekrachtigen en dat dit jaarlijks wordt goedgekeurd en geëvalueerd en aan de Minister van Defensie (MOD) ter bekrachtiging wordt voorgelegd. Dit strategisch plan bepaalt, overeenkomstig de wettelijke verplichtingen en opdrachten van de ADIV, de middelen die moeten worden ingezet en, rekening houdend met deze middelen, de prioriteiten die worden toegekend.

---

386 De aanbevelingen opgenomen in de punten XI.2.6. tot en met XI.2.16. zijn ontleend aan het toezichtonderzoek naar het opsporen en opvolgen van de radicalisering van een militair: de zaak Jürgen Conings (zie Hoofdtsuk I.9.). Deze aanbevelingen kregen een zeer hoge prioriteit.

XI.2.9. BETERE INTERNE COMMUNICATIE BINNEN ADIV

Het Vast Comité I beveelt aan dat de ADIV aanvullend communiceert naar het personeel toe om hen beter vertrouwd te maken met de structuur, de communicatie en de beslissingslijnen, vooraleer wijzigingen te overwegen. Het heeft geen zin om alle realisaties zomaar in twijfel te trekken. Wel moet waar nodig de nieuwe structuur verankerd worden. Het Comité was er zich wel van bewust dat de "Covid"-periode niet bevorderlijk was voor de interne communicatie die essentieel is voor de lancering van een nieuwe structuur.

XI.2.10. BETERE COMMUNICATIE TUSSEN ADIV EN ANDERE OVERHEDEN BIJ TUCHT- OF STRAFBARE FEITEN

Het Vast Comité I beveelt aan om de communicatiekanalen en –procedures, zowel met de tuchtrechtelijke overheden van Defensie als met de politiediensten en gerechtelijke overheden, te evalueren. De ADIV moet steeds tijdig op de hoogte worden gebracht van de administratieve maatregelen, beslissingen (plaatsing onder aanhoudingsmandaat, inbeschuldigingsstelling,…) of strafrechtelijke veroordelingen met betrekking tot een personeelslid van Defensie. Dit soort communicatie moet systematische gebeuren zodat te nemen maatregelen kunnen worden onderzocht, meer bepaald met betrekking tot de veiligheidsmachtigingen.

XI.2.11. BETERE INTERNE COMMUNICATIE DOOR ADIV NAAR COMMANDO EN MOD

Het Comité beveelt aan dat de ADIV duidelijke interne richtslijnenn opstelt voor de informatiestroom naar het Commando en de minister van Defensie. Deze informatiestroom moet gestandaardiseerd en nauwkeurig zijn en de informatie bevatten die nodig is voor besluitvorming op het hoogste niveau. Dit is een voorwaarde voor een adequate controle van de werking van de organisatie en maakt deel uit van de organisatie en ontwikkeling van een intern controlesysteem.

XI.2.12. ACTIEVERE OPVOLGING VAN EXTREMISME BINNEN DEFENSIE DOOR DE ADIV

Het Vast Comité I beveelt aan dat de ADIV de nodige maatregelen treft om een actieve deelname aan de Local Task Forces (LTF) te verzekeren. Het Comité beveelt tevens aan dat er dringend interne richtlijnen en een strategie worden opgesteld over de rol van de ADIV binnen het Strategie TER (de opvolger van het Plan R)

wat betreft het opvolgen van actieve (reserve-) militairen. Meer bepaald dient te worden vastgelegd wat de precieze inbreng van de ADIV dient te zijn in enerzijds de werking van de nationale en thematische werkgroepen, en anderzijds in de LTF.

Het Vast Comité I beveelt ook aan dat de ADIV voldoende middelen inzet om tegemoet te komen aan de detectie van extremisme binnen Defensie. Dit dient het resultaat te zijn van een voorafgaande analyse van welke middelen voor welke opdracht/dreiging vereist zijn.

Tevens formuleerde het Comité de aanbeveling dat de ADIV richtslijnen opstelt met betrekking tot de raadpleging en de voeding van de GGB TF door zijn medewerkers.

XI.2.13. EVALUATIE VAN HET NATIONAAL STRATEGISCH INLICHTINGENPLAN (NSIP)

Het Vast Comité I verzoekt de ministers van Justitie en Defensie een evaluatie te verrichten van het eerste NSIP, teneinde de synergieën tussen de twee diensten in het licht van deze evaluatie te versterken.

XI.2.14. BETERE REGELS EN KENNIS INZAKE OPNAME ENTITEIT IN DE GEMEENSCHAPPELIJKE GEGEVENSBANK

Het Vast Comité I nodigt de minister van Defensie uit om samen met de bevoegde ministers de nodige initiatieven te nemen opdat de wetgevende en/of regelgevende teksten voortaan de regels zouden vaststellen voor de eventuele inschrijving van een entiteit in de Gemeenschappelijke gegevensbank 'Terrorist Fighters' (GGB TF) of de toewijzing van een bepaald niveau aan een lid door het OCAD.

Het Vast Comité I verzoekt de minister van Defensie om de bevoegde ministers te verzoeken ervoor te zorgen dat het OCAD zijn personeel op dit gebied regelmatig bijschoolt.

Het Vast Comité I beveelt aan dat het IF5-reglement wordt herzien om het in overeenstemming te brengen met de huidige structuur en uitrusting van Defensie. Met name moeten in de herziene IF5 de taken van de veiligheidsbeambte en zijn of haar prerogatieven duidelijk worden omschreven. Ook moeten de maatregelen voor en de controle op munitiedepots, met inbegrip van de rol en de taken van de ADIV, formeel worden vastgelegd.

XI.2.15. INFORMATIEUITWISSELING TUSSEN DE INLICHTINGENDIENSTEN OVER DEFENSIEPERSONEEL

Het Vast Comité I beveelt aan dat de VSSE de ADIV systematisch op de hoogte brengt wanneer het over informatie beschikt betreffende het (burgerlijk of militair) defensiepersoneel. Bovendien lijkt het noodzakelijk dat de twee diensten een samenwerkingsovereenkomst sluiten inzake het toezicht op defensiepersoneel.

XI.2.16. NALEVING HUMINT-AFSPRAKEN [387]

Het Vast Comité I beveelt de naleving aan van de door de Nationale Veiligheidsraad goedgekeurde afspraken tussen de inlichtingendiensten wat betreft de HUMINT-afspraken uit het Nationaal Strategisch Inlichtingenplan.

XI.2.17. NALEVING INFORMATIEOVERDRACHT NAAR HET OCAD

Het Vast Comité I beveelt aan, zoals voorzien in de OCAD-Wet, dat de inlichtingendiensten daadwerkelijk alle informatie die pertinent is voor de analyse en evaluatie van de dreiging stelselmatig en tijdig, binnen de wettelijk voorziene termijnen, bezorgen aan het OCAD.

XI.2.18. EEN FLEXIBEL EN PROACTIEF REKRUTERINGSBELEID VOOR DE INLICHTINGENDIENSTEN

Het Vast Comité I beveelt aan dat de mogelijkheden worden gecreëerd opdat de inlichtingendiensten een flexibel en proactief rekruteringsbeleid kunnen voeren. Dit vereist een betere samenwerking met SELOR, maar ook een versterking van het personeel dat nodig is om de in de komende jaren verwachte toevloed van burgerpersoneel in goede banen te leiden.

---

387 De aanbevelingen opgenomen in de punten XI.2.17. tot en met XI.2.31. zijn ontleend aan het toezichtonderzoek naar het opsporen en opvolgen van de radicalisering van een militair: de zaak Jürgen Conings (zie Hoofdtsuk I.9.). Deze aanbevelingen kregen een hoge prioriteit.

XI.2.19. EEN KWALITETISVOLLE DIGITALE OMGEVING

Om het personeel aan zich te binden, moet de ADIV bovendien beschikken over een digitale omgeving die in overeenstemming is met zijn verplichtingen en opdrachten. Uit het laatste verslag van het Comité over dit onderwerp blijkt dat de algemene IT-infrastructuur ontoereikend is voor een dienst van dit belang.

XI.2.20. EEN UNIFORME METHODOLOGIE INZAKE DREIGINGSEVALUATIE IN DE INLICHTINGENSECTOR

Het Vast Comité I beveelt aan, met het oog op het verbeteren van de communicatie tussen de verschillende partners in de inlichtingensector (VSSE en OCAD in het bijzonder) dat de ADIV zich zo veel als mogelijk op dezelfde lijn plaatst van de methodologieën die al zijn ontwikkeld en goedgekeurd door zijn partners, zodat dezelfde dreiging in dezelfde mate aandacht krijgt binnen de inlichtingengemeenschap.

Deze methodologie dient een actualisering van de individuele fiches in te houden, zowel voor wat betreft de te verzamelen gegevens als voor de te ondernemen acties om de dreiging te beteugelen.

Het geheel van de 'watchlist' dient het voorwerp uit te maken van een periodieke herbeoordeling, aan het eind waarvan de dreigingsniveaus worden geëvalueerd en de vastgestelde dreigingen worden gehandhaafd, naar boven of beneden worden bijgesteld, of zelfs volledig uit het informatiesysteem worden verwijderd wanneer uit de uitgevoerde analyse blijkt dat de aandacht van de ADIV niet langer (of niet) vereist is.

Het Vast Comité I beveelt tevens aan dat het beginsel van de 'watchlist' systematisch wordt toegepast voor alle bedreigingen die onder de bevoegdheid van de ADIV vallen, d.w.z. ook die welke slechts een minimaal niveau van toezicht vereisen (passief toezicht), maar niettemin toezicht vereisen. Zodra de 'watchlist' de dreigingsniveaus en de te nemen follow-up-maatregelen bevat, is er geen reden meer om twee afzonderlijke documenten te handhaven: het moet een alomvattend beeld kunnen geven van de dreiging.

XI.2.21. HET BELANG VAN DIVERSE REGLEMENTEN

Het Vast Comité I nodigt de Minister van Defensie uit om de COL 8/2014, geactualiseerd in januari 2018, bij de Minister van Justitie in herinnering te brengen en er op aan te dringen dat die systematisch wordt nageleefd.

Het Vast Comité I beveelt aan om de regels (SOP's) te harmoniseren en te centraliseren.

Het Vast Comité I beveelt aan dat de ADIV, en in het verlengde daarvan Defensie, het plan Strategie TER ter harte neemt en meer in een constructieve geest samenwerkt.

XI.2.22. TUCHTRECHTELIJK GEZAG OVER HET BURGERPERSONEEL ADIV

Het Vast Comité I beveelt andermaal aan om tegemoet te komen aan de actuele situatie dat het hoofd van de ADIV geen tuchtrechtelijk gezag heeft over het burgerpersoneel van de ADIV. Er moet absoluut een eenheid van bevel komen en geen twee parallelle commandostructuren (een civiele en een militaire), zoals nu het geval is.

XI.2.23. INZET INLICHTINGENMETHODEN

Het Vast Comité I beveelt aan om maximaal gebruik te maken van de mogelijkheden (o.a. bijzondere inlichtingenmethoden (BIM), Humint), in samenwerking met de VSSE teneinde de middelen te maximaliseren, die de wetten toelaten om de informatie te verzamelen.

XI.2.24. AANWERVING JURISTEN

Het Vast Comité I beveelt aan dat meer juristen zouden worden aangeworven die belast zijn met een juridisch-operationele functie ter ondersteuning van de collecte-medewerkers en analisten.

XI.2.25. INVESTEREN IN MANAGEMENT

Het Vast Comité I beveelt aan dat de ADIV investeert in een '*knowledge management* strategie'.

Het Vast Comité I beveelt aan om het *Steering Committee* te hervormen tot een volwaardig en daadwerkelijk directiecomité dat moet worden aangevuld met een verantwoordelijke collecte, een verantwoordelijke analyse en eventueel een jurist om de coördinatie en de synchronisatie van alle inlichtingenactiviteiten te verzekeren. Zij moet worden onttrokken aan het beheer van projecten op middellange en lange termijn en aan haar betrokkenheid bij de basislogistiek. Binnen de ADIV is

voorzien in andere entiteiten om deze taken uit te voeren, maar door personeelsgebrek worden zij niet naar behoren uitgevoerd.

XI.2.26. VERDUIDELIJKING COUNTERINTELLIGENCE BINNEN ADIV

Het Vast Comité I beveelt aan dat er binnen Defensie bijkomende inspanningen worden geleverd om de opdracht van counter*intelligence* te verduidelijken en uit te dragen naar alle geledingen van de Krijgsmacht.

XI.2.27. WERKING VEILIGHEIDSOFFICIEREN BINNEN ADIV

Het Vast Comité I beveelt aan dat de ADIV de veiligheidsofficieren (S2) meer bewust maakt van alle mogelijke veiligheidsproblemen, hen responsabiliseert en hen aanzet tot proactieve samenwerking met de eenheden en de ADIV. De ADIV dient dan ook een vertrouwensrelatie uit te bouwen met de diverse veiligheidsofficieren.

XI.2.28. VASTSTELLING RADICALISERINGSINDICATOREN DOOR ADIV

Het Vast Comité I beveelt met betrekking tot de opsporing van radicalisering aan dat de ADIV specifieke instructies geeft om duidelijke indicatoren van radicalisering vast te stellen.

XI.2.29. WEDERZIJDS ZICHT OP OPGEVOLGDE ENTITEITEN DOOR VSSE EN ADIV

Het Vast Comité I beveelt aan dat naar een informaticaoplossing (hit/no hit) moet gezocht worden zodat de inlichtingendiensten kennis kunnen nemen van elkaars op te volgen entiteiten, met alle respect voor elkaars finaliteit en het brongeheim.

XI.2.30. MIDDELEN IN DE STRIJD TEGEN EXTREMISME

Het Vast Comité I beveelt aan dat de ADIV voldoende middelen inzet om tegemoet te komen aan de detectie van extremisme binnen Defensie. Dit dient het

resultaat te zijn van een voorafgaande analyse van welke middelen voor welke opdracht/dreiging vereist zijn.

XI.2.31. ACTUALISERING BESTAANDE REGLEMENTERINGEN[388]

De richtlijnen van het Ministerieel Comité voor inlichting en veiligheid handelend over allerhande veiligheidsvoorschriften zouden moeten geactualiseerd worden (omvang veiligheidsonderzoeken, classificatieregels, bewaring geclassificeerde stukken, informatieveiligheid, taken veiligheidsofficieren). Deze richtlijnen dateren allen van het jaar 2001.

Het Vast Comité I nodigt de minister van Defensie uit om met haar bevoegde collega's de opmaak van een gemeenschappelijke richtlijn voorop te stellen om de wettelijke criteria (Wet 11 december 1998) nader te bepalen.

XI.2.32. CUMUL BINNEN DEFENSIE

Het Vast Comité I beveelt Defensie aan na te gaan of het passend is militairen toe te staan een bijkomende beroepsactiviteit uit te oefenen en of dit strookt met de waardigheid van het ambt, en zo ja, welke taken in aanmerking kunnen komen.

XI.2.33. WERKING VAN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN BINNEN DE ADIV

Het Vast Comité I beveelt aan dat de ADIV zijn personeel informeert over het bestaan van de GGB TF en hen sensibiliseert over zijn belang en zijn gebruik. Tevens moet een scenario worden opgesteld voor de eventuele opname van een lid in de GGB TF of de toekenning van een bepaald dreigingsniveau aan een lid door het OCAD.

Het Vast Comité I beveelt aan dat de inlichtingendiensten verantwoordelijken aanzetten om op systematische en dagelijkse wijze de GGB TF te consulteren en de informatie waar nodig te delen met de hiërarchische lijn tot op het hoogste niveau. De ADIV dient ook hoogdringend de finaliteit (raadplegen, voeden…) van de gemeenschappelijke gegevensbanken op te nemen in zijn werking. Overigens dient de ADIV de lijst van gebruikers van de GGB TF systematisch te actualiseren.

---

388 De aanbevelingen opgenomen in de punten XI.2.32. tot en met XI.2.36. zijn ontleend aan het toezichtonderzoek naar het opsporen en opvolgen van de radicalisering van een militair: de zaak Jürgen Conings (zie Hoofdtsuk I.9.). Deze aanbevelingen kregen een prioriteit van 'gemiddelde urgentie'.

XI.2.34. MELDING EN OPVOLGING VEILIGHEIDSINCIDENTEN BINNEN DE ADIV

Het Vast Comité I beveelt aan dat de ADIV van ieder veiligheidsincident een uitvoerig verslag opmaakt dat alle dimensies (niet alleen technisch, maar ook op het vlak van het gedrag), onderzoekt en analyseert, maar vooral wanneer één van de betrokkenen houder is van een veiligheidsmachtiging. Dit verslag moet worden bezorgd aan de bevoegde veiligheidsautoriteit, eventueel samen met een voorstel van besluit.

XI.2.35. SAMENWERKING VEILIGHEIDSBUREAUS ADIV EN VSSE

Het Vast Comité I beveelt aan dat het veiligheidsbureau van de VSSE en de Directie S van de ADIV nauwer en formeler samenwerken, middels het afsluiten van een protocolakkoord.

XI.2.36. COHERENT GEBRUIK VAN DREIGINGSNIVEAUS EN COMMUNICATIE VAN EVALUATIES DOOR HET OCAD[389]

Bij het toekennen van een dreigingsniveau (1,2,3 of 4) wordt bij de registratie in de GGB ook een categorie voor de opvolging (A, B of C) toegekend. De beide parameters staan los van elkaar. De Vaste Comités I en P bevelen aan om een grotere coherentie en harmonisatie tussen het dreigingsniveau enerzijds en de opvolgingscategorie anderzijds na te streven.

Voor wat betreft de communicatiewijze en de bestemmelingen van de dreigingsanalyses van het OCAD bestaat er een verschil naargelang het om een punctuele dreigingsevaluatie gericht tegen personen, groeperingen of gebeurtenissen gaat, dan wel of het een evaluatie van de individuele dreiging door een persoon betreft. De Vaste Comités I en P bevelen aan om op het vlak van de communicatie van de evaluatie van de dreiging door een persoon, naast de registratie in de GGB, deze dreigingsanalyse ook te communiceren naar de belanghebbende diensten die de dreigingsevaluaties tegen personen ontvangen overeenkomstig de OCAD-wet.

---

389 Zie Hoofdstuk 'I.10. De rol van het OCAD in de opvolging van de militair Jürgen Conings'. Dit onderzoek werd samen met het Vast Comité P uitgevoerd.

Ondanks het pragmatisme dat het OCAD hanteert bij de toepassing van de Omzendbrief van de minister van Binnenlandse Zaken en de minister van Justitie betreffende de informatie-uitwisseling rond en de opvolging van terrorist fighters en haatpropagandisten lijkt het de Vaste Comités I en P aangewezen om de Omzendbrief aan te passen aan de nieuwe categorieën die met het wijzigingsbesluit d.d. 20/12/2019 aan de GGB werden toegevoegd, m.n. de potentieel gewelddadige extremisten (PGE) en terrorismeveroordeelden (TV).

In de lijn met de voorgaande aanbeveling zou het zinvol kunnen zijn om bij een aanpassing van de Omzendbrief van de ministers van Binnenlandse Zaken en de Justitie betreffende de informatie-uitwisseling rond en de opvolging van terrorist fighters en haatpropagandisten de mogelijkheden te evalueren om de bestaande maatregelen voor het reduceren van de dreiging uit te breiden en verder te specifieren naar de bestaande en nieuwe categorieën.

XI.2.37. SCHRIFTELIJKE COMMUNICATIE BIJ TOEPASSING VAN ARTIKEL 19 W.I&V[390]

In artikel 19 W.I&V wordt niet gespecificeerd hoe de informatie aan de betrokken ministers e.a. moet worden meegedeeld. Het Vast Comité I is van mening dat de mededeling om redenen van rechtszekerheid schriftelijk dient te geschieden, behalve in uiterst dringende gevallen. Het doel is discussies achteraf te voorkomen en parlementaire (of zelfs juridische) controle mogelijk te maken. Het Comité beveelt aan dat het beginsel van systematische schriftelijke communicatie onverwijld wordt toegepast.

XI.2.38. OMGANG MET GECLASSIFICEERDE INFORMATIE DOOR DERDE OVERHEDEN[391]

Ontvangers van geclassificeerde informatie moeten voorzichtige omspringen met dergelijke nota's en zich bewust zijn van de schade die zij kunnen toebrengen aan de personen op wie de nota's betrekking hebben en aan de goede werking van de inlichtingen- en veiligheidsdiensten zelf.

Het Vast Comité I roept de Veiligheid van de Staat en de nationale veiligheidsoverheid op om binnen zes maanden de nodige initiatieven te nemen om de ontvangers bewust te maken van en te herinneren aan de plichten van veiligheidsofficieren.

---

390 Zie Hoofdstuk 'I.11. De opvolging van een regeringscommissaris door de VSSE'

391 *Ibid.*

XI.2.39. VEILIGHEIDSSCREENINGS VOOR VERTROUWENSFUNCTIES[392]

Het Vast Comité I is van mening dat de uitoefening van bepaalde 'openbare functies' een voorafgaande toetsing van de integriteit, loyaliteit en discretie vereist, zoals de vigerende wetgeving in sommige Europese landen voorschrijft.

Volgens het Comité zou die controle in het bijzonder moeten worden uitgevoerd voor kandidaten voor de functie van regeringscommissaris, maar ook voor andere openbare functies zoals die van aalmoezenier of andere belangrijke functies op federaal, gewestelijk en gemeenschapsniveau.

Bijgevolg vraagt het Vast Comité I aan de regering om tegen het einde van april 2022 de nodige wetgevende initiatieven te nemen, samen met de bevoegde federale ministers. Aan de minister van Defensie wordt gevraagd nader te bepalen of sleutelfuncties bij Defensie moeten worden opgenomen in deze initiatieven. In het tegenovergestelde geval wordt aan de minister gevraagd om de noodzakelijke parallelle wetgevende initiatieven te nemen om het rechtskader vast te stellen voor de controles met betrekking tot de functies die een controle vereisen bij Defensie. Tot slot zou de minister van Justitie ook het initiatief moeten nemen om de kwestie van een voorafgaande controle van sleutelfuncties op de andere bevoegdheidsniveaus op de agenda van een vergadering van het Overlegcomité te plaatsen.

XI.2.40. VERMELDING ONTVANGERS OP UITGAANDE NOTA'S[393]

Het Vast Comité I beveelt aan dat de VSSE in de nota's die zij opstelt, alle ontvangers van de nota's vermeldt en de nota's 'individualiseert' wanneer zij worden verzonden, en dit om lekken te voorkomen.

Als algemene regel beveelt het Vast Comité I aan dat de door het directiecomité gevalideerde nota's van de VSSE onverwijld worden toegezonden aan de in de nota vermelde geadresseerden.

---

392 Zie Hoofdstukken 'I.11. De opvolging van een regeringscommissaris door de VSSE' & 'I.12. Een vernieuwde aandacht voor de Moslimbroederschap'

393 Zie Hoofdstuk 'I.11. De opvolging van een regeringscommissaris door de VSSE'

XI.2.41. HET MEEDELEN VAN DE BEHOEFTEN VAN DE NATIONALE VEILIGHEIDSRAAD AAN DE INLICHTINGENDIENSTEN [394]

Het Vast Comité I verzoekt de NVR aan de inlichtingendiensten het soort en de aard te specificeren van de nota's die hij wenst te ontvangen, alsmede de termijnen voor de toezending ervan.

XI.2.42. SAMENWERKING IN HET KADER VAN DE PROBLEMATIEK VAN DE MOSLIMBROEDERS[395]

Volgens het Vast Comité I is het de taak van de ministers van Justitie en Defensie om met hun collega's van Binnenlandse Zaken de samenwerking tussen de inlichtingendiensten en hun partners (Federale Politie, OCAD enz.) te versterken en samen met de diensten te bepalen wat het geschikte samenwerkingskader is. In 2022 moet een actieplan betreffende de problematiek van de Moslimbroeders worden opgemaakt. Het moet:

- een gemeenschappelijke definitie vaststellen:
  - van het fenomeen en zijn componenten;
  - van het niveau van dreiging dat uitgaat van het fenomeen;
  - een strategie voor opvolging van het fenomeen (met een eventuele taakverdeling overeenkomstig het rechtskader)[396], rekening houdend met de middelen waarover de diensten beschikken;
  - een strategie van bewustmaking van de overheden en administraties (met een bevoegdheidsverdeling overeenkomstig het rechtskader);
- een bijgewerkte lijst opstellen van de verenigingen die verbonden zijn met de Moslimbroeders, alsook van de leden en de sympathisanten van de beweging;
- verzekeren dat er voldoende manschappen zijn om de passende opvolging te garanderen.

XI.2.43. ANALYSE VAN DE MIDDELEN VAN ADIV M.B.T. DE PROBLEMATIEK VAN DE MOSLIMBROEDERS

Het Vast Comité I beveelt de ADIV aan om in 2022 een analyse te maken om te bepalen of de middelen die ze inzet bij de opvolging van de Moslimbroeders voldoende zijn ten opzichte van de ingeschatte waarschijnlijkheid van het risico van

---

394 *Ibid.*

395 De aanbevelingen opgenomen in de punten XI.2.43. tot en met XI.2.46. zijn ontleend aan het toezichtonderzoek 'Een vernieuwde aandacht voor de Moslimbroederschap' (Hoofdstuk I.12.)

396 Deze oefening werd al gemaakt voor de ADIV en de VSSE, en werd opgenomen in de strategische plannen (zie *supra*).

poging tot beïnvloeding door de Moslimbroeders bij Defensie, en dit rekening houdend met de prioriteit die de dienst toekent aan de opvolging van het fenomeen. Als dat niet het geval blijkt te zijn, is het de taak van de ADIV om aan de minister van Defensie te vragen een passend aanwervingsplan op te stellen.

XI.2.44. ALGEMENE BEWUSTMAKING M.B.T. DE PROBLEMATIEK VAN DE MOSLIMBROEDERS

Het Vast Comité I looft de ambitie van de VSSE om een brochure over de Moslimbroeders samen te stellen en die op grote schaal te verspreiden met het oog op bewustmaking; het Comité beveelt de VSSE aan om de brochure ten laatste eind 2022 te verspreiden.

XI.2.45. BEWUSTMAKING VEILIGHEIDSOFFICIEREN DEFENSIE M.B.T. DE PROBLEMATIEK VAN DE MOSLIMBROEDERS

Het Vast Comité I vraagt aan de ADIV ook om interne briefings te organiseren voor de aangewezen veiligheidsofficieren met als doel hen bewust te maken van de problematiek en hun vermogen te vergroten om een concrete dreiging voor Defensie op het spoor te komen.

XI.2.46. ICT IN HET INLICHTINGENPROCES BIJ DE DIRECTIE CYBER VAN DE ADIV[397]

Het Vast Comité I beveelt aan om op ICT-vlak met de volgende punten rekening te houden, zodat een optimale doeltreffendheid van de dienstverlening kan worden gewaarborgd om de strategische doelstellingen te halen:

- De nodige verbintenissen aangaan in verband met het personeelsplan dat aan het Vast Comité I werd voorgesteld;
- Bijkomende maatregelen treffen (*no-break*, bijkomende UPS, monitoring) om de problemen met betrekking tot de elektrische infrastructuur in de wijk op te vangen;
- De *hardware resources* vergroten indien dit nodig zou blijken om een betere dienstverlening aan de gebruikers te waarborgen;
- Voldoende aandacht schenken aan de contracten met externe bedrijven, bijv. door de mogelijkheid van '*on premises*'-software te overwegen (op eigen infrastructuur).

397 Zie Hoofdstuk 'I.13. Informatie- en communicatietechnologie in het inlichtingenproces bij de Directie Cyber van de ADIV en bij de VSSE'

XI.3. AANBEVELINGEN IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

XI.3.1. MELDING DOOR DE ADIV VAN DE OPVOLGING VAN POLITIEKE MANDATARISSEN[398]

Het Vast Comité I beveelt de ADIV aan om haar driemaandelijks een overzicht te bezorgen van alle documenten waarin politieke mandatarissen worden vermeld; desgevallend met een '*blanco hit*' zo geen dergelijke vermeldingen werden gemaakt.

398 Zie Hoofdstuk 'I.8. De opvolging van politieke mandatarissen'

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 2021 TOT 31 DECEMBER 2021)

Wet van 27 juni 2021 houdende de derde aanpassing van de Algemene uitgavenbegroting voor het begrotingsjaar 2021, *BS* 9 juli 2021

Wet van 14 augustus 2021 tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, alsook tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van het Vast Comité I en van het Vast Comité P, *BS* 8 december 2021

Wet van 23 december 2021 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2022, *BS* 29 december 2021

K.B. 30 september 2021 tot vaststelling van de begunstigden van de acties die door de Federale Overheidsdienst Beleid en Ondersteuning worden gevoerd in het kader van zijn opdracht om culturele, promotie-, amusements-, opleidings- en sportinitiatieven te ontwikkelen, *BS* 4 november 2021

Gemeenschappelijke richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de bepaling van de nadere regels voor de mededeling van persoonsgegevens en informatie die door de politiediensten worden verwerkt in het raam van hun opdrachten van bestuurlijke en gerechtelijke politie, bedoeld in de artikelen 14 en 15 van de wet op het politieambt, door de politiediensten en tot de rechtstreekse toegang en de rechtstreekse bevraging van de ANG, *BS* 2 februari 2021

Oproep tot kandidaten voor de bestuurlijke Commissie door de inlichtingen- en veiligheidsdiensten belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, *BS* 12 februari 2021

Verlenging bij ministerieel besluit van 3 februari 2021 voor het mandaat van stafdirecteur van de Veiligheid van de Staat van de heer Hugues Brulin voor een periode van 5 jaar, vanaf 1 september 2020, *BS* 16 februari 2021

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 vereniging zonder winstoogmerk Syndicaat van de Belgische Politie, "Sypol.be", heeft de nietigverklaring gevorderd van het koninklijk besluit van 24 september 2020 '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* 16 februari 2021

Beëindiging van de aanstelling voor de Directeur van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 24 februari 2021

Aanstelling ad interim Directeur van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 24 februari 2021

Vast Comité van Toezicht op de Inlichtingen- en Veiligheidsdiensten, vacature voor een Franstalige attaché (m/v/x) van universitair niveau, *BS* 5 maart 2021

Aanwerving bij wijze van detachering en samenstelling van een wervingsreserve van Franstalige commissarissen-auditors (m/v/x) met een bijzondere kennis van gerechtelijk onderzoek en informatiebeheer (Intelligence-led Policing) voor de Dienst Enquêtes van het Vast Comité I, *BS* 18 maart 2021

Oproep tot kandidaten voor de bestuurlijke Commissie door de inlichtingen- en veiligheidsdiensten belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, *BS* 2 april 2021

Benoeming van de griffier van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *BS* 19 juli 2021

Grondwettelijk Hof: uittreksel uit arrest nr. 64/2021 van 22 april 2021, rolnummer 7416, in zake: de prejudiciële vraag betreffende artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, gesteld door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *BS* 20 september 2021

Aanwerving bij wijze van detachering en samenstelling van een wervingsreserve van Franstalige commissarissen-auditors met een bijzondere kennis van ICT/Data (m/v/x) voor de Dienst Enquêtes van het Vast Comité I, *BS* 1 oktober 2021

Grondwettelijk Hof: uittreksel uit arrest nr. 107/2021 van 15 juli 2021, rolnummer 7261, in zake: het beroep tot vernietiging van de wet van 23 maart 2019 'betreffende de organisatie van de penitentiaire diensten en van het statuut van het penitentiair personeel', ingesteld door Michel Jacobs, *BS* 6 oktober 2021

Oproep tot kandidaten voor het mandaat van tweede Nederlandstalig plaatsvervangend lid van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *BS* 25 november 2021

Aanwerving bij wijze van detachering en samenstelling van een wervingsreserve van Franstalige Commissarissen-auditors met een bijzondere kennis van ICT/Data (m/v/x) voor de Dienst Enquêtes van het Vast Comité I, *BS* 23 december 2021

Vergelijkende selecties, voorafgaande proeven in de vergelijkende selecties, resultaten van de vergelijkende selecties van :

- Nederlandstalige HR Business Partners voor de militaire inlichtingendienst (m/v/x) (niveau A1) voor het Ministerie van Defensie, selectienummer: ANG21132, *BS* 17 mei 2021
- Franstalige HR Business Partners voor de militaire inlichtingendienst (m/v/x) (niveau A1) voor het Ministerie van Defensie, selectienummer: ANG21132, *BS* 17 mei 2021
- Franstalige Data Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21100, *BS* 1 juni 2021
- Nederlandstalige Data Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21130, *BS* 1 juni 2021
- Franstalige Technical Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21102, *BS* 1 juni 2021
- Nederlandstalige Technical Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21134, *BS* 1 juni 2021
- Franstalige Windows/Linux systeembeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21119, *BS* 13 juli 2021
- Nederlandstalige Netwerkbeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21153, *BS* 13 juli 2021

- Nederlandstalige Imagery Intelligence medewerkers voor de Algemene Dienst Inlichting en Veiligheid (ADIV) (m/v/x) (niveau B) voor het Ministerie van Defensie, selectienummer: ANG21216, *BS* 19 juli 2021
- Nederlandstalige Documentalisten Inlichtingen en Veiligheid (m/v/x) (niveau B) voor het Ministerie van Defensie, selectienummer: ANG21218, *BS* 26 juli 2021
- Franstalige Specialisten Query & Reporting (m/v/x) (niveau A1) voor Ministerie van Defensie, selectienummer: AFG21134, *BS* 6 augustus 2021
- Franstalige Attachés veiligheidsmachtiging analisten (niveau A1) voor het Ministerie van Defensie, selectienummer: AFG21135, *BS* 6 augustus 2021
- Franstalige Cyberdefensie Onderzoeker (m/v/x) (niveau A2) voor het Ministerie van Defensie, selectienummer: AFG21156, *BS* 16 augustus 2021
- Franstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B) van de Veiligheid van de Staat, selectienummer: ANG21149, *BS* 29 september 2021
- Nederlandstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B) van de Veiligheid van de Staat, selectienummer: ANG21212, *BS* 29 september 2021
- Nederlandstalige Finance Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21303, *BS* 30 september 2021
- Franstalige Technical Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21102, *BS 2*6 oktober 2021
- Franstalige Windows/Linux systeembeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21119, *BS 2*6 oktober 2021
- Nederlandstalige Technical Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21134, *M.B.* 26 oktober 2021
- Nederlandstalige Netwerkbeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21153, *BS 2*6 oktober 2021
- Franstalige Attachés veiligheidsmachtiging analisten (m/v/x) (niveau A1) voor het Ministerie van Defensie, selectienummer AFG21135, *BS* 17 november 2021
- Nederlandstalige voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat, selectienummers: BNG21341 - BNG21342, *BS* 8 december 2021
- Franstalige voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat, selectienummers: BFG21188 - BFG21189, *BS* 8 december 2021
- van Nederlandstalige Data Officers (m/v/x) (niveau B) voor Veiligheid van de Staat, selectienummer: ANG21130, *BS* 16 december 2021
- Franstalige Data Officers (m/v/x) (niveau B) voor Veiligheid van de Staat, selectienummer: AFG21100, *BS* 16 december 2021
- Nederlandstalige Finance Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21303, *BS* 27 december 2021
- Franstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B) van de Veiligheid van de Staat, selectienummer: AFG21149, *BS* 30 december 2021
- Nederlandstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21212, *BS* 30 december 2021

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 2021 TOT 31 DECEMBER 2021)

Senaat

Informatieverslag betreffende de noodzakelijke samenwerking tussen de federale overheid en de Gemeenschappen inzake de bestrijding van fake news van S. D'Hose, E. Ampe, R. Daems, W.-F. Schiltz, C. Van Cauter, F. Ahallouch, L. Gahouchi, G.-L. Bouchez, Ph. Dodrimont, V. Durenne, S. Laruelle, A. Miesen, G. Van Goidsenhoven, J.-P. Wahl, K. Brouwers, B. Anciaux, K. De Loor, A. Lambrecht, K. Segers, A. Antoine, A.-C. Goffinet, F. Ben Chikha, S. Bex, R. Demeuse, S. Hoessen, F. Masai, J. Pitseys, H. Ryckmans, Ch. Steenwegen en F. Tahar, Stuk 7-110, *Hand*. Senaat 2021-22, 17 november 2021, nr. 24, 5

Grondwettelijk Hof: het arrest nr. 158/2021, uitgesproken op 18 november 2021, inzake 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 Patrick Van Assche en anderen (rolnummer 6672), *Hand*. Senaat 2021-22, 17 december 2021, nr. 25, 43

Kamer van volksvertegenwoordigers

Commissies, adviescomités en afvaardigingen naar de internationale vergaderingen, Parl. St. Kamer 2020-21, nr. 55K0008/008

Moties ingediend in openbare commissievergadering (artikelen 133 tot 141 van het Reglement van de Kamer) op 17 maart 2021 tot besluit van de interpellatie van N. Boukili tot de eerste minister over 'Smals en de openbare aanbestedingen betreffende de digitalisering van de openbare diensten', Parl. St. Kamer 2020-21, nr. 55K105/001

Voorstel van resolutie teneinde te voorzien in evenwaardige middelen voor sites met dreigingsniveau 3 in het afbouwplan van Operation Vigilant Guardian (OVG), Parl. St. Kamer 2020-21, nr. 55K1413/002

Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, met het oog op het invoeren van een actieve kennisgevingsplicht met betrekking tot bepaalde specifieke methoden voor het verzamelen van gegevens, Parl. St. Kamer 2020-21, nr. 55K1763/001

Vast Comité van Toezicht op de inlichtingen en veiligheidsdiensten – benoeming van de eerste plaatsvervanger van een Franstalig lid – ingediende kandidaturen, *Hand*. Kamer 2020-21, 28 januari 2021, CRIV55PLEN085, 38

Voorstel van resolutie betreffende cyberdefensie en de attributie van statelijke cyberaanvallen, Parl. St. Kamer 2020-21, nr. 55K1788/001

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 - opvolgingsaudit van het Rekenhof -implementatie van de aanbevelingen, Parl. St. Kamer 2020-21, nr. 55K1924/001

Ordemotie ingediend door P. De Roover, P. Buysrogge en J. Donné: 'de Kamer van Volksvertegenwoordigers: - gelet dat er bewust informatie uit een gedachtewisseling over een toekomstig toezichtonderzoek werd gelekt naar de media, dit door leden van de parlementaire begeleidingscommissie van het Comité P en I; - gelet dat de begeleidingscommissie onder art. 67 van het Kamerreglement valt en de geheimhoudingsplicht geldt met betrekking tot alle informatie die ter zitting verkregen wordt; verzoekt de Kamervoorzitster om een onderzoek te voeren naar de overtreders, om vervolgens onder art. 67 van het Kamerreglement de gepaste sancties te treffen', *Hand*. Kamer 2020-21, 27 mei 2021, CRIV55PLEN106, 26

Mededeling over de inachtneming van artikel 67 van het Reglement, *Hand*. Kamer 2020-21, 27 mei 2021, CRIV55PLEN106, 27

Wetsontwerp houdende de eerste aanpassing van de middelenbegroting voor het begrotingsjaar 2021 (1920/1-8) - wetsontwerp houdende de derde aanpassing van de algemene uitgavenbegroting voor het begrotingsjaar 2021 (1921/1-27) - aanpassing van de begrotingen van ontvangsten en uitgaven voor het begrotingsjaar 2021, algemene toelichting (1919/1), *Hand*. Kamer 2020-21, 24 juni 2021, CRIV55PLEN113, 1

Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, alsook tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van het Vast Comité I en van het Vast Comité P (2064/1-3), *Hand*. Kamer 2020-21, 8 juli 2021, CRIV55PLEN117, 51

Motie ingediend door de heer P. De Roover over: 'vorderen van de aanwezigheid van de premier – art. 100 GW en art. 50 Reglement aangezien de premier maandag in de commissie Gezondheid een verklaring heeft afgelegd over het onderzoek van de Staatsveiligheid in hoofde van de voormalige regeringscommissaris voor het Instituut voor de gelijkheid van mannen en vrouwen en de communicatie van het onderzoek aan het kabinet van de minister van Justitie, *Hand*. Kamer 2020-21, 14 juli 2021, CRIV55PLEN119, 2

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten - vervanging van de griffier - oproep tot kandidaten, *Hand*. Kamer 2020-21, 15 juli 2021, CRIV55PLEN122, 44

Voorstel tot verwerping door de commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken van het voorstel van resolutie teneinde te voorzien in evenwaardige middelen voor sites met dreigingsniveau 3 in het afbouwplan van Operation Vigilant Guardian (OVG) (1413/1-2), *Hand*. Kamer 2020-21, 15 juli 2021, CRIV55PLEN122, 62

Voorstel van resolutie betreffende cyberdefensie en de attributie van statelijke cyberaanvallen, Parl. St. Kamer 2020-21, nr. 55K1788/001

Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, alsook tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van het Vast Comité I en van het Vast Comité P, Parl. St. Kamer 2020-21, nrs. 55K2064/001 tot 55K2064/004

Wetsontwerp 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, Parl. St. Kamer 2020-21, nrs. 55K2074/001 tot 55K2074/003

Wetsontwerp houdende instemming met de overeenkomst tussen het Koninkrijk België en de Republiek Finland inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Helsinki op 20 juli 2016, Parl. St. Kamer 2020-21, nr. 55K2075/001

Wetsontwerp houdende instemming met de overeenkomst tussen het Koninkrijk België en de Republiek Cyprus inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 20 juli 2015, Parl. St. Kamer 2020-21, nr. 55K2085/001

Wetsontwerp 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, Parl. St. Kamer 2020-21, nr. 55K2121/001

Actualisatie van de strategische visie – gedachtewisseling met de minister van Defensie, Parl. St. Kamer 2020-21, nr. 55K2150/001

Voorstel van resolutie betreffende het beschermen van onze nationale veiligheid en strategische onafhankelijkheid tegenover buitenlandse cyberaanvallen door het opstellen van een lijst van hoogrisicoleveranciers, Parl. St. Kamer 2020-21, nr. 55K2167/001

Cyberaanvallen op het IT-systeem van de staat en de overheidsdiensten, Parl. St. Kamer 2020-21, nr. 55K2169/001

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – benoeming van de griffier – ingediende kandidaturen, *Hand.* Kamer 2021-22, 23 september 2021, CRIV55PLEN125, 27

Zaak Jürgen Conings, Parl. St. Kamer 2020-21, nr. 55K2206/001

Activiteitenverslag 2020 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Parl. St. Kamer 2021-22, nr. 55K2209/001

Voorstel van resolutie over de onafhankelijkheid en de werking van de Gegevensbeschermingsautoriteit, Parl. St. Kamer 2021-22, nr. 55K2246/001

Wetsontwerp houdende omzetting van het Europees wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, Parl. St. Kamer 2021-22, nrs. 55K2256/001, 55K2256/007 en 55K2256/008

Wetsontwerp houdende de wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie, Parl. St. Kamer 2021-22, nrs. 55K2257/001 tot 55K2257/004

Onthullingen in de pers met betrekking tot de rol van de banken bij witwaspraktijken (FINCEN FILES), Parl. St. Kamer 2021-22, nr. 55K2261/001

Wetsontwerp houdende de Middelenbegroting voor het begrotingsjaar 2022, Parl. St. Kamer 2021-22, nr. 55K2291/001

Wetsontwerp houdende de Algemene uitgavenbegroting voor het begrotingsjaar 2022, Parl. St. Kamer 2021-22, nrs. 55K2292/001 en 55K2292/006

Verantwoording van de algemene uitgavenbegroting voor het begrotingsjaar 2022, Parl. St. Kamer 2021-22, nrs. 55K2293/006 en 55K2293/007

Beleidsnota, Parl. St. Kamer 2021-22, nrs. 55K2294/002, 55K2294/008, 55K2294/014, 55K2294/016, 55K2294/017, 55K2294/018 en 55K2294/022

Wetsontwerp tot wijziging van diverse bepalingen betreffende de overgang binnen dezelfde personeelscategorie of de opname in een andere hoedanigheid of personeelscategorie van de beroepsmilitair of van de militair met een loopbaan van beperkte duur, Parl. St. Kamer 2021-22, nr. 55K2302/001

Comité I – ontslag van het tweede plaatsvervangend lid van het Nederlandstalig lid, *Hand.* Kamer 2021-22, 10 november 2021, CRIV55PLEN139, 68

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 2020 - begrotingsaanpassingen van het begrotingsjaar 2021- begrotingsvoorstellen voor het begrotingsjaar 2022,

Parl. St. Kamer 2021-22, nrs. 55K2368/001 tot 55K2368/003, *Hand.* Kamer 2021-22, 22 december 2021, CRIV55PLEN152, 27 en *Hand.* Kamer 2021-22, 22 december 2021, CRIV55PLEN154, 17

Wetsvoorstel tot wijziging van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, teneinde de aanbieders van essentiële diensten in de publieke sector die afhankelijk zijn van netwerk- en informatiesystemen te onderwerpen aan bepaalde eisen inzake beveiliging en meldingen, Parl. St. Kamer 2021-22, nr. 55K2401/001.

BIJLAGE C
OVERZICHT VAN INTERPELLATIES, VRAGEN OM UITLEG EN MONDELINGE EN SCHRIFTELIJKE VRAGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2021 TOT 31 DECEMBER 2021)

Senaat

Schriftelijke vraag van G. D'haeseleer aan de minister van Justitie over de 'personen veroordeeld voor terrorisme - aantal - redenen - nationaliteit' (Senaat 2020-21, 3 maart 2021, Vr. nr. 7-1107)

Schriftelijke vraag van T. Ongena aan de minister van Justitie over 'Turkije - salafisme - buitenlandse staatsinmenging - cijfers en tendensen' (Senaat 2020-21, 5 maart 2021, Vr. nr. 7-1140)

Schriftelijke vraag van T. Ongena aan de minister van Binnenlandse Zaken over 'Turkije - salafisme - buitenlandse staatsinmenging - cijfers en tendensen' (Senaat 2020-21, 5 maart 2021, Vr. nr. 7-1141)

Schriftelijke vraag van R. Daems aan de minister van Justitie over 'sociale media - online privacy - encryptie - Staatsveiligheid - cijfers en tendensen - mogelijke maatregelen' (Senaat 2020-21, 31 maart 2021, Vr. nr. 7-1154)

Schriftelijke vraag van A. Frédéric aan de minister van Justitie over 'sekten - nieuwe praktijken - bestrijding - evolutie van de wetgeving - menselijke, financiële en institutionele middelen - versterking - Coronacrisis - gevolgen - evaluatie' (Senaat 2020-21, 28 april 2021, Vr. nr. 7-1219)

Schriftelijke vraag van R. Daems aan de minister van Justitie over 'ecologie - klimaat - vermindering van de uitstoot - doelstellingen - nakoming van de beloften – 'green spying' - monitoring door en van derde landen - dienst Veiligheid van de Staat - deelneming' (Senaat 2020-21, 3 mei 2021, Vr. nr. 7-1227)

Schriftelijke vraag van T. Ongena aan de minister van Justitie over 'Turkije - Gülen-beweging - haatmisdrijven in België - politiebescherming - incidenten - cijfers en tendensen – Turkse gemeenschap - bescherming - maatregelen' (Senaat 2020-21, 3 mei 2021, Vr. nr. 7-1229)

Schriftelijke vraag van T. Ongena aan de minister van Binnenlandse Zaken over 'extreemrechts - bewakings- en beveiligingsfirma's - infiltratie - cijfers en tendensen' (Senaat 2020-21, 21 mei 2021, Vr. nr. 7-1248)

Schriftelijke vraag van T. Ongena aan de minister van Justitie over 'extreemrechts - risico op aanslagen - overleg - geweld – Corona - chatsites (Covid-19)' (Senaat 2020-21, 21 mei 2021, Vr. nr. 7-1249)

Schriftelijke vraag van T. Ongena aan de minister van Binnenlandse Zaken over de 'cyberaanvallen - cybersecurity - cijfers en tendensen - daders - statelijke actoren - privacy - bescherming - maatregelen' (Senaat 2020-21, 22 juli 2021, Vr. nr. 7-1311)

Schriftelijke vraag van A. Miesen aan de minister van Defensie over de 'Militärdienste - Reform der Nachrichtendienste - Extremismusbekämpfung Militaire diensten - hervorming van de inlichtingendiensten - extremismebestrijding' (Senaat 2020-21, 24 augustus 2021, Vr. nr. 7-1322)

Schriftelijke vraag van E. Ampe aan de minister van Justitie over 'smartphones - statelijke actoren - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1385)

Schriftelijke vraag van E. Ampe aan de minister van Binnenlandse Zaken over 'smartphones - statelijke actoren - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7- 1386)

Schriftelijke vraag van E. Ampe aan de minister van Justitie over 'smartphones - stalkerware - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1387)

Schriftelijke vraag van E. Ampe aan de minister van Binnenlandse Zaken over 'smartphones - stalkerware - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1388)

Schriftelijke vraag van R. Daems aan de minister van Justitie over 'cryptografie - quantumcomputers - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1391)

Schriftelijke vraag van R. Daems aan de minister van Binnenlandse Zaken over 'cryptografie - quantumcomputers - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1392)

Schriftelijke vraag van T. Ongena aan de minister van Defensie over de 'drones - politie - spionage - buitenlandse actoren - privacy - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1395)

Schriftelijke vraag van T. Ongena aan de minister van Binnenlandse Zaken over de 'drones - politie - spionage - buitenlandse actoren - privacy - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1396)

Kamer van volksvertegenwoordigers

Vraag van S. Moutquin aan de Staatssecretaris voor Asiel en Migratie over 'de doorstart van de Grote Moskee te Brussel' (*Hand.* Kamer 2020-21, 6 januari 2021, CRIV55COM322, 16, Vr. nr. 11488C)

Samengevoegde interpellatie en vragen van D. Van Langenhove, K. Metsu en Ph. Pivin aan de minister van Justitie over 'het negatieve advies van Justitie over de doorstart van de Grote Moskee te Brussel' (*Hand.* Kamer 2020-21, 6 januari 2021, CRIV55COM324, 1, Vrs. nrs. 58I, 11916C en 12037C)

Vraag van Th. Francken aan de minister van Justitie over 'het subsidiebesluit voor de Moslimexecutieve' (*Hand.* Kamer 2020-21, 6 januari 2021, CRIV55COM324, 36, Vr. nr. 11948C)

Vraag van D. Safai aan de Staatssecretaris voor Asiel en Migratie over de 'opvolging en screening van geradicaliseerde illegalen en geradicaliseerde erkende vluchtelingen in België' (*Vr. en Ant*. Kamer 2020-21, 12 januari 2021, QRVA34, 151, Vr. nr. 59)

Vraag van E. Burton aan de minister van Binnenlandse Zaken over de 'aanhouding van een geradicaliseerde vóór het politiebureau Brussel Hoofdstad Elsene' (*Vr. en Ant*. Kamer 2020-21, 12 januari 2021, QRVA34, 394, Vr. nr. 110)

Vraag van T. Vandenput aan de minister van Binnenlandse Zaken over de 'update OCAD-databank' (*Vr. en Ant*. Kamer 2020-21, 12 januari 2021, QRVA34, 408, Vr. nr. 119)

Samengevoegde vraag en interpellatie van S. De Wit en M. Dillen aan de minister van Justitie over 'de zwaargewonde cipier in de gevangenis van Gent' (*Hand.* Kamer 2020-21, 13 januari 2021, CRIV55COM334, 9, Vr. nrs. 12064C en 75I)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'de aanpak van het gewelddadige extremisme' (*Hand.* Kamer 2020-21, 13 januari 2021, CRIV55COM336, 49, Vr. nr. 11874C)

Vraag van E. Samyn aan de minister van Buitenlandse Zaken over het 'gevaar voor nieuwe terreurcampagnes in Europa door Islamitische Staat - VN-rapport' (*Vr. en Ant.* Kamer 2020-21, 18 januari 2021, QRVA35, 91, Vr. nr. 117)

Vraag van J. Pillen aan de minister van Defensie over 'het dragen van het uniform door militairen' (*Vr. en Ant.* Kamer 2020-21, 18 januari 2021, QRVA35, 297, Vr. nr. 83)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over 'aanhoudingen voor bedreiging van publieke figuren' (*Vr. en Ant.* Kamer 2020-21, 18 januari 2021, QRVA35, 405, Vr. nr. 171)

Actualiteitsdebat en toegevoegde vragen van B. Segers, H. Rigot, S. Moutquin, T. Vandenput en G. Daems aan de Staatssecretaris voor Asiel en Migratie over 'de zaak-Kucam' (*Hand.* Kamer 2020-21, 19 januari 2021, CRIV55COM337, 1, Vr. nrs. 12673C, 12674C, 12721C, 12723C, 12735C en 12756C)

Vraag van Th. Francken aan de Staatssecretaris voor Asiel en Migratie over 'het terugsturen van extremisten' (*Hand.* Kamer 2020-21, 19 januari 2021, CRIV55COM337, 18, Vr. nr. 12073C)

Vraag van K. Jadin aan de minister van Justitie over 'extreemrechts in België' (*Hand.* Kamer 2020-21, 21 januari 2021, CRIV55PLEN084, 42, Vr. nr. 1286P)

Vraag van J. Pillen aan de minister van Defensie over 'trespassing militaire domeinen' (*Vr. en Ant.* Kamer 2020-21, 27 januari 2021, QRVA36, 349, Vr. nr. 80)

Vraag van A. Ponthier aan de minister van Defensie over 'telefoonfraude vanuit Syrië' (*Vr. en Ant.* Kamer 2020-21, 27 januari 2021, QRVA36, 352, Vr. nr. 92)

Vraag van J. Pillen aan de minister van Defensie over 'verdachte telefoons' (*Vr. en Ant.* Kamer 2020-21, 27 januari 2021, QRVA36, 356, Vr. nr. 98)

Samengevoegde vragen van B. Moyaers, P. Pivin, S. Matheï en K. Van Vaerenbergh aan de minister van Justitie over 'de oproepen op sociale media tot rellen in België' (*Hand.* Kamer 2020-21, 28 januari 2021, CRIV55PLEN085, 2, Vr. nrs. 1303P, 1311P, 1312P en 1315P)

Vraag van M. Freilich aan de minister van Ambtenarenzaken over 'de intimidatiecampagne van Huawei tegen de Belgische regering' (*Hand.* Kamer 2020-21, 24 februari 2021, CRIV55COM387, 6, Vr. nr. 12479C)

Samengevoegde vragen van Th. Francken, D. Ducarme en G. Dallemagne aan de minister van Justitie over 'het CCIF in België' (*Hand.* Kamer 2020-21, 24 februari 2021, CRIV55COM389, 17, Vr. nrs. 14172C, 14331C en 14455C)

Vraag van L. Dierick aan de minister van Justitie over 'de betalingstermijnen bij de FOD Justitie' (*Vr. en Ant.* Kamer 2020-21, 4 maart 2021, QRVA41, 167, Vr. nr. 289)

Vraag van J.-M. Delizée aan de minister van Justitie over de 'declassificering van het zogenaamde Afrika-archief' (*Vr. en Ant.* Kamer 2020-21, 4 maart 2021, QRVA41, 178, Vr. nr. 369)

Actualiteitsdebat en toegevoegde vragen van H. Rigot, B. Segers, P. De Roover, S. Moutquin, G. Daems en E. Platteau aan de Staatssecretaris voor Asiel en Migratie over 'de humanitaire visa' (*Hand.* Kamer 2020-21, 9 maart 2021, CRIV55COM397, 1, Vr. nrs. 14898C, 14920C, 15041C, 15045C, 15067C en 15086C)

Actualiteitsdebat toegevoegde vragen van Th. Francken, J. Pillen, A. Ponthier, H. Bayet, G. Defossé en K. Verduyckt aan de minister van Defensie over 'de verbetering van de voorwaarden van militairen' (*Hand.* Kamer 2020-21, 10 maart 2021, CRIV55COM402, 1, Vr. nrs. 12466C, 13889C, 14028C, 14251C, 14265C, 15097C, 15109C en 15144C)

Vraag van E. Van Hoof aan de minister van Buitenlandse Zaken over een 'Iraanse diplomaat' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 115, Vr. nr. 60)

Vraag van W. Vermeersch aan de minister van Financiën over de 'douane - groeiende bezorgdheid om Chinese scanners' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 205, Vr. nr. 230)

Vraag van M. Freilich aan de minister van Financiën over de 'Nuctech - Chinese scanners' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 208, Vr. nr. 231)

Vraag van K. Metsu aan de minister van Justitie over de 'huiszoekingen in onderzoek naar financiering terreurgroepen' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 288, Vr. nr. 368)

Vraag van A. Ponthier aan de minister van Defensie over de 'samenwerking tussen Belgische universiteiten en de Seven Sons of National Defence in China' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 304, Vr. nr. 124)

Samengevoegde vragen van B. Segers, F. Demon en K. Gabriëls aan de minister van Justitie over 'Operatie Sky' (*Hand.* Kamer 2020-21, 11 maart 2021, CRIV55PLEN091, 24, Vr. nrs. 1428P, 1431P en 1430P)

Samengevoegde vragen van K. Aouasti, N. Gilson, N. Boukili, G. Dallemagne en G. Vanden Burre aan de minister van Digitalisering over 'de eerbiediging van de privacy en het project 'Putting data at the center'' (*Hand.* Kamer 2020-21, 11 maart 2021, CRIV55PLEN091, 35, Vr. nrs. 1427P, 1435P, 1438P, 1445P en 1449P)

Vraag van S. Van Hecke aan de minister van Justitie over 'de opvolging van sektarische organisaties in het kader van de coronacrisis' (*Vr. en Ant.* Kamer 2020-21, 17 maart 2021, QRVA43, 218, Vr. nr. 381)

Vraag van S. Goethals aan de minister van Binnenlandse Zaken over 'de organen onder uw bevoegdheid' (*Vr. en Ant.* Kamer 2020-21, 17 maart 2021, QRVA43, 269, Vr. nr. 313)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'beschermende maatregelen voor leerkrachten – dreiging van radicalisme en terrorisme' (*Vr. en Ant.* Kamer 2020-21, 17 maart 2021, QRVA43, 279, Vr. nr. 318)

Interpellatie van N. Boukili aan de eerste minister over 'Smals en de openbare aanbestedingen betreffende de digitalisering van de openbare diensten' (*Hand.* Kamer 2020-21, 17 maart 2021, CRIV55COM411, 31, Vr. nr. 105I)

Vraag van K. Gabriëls aan de minister van Justitie over 'de digitalisering van de Staatsveiligheid' (*Hand.* Kamer 2020-21, 17 maart 2021, CRIV55COM415, 36, Vr. nr. 15422C)

Vraag van S. Cogolati aan de minister van Justitie over 'de bedreiging en intimidatie van opposanten in België door de Turkse regering' (*Hand.* Kamer 2020-21, 17 maart 2021, CRIV55COM415, 42, Vr. nr. 15442C)

Samengevoegde vragen van B. Pas en K. Metsu aan de eerste minister over 'de groeiende terreurdreiging in Europa' (*Hand.* Kamer 2020-21, 18 maart 2021, CRIV55PLEN093, 33, Vr. nrs. 1462P en 1471P)

Toegevoegde vragen en interpellaties van Ph. Pivin, M. Dillen, N. Boukili, K. Van Vaerenbergh, K. Geens en G. Dallemagne aan de minister van Justitie over 'de begeleiding van en schadevergoeding voor de slachtoffers van terreuraanslagen' (*Hand.* Kamer 2020-21, 19 maart 2021, CRIV55COM418, 1, Vr. nr. 15257C, 110I, 111I, 15426C, 15448C, 15490C, 15507C, 15511C, 15519C en 15520C)

Opvolging van de aanbevelingen van de parlementaire onderzoekscommissie "Terroristische aanslagen", gedachtewisseling en toegevoegde vragen van S. Rohonyi aan de minister van Justitie over 'een fonds voor de vergoeding van de slachtoffers van terreuraanslagen' (*Hand.* Kamer 2020-21, 23 maart 2021, CRIV55COM422, 1, Vr. nrs. 15751C, 15752C, 15754C, 15755C en 15760C)

Vraag van Th. Francken aan de Staatssecretaris voor Asiel en Migratie over 'de repatriëring van moslimextremisten en Syriestrijders naar hun thuisland' (*Hand.* Kamer 2020-21, 26 maart 2021, CRIV55COM425, 10, Vr. nr. 15509C)

Samengevoegde vragen van Y. Van Camp, F. Demon, E. Platteau en H. Rigot aan de Staatssecretaris voor Asiel en Migratie over 'outreachteams bij transmigranten' (*Hand.* Kamer 2020-21, 26 maart 2021, CRIV55COM425, 12, Vr. nrs. 15575C, 15585C, 15851C en 15857C)

Vraag van B. Segers aan de Staatssecretaris voor Asiel en Migratie over 'het elektronische platform voor gecombineerde verblijfsaanvraagprocedures' (*Hand.* Kamer 2020-21, 26 maart 2021, CRIV55COM425, 43, Vr. nr. 15814C)

Vraag van V. Scourneau aan de minister van Buitenlandse Zaken over de 'veiligheid van onze diplomaten in de Democratische Republiek Congo' (*Vr. en Ant*. Kamer 2020-21, 31 maart 2021, QRVA45, 99, Vr. nr. 218)

Vraag van A. Ponthier aan de minister van Buitenlandse Zaken over 'Oost-Congo - moord op Italiaans ambassadeur' (*Vr. en Ant*. Kamer 2020-21, 31 maart 2021, QRVA45, 113, Vr. nr. 242)

Vraag van K. Metsu aan de minister van Justitie over 'de terugkomst van Syriëstrijders en de OCAD analyse betreffende IS-vrouwen en -kinderen' (*Hand.* Kamer 2020-21, 31 maart 2021, CRIV55COM436, 35, Vr. nr. 15824C)

Vraag van K. Jadin aan de minister van Buitenlandse Zaken over 'IS-terreur in het gevangenenkamp Al-Hol' (*Vr. en Ant*. Kamer 2020-21, 7 april 2021, QRVA46, 124, Vr. nr. 228)

Vraag van E. Burton aan de minister van Buitenlandse Zaken over de 'risico's voor Belgische diplomaten in de DRC' (*Vr. en Ant*. Kamer 2020-21, 7 april 2021, QRVA46, 130, Vr. nr. 248)

Vraag van M. Freilich aan de minister van Justitie over 'Circles' (*Vr. en Ant*. Kamer 2020-21, 7 april 2021, QRVA46, 221, Vr. nr. 378)

Vraag van M. Vindevoghel aan de minister van Mobiliteit over de 'terreurdreiging voor het spoor' (*Vr. en Ant*. Kamer 2020-21, 15 april 2021, QRVA47, 122, Vr. nr. 112)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'het Brusselse kanaalplan en LIVC's' (*Vr. en Ant*. Kamer 2020-21, 15 april 2021, QRVA47, 294, Vr. nr. 400)

Vraag van B. Segers aan de Staatssecretaris voor Asiel en Migratie over 'de humanitaire visa via tussenpersonen' (*Vr. en Ant*. Kamer 2020-21, 15 april 2021, QRVA47, 352, Vr. nr. 155)

Vraag van P. Buysrogge aan de minister van Defensie over 'de nieuwe mini-drones' (*Hand.* Kamer 2020-21, 20 april 2021, CRIV55COM438, 10, Vr. nr. 14240C)

Vraag van A. Ponthier aan de minister van Defensie over 'de stopzetting van het contract voor het Open Source Intelligence System' (*Hand.* Kamer 2020-21, 20 april 2021, CRIV55COM438, 16, Vr. nr. 14534C)

Samengevoegde vragen van G. Defossé en P. Buysrogge aan de minister van Defensie over 'de offensieve cyberoperaties' (*Hand.* Kamer 2020-21, 20 april 2021, CRIV55COM438, 19, Vr. nrs. 14627C en 16305C)

Samengevoegde vragen van G. Defossé, Ch. Lacroix en K. Verduyckt aan de minister van Defensie over de 'militairen die banden hebben met extreemrechts' (*Hand.* Kamer 2020-21, 20 april 2021, CRIV55COM438, 45, Vr. nrs. 15600C, 5621C en 16526C)

Vraag van K. Metsu aan de minister van Justitie over 'het OCAD' (*Hand.* Kamer 2020-21, 21 april 2021, CRIV55COM442, 32, Vr. nr. 16385C)

Vraag van M. Freilich aan de minister van Justitie over 'de Chinese cyberspionage' (*Hand.* Kamer 2020-21, 21 april 2021, CRIV55COM445, 33, Vr. nr. 16518C)

Vraag van K. Metsu aan de minister van Justitie over 'de medeoprichter van het CCIB als lid van de raad van bestuur van Myria en Unia' (*Hand.* Kamer 2020-21, 21 april 2021, CRIV55COM445, 42, Vr. nr. 16626C)

Samengevoegde vragen van E. Samyn, K. Aouasti, K. Metsu en Th. Francken aan de minister van Buitenlandse Zaken over 'de Belgische IS-vrouwen in Syrië' (*Hand.* Kamer 2020-21, 27 april 2021, CRIV55COM449, 33, Vr. nrs. 14807C, 15558C, 15825C en 16400C)

Samengevoegde vragen van S. Cogolati, E. Samyn en Ch. Lacroix aan de minister van Buitenlandse Zaken over 'de bedreiging en intimidatie van opposanten in België door de Turkse regering' (*Hand.* Kamer 2020-21, 27 april 2021, CRIV55COM449, 82, Vr. nrs. 15441C, 113I en 16346C)

Actualiteitsdebat en toegevoegde vragen van G. Defossé, J. Pillen, Th. Francken, K. Jadin, Ch. Lacroix en A. Ponthier aan de minister van Defensie over 'het einde van Resolute Support Afghanistan' (*Hand.* Kamer 2020-21, 28 april 2021, CRIV55COM452, 1, Vr. nrs. 16438C, 16504C, 16580C, 16622C, 16820C en 16842C)

Vraag van C. Thibaut aan de minister van Binnenlandse Zaken over 'het toezicht op de gegevens in de ANG' (*Hand.* Kamer 2020-21, 28 april 2021, CRIV55COM453, 16, Vr. nr. 16719C)

Vraag van E. Platteau aan de minister van Ambtenarenzaken over 'het arrest van het Grondwettelijk Hof over de opslag van telecomdata' (*Hand.* Kamer 2020-21, 28 april 2021, CRIV55COM456, 13, Vr. nr. 16918C)

Vraag van S. Thémont aan de minister van Binnenlandse Zaken over de 'software om terreurdreigingen of radicalisering op te sporen' (*Vr. en Ant*. Kamer 2020-21, 3 mei 2021, QRVA50, 306, Vr. nr. 456)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'risico van aanslagen op de vaccinatiecentra' (*Vr. en Ant*. Kamer 2020-21, 3 mei 2021, QRVA50, 313, Vr. nr. 461)

Interpellatie van E. Gilissen aan de minister van Ambtenarenzaken over 'de vernietiging van de dataretentiewet door het Grondwettelijk Hof' (*Hand.* Kamer 2020-21, 3 mei 2021, CRIV55COM457, 1, Vr. nr. 122I)

Samengevoegde interpellatie en vragen van K. Bury, S. De Wit, K. Geens en N. Boukili aan de minister van Justitie over 'de dataretentiewetgeving' (*Hand.* Kamer 2020-21, 5 mei 2021, CRIV55COM463, 1, Vr. nrs. 120I, 16763C, 16799C en 17247C)

Samengevoegde vragen van K. Jadin en S. Van Hecke aan de minister van Justitie over 'de strijd tegen schadelijke sekten' (*Hand.* Kamer 2020-21, 5 mei 2021, CRIV55COM463, 19, Vr. nrs. 17266C en 17275C)

Vraag van E. Platteau aan de minister van Binnenlandse Zaken over 'de omvang van de dreiging die uitgaat van extreemrechts' (*Hand.* Kamer 2020-21, 5 mei 2021, CRIV-55COM464, 53, Vr. nr. 17111C)

Vraag van O. Depoortere aan de minister van Binnenlandse Zaken over 'de dreiging van extreemlinks' (*Hand.* Kamer 2020-21, 5 mei 2021, CRIV55COM464, 56, Vr. nr. 17199C)

Vraag van K. Metsu aan de minister van Buitenlandse Zaken over de 'toenemende kracht van de zelfverklaarde Islamitische Staat in het Midden-Oosten' (*Vr. en Ant*. Kamer 2020-21, 10 mei 2021, QRVA51, 140, Vr. nr. 68)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over de 'bestrijding van radicalisme tijdens de coronacrisis' (*Vr. en Ant*. Kamer 2020-21, 10 mei 2021, QRVA51, 323, Vr. nr. 470)

Vraag van V. Scourneau aan de minister van Buitenlandse Zaken over de 'cyberveiligheid' (*Vr. en Ant*. Kamer 2020-21, 18 mei 2021, QRVA52, 117, Vr. nr. 281)

Vraag van M. Freilich aan de minister van Justitie over de 'smartphones - Xiaomi, Oppo en OnePlus' (*Vr. en Ant*. Kamer 2020-21, 27 mei 2021, QRVA53, 317, Vr. nr. 466)

Vraag van V. Scourneau aan de minister van Defensie over de 'aankoop van miniatuurdrones door Defensie' (*Vr. en Ant*. Kamer 2020-21, 27 mei 2021, QRVA53, 331, Vr. nr. 230)

Vraag van Ch. Lacroix aan de minister van Defensie over de 'intrekking van de veiligheidsmachtiging van onze defensieattaché in Parijs' (*Vr. en Ant*. Kamer 2020-21, 27 mei 2021, QRVA53, 343, Vr. nr. 258)

Vraag van K. Jadin aan de minister van Defensie over de 'archieven van Defensie' (*Vr. en Ant*. Kamer 2020-21, 27 mei 2021, QRVA53, 344, Vr. nr. 259)

Samengevoegde vragen van E. Gilissen, Y. Ingels, Ph. Pivin, K. Verhelst, F. Demon en M. Freilich aan de minister van Binnenlandse Zaken over 'de hacking van de FOD Binnenlandse Zaken' (*Hand.* Kamer 2020-21, 27 mei 2021, CRIV55PLEN106, 13, Vr. nrs. 1679P, 1684P, 1685P, 1686P, 1689P en 1695P)

Samengevoegde vragen van A. Ponthier, S. De Vuyst en P. Buysrogge aan de minister van Defensie over 'de zaak-Jürgen Conings en de verantwoordelijkheid van de minister en van Defensie' (*Hand.* Kamer 2020-21, 27 mei 2021, CRIV55PLEN106, 101, Vr. nrs. 131I tot 133I)

Vraag van C. Taquin aan de minister van Binnenlandse Zaken over de 'evaluatie van de LIVC-R's' (*Vr. en Ant*. Kamer 2020-21, 2 juni 2021, QRVA54, 229, Vr. nr. 555)

Actualiteitsdebat en samengevoegde vragen van G. Defossé, P. Buysrogge, Th. Francken, S. De Vuyst, N. Boukili, D. Ducarme, K. Verduyckt, Ch. Lacroix, W. De Vriendt en A. Ponthier aan de minister van Defensie over 'de opvolging van de zaak van de voortvluchtige militair' (*Hand.* Kamer 2020-21, 2 juin 2021, CRIV55COM495, 14, Vr. nrs. 18241C, 18242C, 18309C, 18311C, 18318C, 18320C, 18321C, 18328C, 18388C, 18429C, 18466C en 18482C)

Samengevoegde vragen van J. Chanson, E. Platteau, K. Jadin, Ph. Pivin, D. Ducarme en K. Aouasti aan de minister van Binnenlandse Zaken over de 'politieagenten die op de radar staan van de inlichtingendiensten' (*Hand.* Kamer 2020-21, 2 juin 2021, CRIV55COM500, 7, Vr. nrs. 17992C, 18183C, 18401C, 18420C, 18421C, 18459C en 18460C)

Samengevoegde vragen van S. De Vuyst en N. Boukili aan de eerste minister over 'de zoektocht naar de zwaarbewapende militair' (*Hand.* Kamer 2020-21, 2 juin 2021, CRIV55COM501, 14, Vr. nrs. 18075C en 18161C)

Vraag van N. Boukili aan de minister van Justitie over 'het bespioneren van een aantal Europese landen door de Verenigde Staten' (*Hand.* Kamer 2020-21, 2 juin 2021, CRIV55COM501, 55, Vr. nr. 18457C)

Vraag van P. De Roover aan de eerste minister over 'de perslekken over geheime rapporten van de Staatsveiligheid' (*Hand.* Kamer 2020-21, 9 juin 2021, CRIV55COM511, 12, Vr. nr. 15727C)

Vraag van W. Vermeersch aan de minister van Justitie over de 'erkenning moskeeën' (*Vr. en Ant*. Kamer 2020-21, 12 juni 2021, QRVA55, 247, Vr. nr. 510)

Vraag van C. Thibaut aan de minister van Justitie over de 'verplichte kennisgeving met betrekking tot elke in de GGB Terrorist Fighters opgenomen medewerker' (*Vr. en Ant*. Kamer 2020-21, 12 juni 2021, QRVA55, 274, Vr. nr. 576)

Vraag van W. Vermeersch aan de minister van Binnenlandse Zaken over de 'erkenning moskeeën' (*Vr. en Ant*. Kamer 2020-21, 12 juni 2021, QRVA55, 334, Vr. nr. 561)

Vraag van C. Thibaut aan de minister van Binnenlandse Zaken over de 'meedelen van informatie door de inlichtingendiensten aan instanties of privaatrechtelijke of publiekrechtelijke personen' (*Vr. en Ant*. Kamer 2020-21, 12 juni 2021, QRVA55, 351, Vr. nr. 570)

Samengevoegde vragen van N. Boukili, R. Hedebouw en D. Ducarme aan de minister van Binnenlandse Zaken over 'de zaak-Conings' (*Hand.* Kamer 2020-21, 16 juin 2021, CRIV55COM518, 21, Vr. nrs. 18652C, 18653C en 18943C)

Gedachtewisseling en toegevoegde vragen van P. Buysrogge, Th. Francken, S. De Vuyst, K. Verduyckt, G. Defossé, M. De Maegd, A. Ponthier, D. Ducarme, Ch. Lacroix en H. Bogaert aan de minister van Defensie over 'het intern verslag van de algemene inspectie van Landsverdediging over de zaak Jürgen Conings' (*Hand.* Kamer 2020-21, 16 juin 2021, CRIV55COM519, 1, Vr. nrs. 18607C, 18605C, 18618C, 18656C, 18745C, 18808C, 18835C, 18907C, 18914C, 19011C en 19020C)

Vraag van Th. Francken aan Staatssecretaris voor Asiel en Migratie over 'de interne inspectie Fedasil van overlastgevende asielzoekers in de asielcentra' (*Hand.* Kamer 2020-21, 18 juin 2021, CRIV55COM520, 47, Vr. nr. 19059C)

Vraag van T. Van Grieken aan de minister van Justitie over 'de erkenning van moskeeën' (*Vr. en Ant*. Kamer 2020-21, 22 juni 2021, QRVA56, 177, Vr. nr. 507)

Vraag van T. Van Grieken aan de minister van Justitie over 'de screening van kandidaat-asielzoekers op linken met terroristische groeperingen of met radicale potentieel gewelddadige groeperingen' (*Vr. en Ant*. Kamer 2020-21, 22 juni 2021, QRVA56, 190, Vr. nr. 530)

Vraag van C. Thibaut aan de minister van Defensie over de 'meedelen van informatie door de ADIV aan instanties of privaatrechtelijke of publiekerechtelijke personen' (*Vr. en Ant*. Kamer 2020-21, 22 juni 2021, QRVA56, 233, Vr. nr. 560)

Vraag van C. Thibaut aan de minister van Binnenlandse Zaken over de 'ontruiming van de ZAD in Aarlen' (*Vr. en Ant*. Kamer 2020-21, 22 juni 2021, QRVA56, 252, Vr. nr. 578)

Samengevoegde vragen van M. De Maegd, M. Ben Achour en P. De Roover aan de minister van Buitenlandse Zaken over 'de Belgische missie in het kamp Al-Roj' (*Hand.* Kamer 2020-21, 29 juni 2021, CRIV55COM530, 89, Vr. nrs. 18768C, 18798C en 18884C)

Samengevoegde vragen van O. Depoortere, Y. Ingels en T. Vandenput aan de minister van Binnenlandse Zaken over 'het personeelstekort bij de politie' (*Hand.* Kamer 2020-21, 30 juni 2021, CRIV55COM531, 20, Vr. nrs. 19355C, 19400C en 19429C)

Vraag van E. Burton aan de minister van Buitenlandse Zaken over de 'aanwezigheid van Chinese inlichtingendiensten in Luik' (*Vr. en Ant*. Kamer 2020-21, 30 juni 2021, QRVA57, 118, Vr. nr. 327)

Vraag van C. Thibaut aan de minister van Justitie over de 'beoordeling van de dreiging die uitgaat van de anti-5g-activisten' (*Vr. en Ant*. Kamer 2020-21, 30 juni 2021, QRVA57, 192, Vr. nr. 587)

Vraag van Ph. Pivin aan de minister van Justitie over de 'Cel Radicalisme bij de Dienst Vreemdelingenzakenscreening van buitenlandse investeringen – interdepartementale screeningcommissie' (*Vr. en Ant*. Kamer 2020-21, 30 juni 2021, QRVA57, 196, Vr. nr. 597)

Vraag van D. Safai aan Staatssecretaris voor Asiel en Migratie over 'de humanitaire visa voor IS-vrouwen en -kinderen' (*Hand.* Kamer 2020-21, 2 juli 2021, CRIV55COM535, 21, Vr. nr. 19570C)

Gedachtewisseling, toegevoegde interpellatie en vragen van K. Jadin, A. Ponthier, Th. Francken en G. Defossé aan de minister van Defensie over 'het rapport van Comité I en de psychosociale zorg in het leger' (*Hand.* Kamer 2020-21, 5 juli 2021, CRIV55COM537, 1, Vr. nrs. 18547C, 19099C, 19136C, 00149I, 19252C, 19257C en 19595C)

Vraag van S. Loones aan de minister van Begroting over 'het budget van Defensie' (*Hand.* Kamer 2020-21, 6 juli 2021, CRIV55COM539, 20, Vr. nr. 18077C)

Vraag van A. Ponthier aan de minister van Justitie over de 'invloed Soros' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 250, Vr. nr. 595)

Vraag van Y. Van Camp aan de minister van Justitie over de 'screening haatimam' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 261, Vr. nr. 553)

Vraag van K. Verduyckt aan de minister van Justitie over 'extreemrechts bij penitentiaire bewaking' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 268, Vr. nr. 583)

Vraag van A. Van Bossuyt aan de minister van Justitie over de 'Chine spionage via Thousand Talents programma' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 279, Vr. nr. 612)

Vraag van K. Jadin aan de minister van Defensie over de 'opvolging van het personeel van Defensie' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 291, Vr. nr. 274)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'Cel Radicalisme bij de Dienst Vreemdelingenzaken' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 345, Vr. nr. 148)

Vraag van G. Dallemagne aan de minister van Justitie over 'het OCAD-rapport over het wahabisme, het jihadisme en het terrorisme' (*Hand.* Kamer 2020-21, 14 juli 2021, CRIV55COM556, 7, Vr. nr. 19771C)

Samengevoegde vragen van J. Pillen, S. Creyelman en K. Jadin aan de minister van Defensie over 'de cybercomponent' (*Hand.* Kamer 2020-21, 14 juli 2021, CRIV55COM557, 23, Vr. nrs. 17854C, 18003C en 19321C)

Samengevoegde vragen van G. Defossé, V. Reynaert en Ch. Lacroix aan de minister van Defensie over 'de onthulling van geheime informatie over de in Europa opgeslagen kernwapens' (*Hand.* Kamer 2020-21, 14 juli 2021, CRIV55COM557, 27, Vr. nrs. 18336C, 18384C en 18433C)

Vraag van Th. Francken aan de minister van Defensie over 'Psyops' (*Hand.* Kamer 2020-21, 14 juli 2021, CRIV55COM557, 34, Vr. nr.18783C)

Samengevoegde interpellaties van P. De Roover en B. Pas aan de eerste minister over 'het ontslag van regeringscommissaris Haouach' (*Hand.* Kamer 2020-21, 15 juillet 2021, CRIV55PLEN122, 26, Vr. nrs. 162I en 163I)

Vraag van S. Van Hecke aan de minister van Buitenlandse Zaken over het 'nationaal veiligheidsoverleg – moeizame communicatie' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 105, Vr. nr. 341)

Vraag van C. Thibaut aan de minister van Buitenlandse Zaken over het 'uitblijven van antwoorden van de NVO aan het Comité I inzake veiligheidsmachtigingen' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 108, Vr. nr. 342)

Vraag van Y. Ingels aan de minister van Mobiliteit over de 'toekenning van toegangsbadges voor airside' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 185, Vr. nr. 601)

Vraag van K. Metsu aan de minister van Justitie over de 'erkenning Brusselse geloofsgemeenschappen' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 261, Vr. nr. 617)

Vraag van K. Verduyckt aan de minister van Binnenlandse Zaken over 'extreemrechts bij politie' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 347, Vr. nr. 665)

Gedachtewisseling en toegevoegde vragen van B. Pas, E. Samyn, D. Van Langenhove en K. Metsu aan de eerste minister en de minister van Buitenlandse Zaken over 'het terughalen van IS-terroristen naar België' (*Hand.* Kamer 2020-21, 22 juli 2021, CRIV55COM560, 1, Vr. nrs. 19979C, 19977C, 19981C en 19995C)

Gedachtewisseling en toegevoegde vragen van Th. Francken, A. Ponthier, W. De Vriendt, G. Dallemagne, K. Verduyckt, S. De Vuyst, G. Defossé en Ch. Lacroix aan de minister van Defensie over 'de vervanging van generaal-majoor Boucké aan het hoofd van ADIV' (*Hand.* Kamer 2020-21, 22 juli 2021, CRIV55COM561, 1, Vr. nrs. 19973C, 19974C, 19975C, 19976C, 19983C, 19990C, 19993C en 19994C)

Vraag van Y. Ingels aan de minister van Buitenlandse Zaken over de 'nationale veiligheidsoverheid – rol en opdrachten' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 92, Vr. nr. 347)

Vraag van S. Cogolati aan de minister van Buitenlandse Zaken over 'spionage door NSA met de hulp van Denemarken' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 105, Vr. nr. 363)

Vraag van K. Jadin aan de minister van Buitenlandse Zaken over 'spionage door NSA met de hulp van Denemarken' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 109, Vr. nr. 365)

Vraag van B. Moyaers aan de minister van Buitenlandse Zaken over de 'politieke zoektocht naar hackers' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 120, Vr. nr. 376)

Vraag van S. De Vuyst aan de minister van Buitenlandse Zaken over 'Amerikaanse spionage' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 123, Vr. nr. 380)

Vraag van C. Taquin aan de minister van Justitie over de 'strijd tegen sektarische excessen tijdens de pandemie' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 184, Vr. nr. 567)

Vraag van E. Burton aan de minister van Justitie over de 'Veiligheid van de Staat en spionnage' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 194, Vr. nr. 592)

Vraag van J. Pillen aan de minister van Defensie over het 'personeel van de ADIV' (*Vr. en Ant*. Kamer 2020-21, 24 juli 2021, QRVA60, 303, Vr. nr. 286)

Vraag van Y. Ingels aan de eerste minister over 'het veilig kunnen uitwisselen van gevoelige informatie' (*Vr. en Ant*. Kamer 2020-21, 11 augustus 2021, QRVA61, 135, Vr. nr. 111)

Vraag van D. Safai aan de minister van Binnenlandse Zaken over de 'cursussen radicalisme en meldpunt radicalisering' (*Vr. en Ant*. Kamer 2020-21, 11 augustus 2021, QRVA61, 337, Vr. nr. 227)

Gedachtewisseling en toegevoegde vragen van Th. Francken, A. Flahaut, G. Liekens, S. de Laveleye, G. Defossé, Ch. Lacroix, V. Reynaert, D. Van Langenhove, W. De Vriendt, Fr. De Smet, H. Rigot, K. Jadin, J. Chanson, T. Vandenput, S. Moutquin, E. Platteau, N. Boukili en B. Segers aan de eerste minister over 'de situatie in Afghanistan' (*Hand.* Kamer 2020-21, 26 augustus 2021, CRIV55COM563, 1, Vr. nrs. 20147C, 20148C, 20156C, 20147C, 20118C, 20094C, 20103C, 20104C, 20140C, 20162C, 20122C, 20154C, 20155C, 20083C, 20093C, 20115C, 20158C, 20137C, 20146C, 20157C, 20057C, 20067C, 20095C, 20110C, 20119C, 20120C, 20127C, 20145C, 20130C, 20132C, 20133C, 20134C, 20135C, 20136C, 20138C, 20139C, 20141C, 20142C, 20161C, 20163C, 20164C en 20165C)

Vraag van J. Donné aan de minister van Financiën over de 'raadplegingen CAP2' (*Vr. en Ant*. Kamer 2020-21, 6 september 2021, QRVA62, 216, Vr. nr. 146)

Vraag van W. Vermeersch aan de minister van Financiën over de 'erkenning van moskeeën' (*Vr. en Ant*. Kamer 2020-21, 6 september 2021, QRVA62, 228, Vr. nr. 398)

Vraag van B. Segers aan de minister van Justitie over de 'screening van humanitaire visa' (*Vr. en Ant*. Kamer 2020-21, 6 september 2021, QRVA62, 319, Vr. nr. 606)

Vraag van M. Freilich aan de minister van Justitie over de 'NSO group software' (*Vr. en Ant*. Kamer 2020-21, 6 september 2021, QRVA62, 337, Vr. nr. 658)

Vraag van Y. Ingels aan de eerste minister over de 'projecten van veiligheidsdepartementen bij de Regie der Gebouwen' (*Vr. en Ant*. Kamer 2020-21, 20 september 2021, QRVA 63, 338, Vr. nr. 150)

Samengevoegde vragen van Th. Francken, S. Moutquin en D. Van Langenhove aan de Staatssecretaris voor Asiel en Migratie over 'het humanitaire visaprogramma voor Afghanen' (*Hand.* Kamer 2020-21, 22 september 2021, CRIV55COM575, 31, Vr. nrs. 20703C, 20883C, 20886C, 20888C, 20916C en 20931C)

Samengevoegde vragen van M. Freilich, S. Van Hecke, N. Boukili en E. Van Hoof aan de minister van Justitie over 'de afluistersoftware' (*Hand.* Kamer 2020-21, 22 september 2021, CRIV55COM577, 1, Vr. nrs. 19985C, 20000C, 20448C en 20845C)

Samengevoegde vragen van M. Freilich, E. Gilissen en K. Gabriëls aan de minister van Justitie over 'de seponering in het kader van het onderzoek naar de Chinese spionnen' (*Hand.* Kamer 2020-21, 22 september 2021, CRIV55COM577, 41, Vr. nrs. 20313C, 20325C en 20903C)

Vraag van K. Jiroflée aan de minister van Justitie over 'de niet-naleving van tijdelijke huisverboden' (*Hand.* Kamer 2020-21, 22 september 2021, CRIV55COM577, 45, Vr. nr. 20335C)

Actualiteitsdebat en toegevoegde vragen van P. De Roover, K. Jadin, V. Reynaert, H. Rigot en S. Cogolati aan de minister van Buitenlandse zaken over 'Afghanistan' (*Hand.* Kamer 2020-21, 28 september 2021, CRIV55COM579, 7, Vr. nrs. 20256C, 20270C, 20271C, 20408C, 21142C, 21173C en 21221C)

Samengevoegde vragen van S. Van Hecke en E. Van Hoof aan de minister van Buitenlandse zaken over 'de impact van Pegasus op diplomatieke relaties en de te nemen maatregelen in het kader daarvan' (*Hand.* Kamer 2020-21, 28 september 2021, CRIV55COM579, 19, Vr. nrs. 20007C en 21061C)

Vraag van M. Dillen aan de minister van Justitie over 'Oussama Atar en de aanslagen in Parijs en Brussel' (*Hand.* Kamer 2020-21, 29 september 2021, CRIV55COM586, 15, Vr. nr. 20496C)

Vraag van Ph. Pivin aan de minister van Economie over de 'screening van buitenlandse investeringen – interdepartementale screeningscommissie' (*Vr. en Ant*. Kamer 2020-21, 2 oktober 2021, QRVA 64, 29, Vr. nr. 566)

Vraag van S. Creyelman aan de minister van Defensie over het 'spionagemateriaal in de Belgische ambassade in Ankara' (*Vr. en Ant*. Kamer 2020-21, 2 oktober 2021, QRVA 64, 175, Vr. nr. 315)

Vraag van S. Verherstraeten aan de minister van Defensie over de 'militairen – rechts-extremistische sympathieën' (*Vr. en Ant*. Kamer 2020-21, 2 oktober 2021, QRVA 64, 178, Vr. nr. 320)

Vraag van D. Safai aan Staatssecretaris voor Asiel en Migratie over 'de repatriëring van IS-terroristen en hun kinderen' (*Hand.* Kamer 2020-21, 5 oktober 2021, CRIV55COM588, 31, Vr. nr. 20943C)

Vraag van D. Van Langenhove aan Staatssecretaris voor Asiel en Migratie over 'de resultaten van de veiligheidsscreening' (*Hand.* Kamer 2020-21, 5 oktober 2021, CRIV55COM588, 31, Vr. nr. 20993C)

Vraag van G. Dallemagne aan de minister van Justitie over de 'salafistische kern te Molenbeek' (*Vr. en Ant*. Kamer 2020-21, 6 oktober 2021, QRVA 65, 422, Vr. nr. 724)

Vraag van E. Van Hoof aan de minister van Defensie over de 'spionagesoftware Pegasus' (*Vr. en Ant*. Kamer 2020-21, 6 oktober 2021, QRVA 65, 439, Vr. nr. 326)

Vraag van S. Cogolati aan de minister van Justitie over 'het onderzoek naar de daders van de cyberaanval tegen Belnet op 4 mei 2021' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV55COM596, 4, Vr. nr. 21135C)

Vraag van K. Metsu aan de minister van Justitie over de 'vastgestelde malversaties bij vzw Moslimexecutieve' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV55COM596, 26, Vr. nr. 21579C)

Vraag van S. Verherstraeten aan de minister van Binnenlandse Zaken over 'de toename van de rechts-extremistische dreiging' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV-55COM597, 35, Vr. nr. 20009C)

Samengevoegde vragen van M. Freilich en J. Chanson aan de minister van Binnenlandse Zaken over 'het beëindigen van OVG' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV-55COM597, 55, Vr. nrs. 20331C en 20404C)

Samengevoegde vragen van M. Freilich en K. Metsu aan de minister van Binnenlandse Zaken over 'de aanhouding van enkele geradicaliseerde mannen' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV55COM597, 76, Vr. nrs. 20744C, 21288C en 21384C)

Samengevoegde vragen van A. Ponthier, K. Metsu en P. Dewael aan de eerste minister over 'de aanhoudende problemen met islamfundamentalisme bij de Moslimexecutieve' (*Hand.* Kamer 2020-21, 7 oktober 2021, CRIV55PLEN127, 5, Vr. nrs. 1932P, 1945P en 1948P)

Vraag van M. Freilich aan de eerste minister over de 'NSO group software' (*Vr. en Ant*. Kamer 2020-21, 10 oktober 2021, QRVA 66, 39, Vr. nr. 129)

Actualiteitsdebat en samengevoegde vragen van K. Jadin, A. Ponthier, G. Defossé, Th. Francken en A. FLahaut aan de minister van Defensie over 'het onderzoek naar extremisme' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM606, 1, Vr. nrs. 20281C, 20292C, 20864C, 20942C,21565C, 22019C en 21674C)

Samengevoegde vragen van A. Ponthier en G. Dallemagne aan de minister van Defensie over 'de hervormingen binnen de ADIV na aanstelling van vice-admiraal W. Robberechts als diensthoofd' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM606, 10, Vr. nrs. 20306C en 20923C)

Samengevoegde vragen van T. Vandenput en J. Chanson aan de minister van Binnenlandse Zaken over 'de problemen met het ASTRID-netwerk' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM611, 40, Vr. nrs. 21129C en 21212C)

Vraag van S. Loones aan de minister van Binnenlandse Zaken over 'seining van de heer Puigdemont in het Schengen Information System (SIS)' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM611, 53, Vr. nr. 21308C)

Samengevoegde vragen van S. Goethals en O. Depoortere aan de minister van Binnenlandse Zaken over 'de burgerlijke partijstelling van de minister' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM611, 66, Vr. nrs. 21542C en 21575C)

Vraag van E. Van Hoof aan de minister van Justitie over de 'spionagesoftware Pegasus' (*Vr. en Ant*. Kamer 2021-22, 26 oktober 2021, QRVA 67, 247, Vr. nr. 689)

Vraag van A. Ponthier aan de minister van Justitie over de 'kostprijs operatie Jürgen Conings' (*Vr. en Ant*. Kamer 2021-22, 26 oktober 2021, QRVA 67, 252, Vr. nr. 699)

Vraag van S. Creyelman aan de minister van Defensie over 'de mogelijke verspreiding van complottheorieën door Rusland' (*Hand.* Kamer 2021-22, 27 oktober 2021, CRIV55COM618, 13, Vr. nr. 22136C)

Samengevoegde vragen van G. Defossé en P. Buysrogge aan de minister van Defensie over 'de uitspraken van de heer Lipszyc in een interview' (*Hand.* Kamer 2021-22, 27 oktober 2021, CRIV55COM618, 21, Vr. nrs. 22258C en 22364C)

Vraag van M. Freilich aan de eerste minister over 'het ondermijnen van encryptie' (*Hand.* Kamer 2021-22, 27 oktober 2021, CRIV55COM623, 20, Vr. nr. 22038C)

Vraag van K. Geens aan de minister van Binnenlandse Zaken over de 'Operatie Sky' (*Hand*. Kamer 2021-22, 28 oktober 2021, CRIV55PLEN136, 24, Vr. nr. 1990P)

Samengevoegde vragen van A. Ponthier en N. Boukili aan de minister van Justitie over 'de huiszoekingen bij militairen op grond van een vermoeden van aanzetten tot terreur' (*Hand.* Kamer 2021-22, 10 november 2021, CRIV55COM625, 15, Vr. nrs. 22510C en 22521C)

Vraag van M. Freilich aan de minister de Justitie over de 'afluistersoftware NSO' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 257, Vr. nr. 728)

Vraag van S. Creyelman aan de minister van Defensie over 'extremisme bij Defensie - opvolging' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 338, Vr. nr. 321)

Vraag van M. Freilich aan de eerste minister over de 'aanpak dark web' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 129, Vr. nr. 145)

Vraag van M. Freilich aan de eerste minister over de 'repressieve capaciteit inzake cybercriminaliteit' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 130, Vr. nr. 146)

Vraag van Th. Francken aan de minister van Justitie over 'de kolos van Molenbeek' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 260, Vr. nr. 747)

Vraag van S. Creyelman aan de minister van Defensie over de 'extremisme bij Defensie - opvolging' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 338, Vr. nr. 321)

Vraag van S. Van Hecke aan de minister van Defensie over het 'Pegasus-project – de acties van ADIV' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 349, Vr. nr. 355)

Vraag van S. Matheï aan de eerste minister over de 'evaluatie GDPR' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 402, Vr. nr. 221)

Vraag van K. Jadin aan de minister van Defensie over de 'veiligheid van apparaten van Chinese makelij' (*Vr. en Ant*. Kamer 2021-22, 25 november 2021, QRVA 70, 285, Vr. nr. 357)

Vraag van A. Vicaire aan de minister van Digitalisering over 'de zaak Pegasus en de bescherming van Belgische politici' (*Hand*. Kamer 2021-22, 30 november 2021, CRIV55COM630, 1, Vr. nr. 20099C)

Vraag van K. Metsu aan de minister van Justitie over 'de aanpak van geradicaliseerden in onze gevangenissen' (*Hand*. Kamer 2021-22, 2 december 2021, CRIV55PLEN144, 15, Vr. nr. 2090P)

Vraag van Y. Ingels aan de eerste minister over het 'Federaal beleid inzake drugs – georganiseerde misdaad' (*Vr. en Ant.* Kamer 2021-22, 6 december 2021, QRVA 71, 67, Vr. nr. 153)

Vraag van M. Dillen aan de minister van Justitie over de 'verslag Rekenhof DAV – transversale doelstellingen AV' (*Vr. en Ant.* Kamer 2021-22, 6 december 2021, QRVA 71, 225, Vr. nr. 796)

Vraag van E. Burton aan de minister van Justitie over 'deepfakes' (*Vr. en Ant.* Kamer 2021-22, 6 december 2021, QRVA 71, 248, Vr. nr. 823)

Vraag van S. Cogolati aan de minister van Justitie over het 'gevaar voor spionage in het China-Belgium Technology Center' (*Vr. en Ant.* Kamer 2021-22, 6 december 2021, QRVA 71, 250, Vr. nr. 824)

Samengevoegde vragen van B. Pas en K. Metsu aan de eerste minister over 'de manke opvolging van jihadisten in dit land' (*Hand.* Kamer 2021-22, 9 december 2021, CRIV55PLEN145, 23, Vr. nrs. 2099P en 2124P)

Samengevoegde vragen van K. Jadin en M. Vindevoghel aan de minister van Defensie over de 'rekrutering van Belgische militairen' (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM640, 3, Vr. nrs. 23244C en 23388C)

Vraag van G. Defossé aan de minister van Defensie over 'de doodsbedreiging van een minister door een militair' (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM640, 7, Vr. nr. 23346C)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over 'het extremisme in België' (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM642, 6, Vr. nr. 23074C)

Vraag van E. Platteau aan de minister van Binnenlandse Zaken over 'de bestrijding van extremisme door sociale re-integratie en 'disengagement'" (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM642, 13, Vr. nr. 23104C)

Samengevoegde vragen van E. Platteau, F. Demon, T. Vandenput en O. Depoortere aan de minister van Binnenlandse Zaken over 'het OCAD-rapport over de coronacrisis' (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM642, 14, Vr. nrs. 23178C, 23229C, 23393C en 23415C)

Samengevoegde vragen van K. Metsu en Ph. Pivin aan de minister van Justitie over 'het Executief van de Moslims van België' (*Hand.* Kamer 2021-22, 16 december 2021, CRIV55PLEN148, 15, Vr. nrs. 2131P en 2143P)

Samengevoegde vragen van K. Metsu en B. Pas aan de minister van Justitie over 'het foutief informeren van het Parlement' (*Hand.* Kamer 2021-22, 16 december 2021, CRIV55PLEN148, 21, Vr. nrs. 206I en 214I)

Vraag van S. Cogolati aan de minister van Ambtenarenzaken over het 'gevaar voor censuur en cybersurveillance op smarphones van Huawei, Xiaomi en OnePlus' (*Vr. en Ant.* Kamer 2021-22, 16 december 2021, QRVA 72, 180, Vr. nr. 349)

Vraag van S. Creyelman aan de minister van Defensie over 'de uitbouw van de cybercomponent binnen Defensie' (*Vr. en Ant.* Kamer 2021-22, 16 december 2021, QRVA 72, 228, Vr. nr. 346)

Vraag van Th. Francken aan de minister van Binnenlandse Zaken over 'de screening bij de evacuatieoperatie' (*Vr. en Ant.* Kamer 2021-22, 16 december 2021, QRVA 72, 335, Vr. nr. 386)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over 'het jaarverslag van de Veiligheid van de Staat' (*Hand.* Kamer 2021-22, 20 december 2021, CRIV55COM645, 2, Vr. nr. 22634C)

Vraag van K. Bury aan de minister van Justitie over 'de aankoop van kantoorgebouwen in de Brusselse Noordwijk' (*Hand.* Kamer 2021-22, 20 december 2021, CRIV55COM645, 26, Vr. nr. 23267C)